CONTEMPORARY SECURITY MANAGEMENT

FOURTH EDITION

John J. Fay | David Patterson

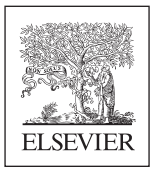
Contemporary Security Management

Contemporary Security Management

Fourth Edition

John J. Fay

David Patterson



Butterworth-Heinemann
An imprint of Elsevier

Butterworth-Heinemann is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-809278-1

Publisher: Candice Janco
Acquisition Editor: Laura S. Kelleher
Editorial Project Manager: Hilary Carr
Production Project Manager: Anitha Sivaraj
Cover Designer: Victoria Pearson

Typeset by MPS Limited, Chennai, India

Contents

Introduction

Security is a difficult concept because it can refer to the objective absence of threats and subjective feeling of being secure. To be a successful manager, you must have specialized knowledge of security technology as well as knowledge of management principles. I first became familiar with Jack Fay's books after I had worked as a manager for several years. I had worked in security functions for several years so I had the technical knowledge, but had limited managerial knowledge. In 1994, I discovered Jack's book "Contemporary Security Management" and found it was an excellent source for guidance in organizing my security department, establishing our mission, preparing job descriptions for each of the analysts who worked for me, interviewing them, and training them.

I have continued to use his book through the years and looked forward to the later editions in my career and have always found them useful—especially in understanding security terminology, technology, and various security functions. I have also found that my peers in other organizations have used the text and have recommended it to others. I have found this book to be well written, easy to read, and up to date. This book explains in exact detail an abundance of fresh new strategies you can implement to improve security awareness in your organization.

I was honored and yet humbled when Jack asked me to participate in writing this edition as co-author and I have sincerely tried to contribute to this book through my experience in applying the concepts.

The information you are about to read has proven results. Each chapter provides new information that will help you stay in control of your organization, and stay ahead of the competition. If you follow the information we reveal in this book, it is highly possible you will enjoy a very successful security career.

CHAPTER 1

Future of the Chief Security Officer

What You Will Learn

- Security concepts used in the earliest history of mankind.
- The impact of technological advances on security.
- The meaning of security convergence.
- How the consolidation of functions improves security productivity.
- Challenges facing the Chief Security Officer.

INTRODUCTION

Security was essential to civilization in its earliest stages. During the late Stone Age (Neolithic Period) when settlements were created and people made the transition from hunters to farmers, they created villages with fortified living areas for individual families. The villages had many physical barriers for protection against the risk at the time which was being attacked by people from another village. Walls, posts, thick enclosures, heavy doors with stout closures, animals, moats, and traps all served to protect communities from attack from their enemies. Therefore, even at these ancient times, a variety of physical security resources were employed to mitigate their risks (Saint-Blanquat, 1986).

The earliest alarms to signal the approach of strangers were animate, and communications depended upon smoke and light signals. In the modern era, Information Technology (IT) traces its origins to the patent of the telegraph by William Cooke and Charles Wheatstone in 1836. Remote voice communication became possible by Alexander Graham Bell's development of the telephone in 1876 (Greer, 1979; Grosvenor, 1997).

The alarm industry grew in tandem with the telephone. Edwin T. Holmes was able to have cable for alarm connections laid at the same time cables for telephones were being installed in buildings (Holmes, 1990). Wires historically transmitted alarm signals. These signals are transmitted over a

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00001-3

proprietary connection or on a common carrier (telephone line) of various types. In modern times, wireless communications and computer-based systems have increased the reliability and speed of such signals. An operator in a monitoring station no longer is bound to record routine opening and closing signals. Now the operator can be alert to any exceptions to the system and respond to them without distraction (Mahoney, 1995).

The physical security measures described earlier have been enhanced first by electrification and later by computerization. A broad range of devices have been developed to aid security personnel in protecting the organization's assets:

- Closed Circuit Television (CCTV) that allows an operator to view various locations around the facility from their desk and assess the reason for an alarm. The system will also record images that are viewed at a later time for forensic analysis.
- Intrusion detection systems that offer overt and covert capabilities as well as improved accuracy for detecting unwanted personnel.
- Access control systems using advanced biometric-based automatic identification systems that offer a higher degree of certainty that individuals who present themselves at a checkpoint are indeed authorized personnel.
- Improved communications systems including networks offering multiple means and paths.
- Computer aided dispatch systems featuring consolidated security functions to assist the operator in interpreting various alarms, and helping him select the most appropriate response.

The first computer device was invented in 1946; by 1958, computer technology had developed rapidly with much promise. At about that time the first computer crimes were discovered. Crimes that consisted mostly of theft of output and theft of computer time to perform unauthorized tasks. Since computing and the internet were not designed with security as a foremost consideration, it was inevitable that serious abuses and misuses would occur, leading eventually to what many people consider a current crisis (Schell, 2004; Parker, 1976). As physical and logical security technologies have matured, they can now be used to support each other. The development of the IP network and the migration of sensors and appliances to a common network have helped drive this transformation. Cameras are now Internet Protocol based and operate over the enterprise network instead of a separate network; access control card readers and intrusion detection sensors also attach to the common enterprise network instead of a proprietary network; identification databases, access logs, policies, and procedures are stored and generated by computers.

Since the network supports the enterprise data and workflow as well as the security devices, the two concerns are now subjected to the same threats and need to be considered together.

ORIGIN OF CORPORATE SECURITY

According to Dalton (2003), corporate security organizations began sometime before 1960 when companies used a person to look after the building during the nighttime and signal a warning if any incidents such as fire or break-ins occurred.

Throughout the 1960s and into the later years of the 20th century, more and more duties were added including more guarding responsibilities such as patrolling throughout the property, building access control, parking control, and similar duties. As time passed, the security organization grew as it continued to perform duties such as security patrols, but, also took on more operational responsibilities such as responding to emergencies, monitoring machinery, operating security equipment such as CCTV cameras and monitors, escorting employees, and investigating incidents (Dalton, 2003).

As industries developed weapons systems in response to the cold war threats, and other government assets became more sophisticated, the need for greater protection of not only governmental assets but also the information and assets of companies manufacturing weapon systems for the government. The government required different levels of control for information and assets considered most critical to the national defense (Kovacich and Halibozek, 2003:51).

CONTEMPORARY DRIVERS FOR CORPORATE SECURITY

One of the adverse effects of organizations growing and becoming internationally involved has been the increase in the number of risks which face large organizations with exposure to operational threats all over the world. This international exposure has made the job of protecting business assets much more complicated and has led to the development of sophisticated physical protection systems (PPS) to assist security personnel in accomplishing the role of protecting the organization's assets. Also, the skills required by the security personnel are more numerous and more complex.

The proliferation of threats to organizations doing business in global markets has driven the growth of security organizations due to

- Dependence on the internet for business transactions
- The appearance of worldwide terrorism and their attacks on civilian targets and symbols of western values has made large commercial organizations realize they are attractive targets for terrorists

- The realization that damage to the US economy causes as much fear as damage to physical infrastructure has propelled the need for disaster recovery and business continuity programs
- The escalation in the hostile activities of animal rights and other activist groups toward an organization's assets and employees
- The growth of government regulations on the conduct of businesses has also caused more growth of security departments due to the need for effective corporate governance and the plethora of associated regulations
- Access to large amounts of private data that can be used for financial gain
- Large and small professional criminal syndicates aimed at cyber crime
- Malicious political activists such as the "Anonymous Group"
- The growth of the Determined Human Adversaries
- Malware mercenaries
- Nation state cyber warfare attacks (such as the attack on Sony Pictures)

These new threats to organizations have resulted in the contemporary security duties that include:

- Protection of intellectual property
- Auditing responsibilities
- Responsibility for ethical policies
- Supply chain security
- Export control compliance
- Oversight of the divestiture of businesses
- Due diligence
- Personal security (Executive Protection)
- Physical security
- Project management for implementing PPS
- Information security
- Corporate governance
- Compliance and ethics programs
- Crime prevention and detection
- Fraud deterrence
- Investigations
- Risk management
- Business continuity planning
- Disaster recovery
- Information security
- Crisis and emergency management
- Environment, safety, and health

HISTORY OF DATA SECURITY

Even in the earliest history of humanity, people realized that they needed to protect the information they were trying to communicate to others and provide some means of detecting altering or tampering.

As civilization progressed, governments developed classification systems to allow them to manage their information according to the degree of sensitivity. In modern times, rapid advancements in telecommunications, computer hardware and software, and data encryption have helped organizations deal with the challenges of data protection. The promotion of smaller, faster, and cheaper computers made electronic data processing within the reach of small business and home users that quickly became interconnected through the Internet.

The rapid growth and extensive use of electronic data processing and electronic business conducted over networks and through the Internet, along with numerous international terrorist acts promoted the need for improved techniques for protecting the computers and particularly the information they store, process and transmit. The academic disciplines of computer security and information assurance emerged along with numerous professional organizations—all sharing the common goals of ensuring the security and reliability of information systems.

EVOLUTION OF INFORMATION THREATS

The threats to the information assets continue to evolve in the IT world as illustrated by the following threat descriptions contained in SCMagazine:

1970s

The 1970s was a timeframe in information security history largely untouched by digital calamity but marked more so by the exploration of emerging telecommunications technology. The first modern day hackers appeared as they attempted to circumvent the system and make free phone calls, a practice that became known as "phreaking." Perhaps, the most publicly well-known phreaker was John Draper, a.k.a. Captain Crunch, who helped pioneer the practice. Draper was later arrested and convicted on charges related to his nefarious phreaking activities multiple times.

1980s

The 1980s saw the birth of computer clubs. This decade subsequently ushered in the era of malware, marking the first virus (named "Brain") in 1986

as well as the infamous Morris Worm in 1988. The Computer Fraud and Abuse Act was instituted in 1986 and for the first time, a computer hacker, Kevin Poulsen, was featured on America's Most Wanted. Poulsen was finally arrested in 1991, after spending several years as a fugitive. Since his release from prison, however, he has reinvented himself as a journalist and at one point, regularly wrote for the online computer security news portal SecurityFocus, which was purchased by Symantec in 2002.

1990s

The 1990s brought with it the dawn of the modern information security industry. Notable threats witnessed during this decade included the Michelangelo virus, Melissa, and Concept. Distributed denial of service attacks and the bots that made them possible were also born, such as Trin00, Tribal Flood Network, and Stacheldracht.

Beyond malware, America OnLine (AOL) suffered through the first real phishing attacks as fraudsters aimed their efforts at stealing users' credentials. Privacy watchdogs called out in concern as tracking cookies were born, allowing ad networks to monitor user surfing behaviors in a rudimentary fashion.

2000s

The first decade of the 21st century saw malicious Internet activity turn into a major criminal enterprise aimed at monetary gain. Adware and spyware entered the scene with such programs as Conducent TimeSink, Aureate/Radiate, and Comet Cursor.

Perhaps even more visible than adware and spyware, aggressively self-propagating malware also appeared. Big name threats such as Code Red, Nimda, Welchia, Slammer, and Conficker all began taking advantage of unpatched machines. Phishing attacks also became mainstream; first heavily targeting online banking then moving onto social networking sites. Zero-day attacks, rootkits, rogue antispyware, SPIM, clickfraud and other attacks also all made their mainstream debut in the current decade. (A brief history of internet security—SCMagazine, http://www.scmagazine.com/a-brief-history-of-internet-security//article/149611/ accessed January 29, 2016.)

OPERATIONAL VS STRATEGIC

In the past, both physical and IT security have been concerned with the operational needs of the organization such as controlling access to buildings and computers; issuing identification credentials, and assigning and withdrawing access rights to the facilities and computer files.

However, organizations need a way to focus and stay focused. They need a precise strategy and well-executed action plan. The strategic plan in and of itself cannot help organizations change and move ahead to capture more market share, improve products, increase customer satisfaction, or improve security. Effective strategic business planning requires a living process that keeps the organization focused on the right issues. Management must diligently define and redefine the essential components of a successful security strategy; in addition, take the tactical actions necessary. The strategic planning is the function that has been neglected in the security organization due to operational commitments. The establishment of the Chief Security Officer (CSO) has been a remarkable improvement in providing both the strategic and operational focus.

Threats to the physical assets and the information assets identified as a result of a threat analysis should be categorized and a corresponding security goal defined for each category of threats. The set of security goals should be revised periodically to ensure its adequacy and conformance with the evolving organization environment. In addition to the four basic goals of security—confidentiality, integrity, availability, and nonrepudiation—a currently relevant set of security goals may include:

- Maintain a quality workforce
- Integrate technology tools
- Provide value-added services
- Offer specialized services

CONVERGENCE OF SECURITY

Convergence of security is defined as the integration of the management of logical security, information security, physical security, business continuity, disaster recovery, and health, safety, and environmental functions.

Logical security provides software safeguards for an organization, including user identification and password controls, access rights, and authorization levels. These measures ensure that only authorized users can perform actions or access information across a network or to use a workstation.

Information security is the discipline of protecting sensitive information from unauthorized access, improper use, disclosure, disruption, modification, examination, inspection, recording, or destruction. It is a term for protecting the data, regardless of the form of the data (e.g., electronic data or physical documents).

Physical security defines security measures that deny unauthorized access to facilities, equipment, and resources, and to protect personnel, property, and

other assets from damage or harm such as espionage, theft, natural hazards, or terrorist attacks.

Business continuity measures allow the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Disaster recovery involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Business continuity addresses the critical functions of the entire enterprise while **disaster recovery** concentrates on the information systems aspects.

Health, safety, and environmental (HSE) management has two goals:

- Prevention of incidents that result from abnormal operating conditions
- Reduction of adverse incidents that result from normal operating conditions

BENEFITS OF CONVERGENCE

There are many advantages to creating a converged security organization:

- A top-level security management strategy helps to align security objectives with high-level organization objectives.
- Managing an integrated security organization is less costly than managing a group of silos because there is duplication in overhead and other programs in a security organization that contains silos. Bringing together different security silos under one organization and running the combined organization can be a lot more efficient when one person has responsibility for all.
- Information sharing among disparate security functions improves.
- Convergence gives you a more versatile staff and saves the organization money with lower staffing costs, lower travel expenses, and reduced duplication of effort and fewer time-wasting turf battles.
- There are savings to be realized from technology convergence by replacing proprietary legacy systems with a centralized, IP-based security management system for both field offices and headquarters that encompasses CCTV, door controls, card access controls, intrusion sensors, alarm monitoring, and panic buttons. These types of systems have eliminated the need for local security guards at each portal; instead, fewer guards can monitor the system 24/7 from a central location and dispatch a response to any alarms.

DRAWBACKS AND CHALLENGES

When there is a significant change in an organization, there will be obstacles and drawbacks to the new change organization:

- Although experience has shown that restructuring of security functions is an ongoing process, many employees, both managers, and lower-level employees, will be unhappy with any change to their turf. They are not going to like whom they report to, whom they have to work with, and the new projects they are assigned. Egos will be bruised, if not battered. Change management principles will be essential to getting the group to work together.
- You must get the CEO and his/her advisors to approve and provide support for convergence proposals. If top management does not feel the same way about it as you do, your proposals will not be approved nor implemented. One way to get support for your initiatives is to demonstrate smaller scale successes first.
- Top management of the security function must report to a senior level of management within the organization. This structure is necessary since security impacts all areas of an organization and the security group must have the organizational authority and political leverage to enforce compliance with defined security policies, standards, and guidelines. A single consistent view of security for the entire organization is essential to the success of the security program.
- Cultural differences between personnel in different departments can cause difficulties when employees have conflicting feelings about security risks or have different views of what security devices and security practices should be implemented.

REQUIREMENTS FOR SUCCESS

Security Governance

As reported in an article in Inside Homeland Security, "For any security organization to be successful, there must be a framework established that guides organizations toward improving their security. This framework includes security governance which is the set of responsibilities and practices exercised by executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. Our research has shown that through their emerging capabilities in the area of security governance and risk management, many organizations are taking proactive steps to ensure their investments in security controls directly

support their objectives for the business. A consistent, organization-wide view of security risks integrating both physical security and IT security is an essential element of this strategy. By combining superior security governance and risk management with an integrated approach to logical and physical security, organizations gain an advantage for competing in the global economy with a distinct advantage through an optimized IT infrastructure and better protection for their digital, physical, and human assets."

Security Program

Successful organizations must create a robust security program. A security program is not merely a binder on a shelf; it is not a quick fix to the latest problem; it is not a collection of nice sounding words. A security program must be a living, ongoing process that is part of the fabric of the organization. A security program is a structure of individuals, processes, policies, standards, and procedures developed to protect an organization's assets, and ensure the organization adheres to all applicable laws and governing the actions. A security program implements a commitment to a new ethical way of conducting business and structure for helping employees to do the right thing which means it is about education, collaboration, and enforcement.

The framework is defined by policies, standards, and procedures. Security policies, standards, and procedures are used to translate the company's business philosophies into action by utilizing sound security principles and offer the following benefits:

- Well-designed security documentation is an invaluable communication tool for efficiently running operations within the security department and bridging the gap between relevant departments in the company.
- They improve decision making by having an authoritative source for guidance and for answering questions.
- They ensure compliance with national and local laws, regulatory agencies affecting business, government contracting authorities, independent certification organizations, and company standards of conduct to ensure respect for employee terminations and other administrative actions.
- They function as a quality-control process that improves operations.
- This program documentation provides the leadership, organizational structure, and processes that ensure the following for the organization:
  - Strategic direction is clear
  - Risks are managed
  - Business objectives are weighed with security risks
  - Organizational resources are used responsibly
  - Security program effectiveness is measured

THE ROLE OF THE CHIEF SECURITY OFFICER

The US Department of Homeland Security has defined critical industries as the following:

- Transportation
- Energy and Utilities
- Financial Services
- Media and Telecommunications
- Information Technology
- Healthcare

All remaining industries are classified as noncritical.

The terrorist strike of Sept. 11, 2001, caused almost every organization to evaluate their security. Most of them found that physical security and information security were not coordinating their efforts and had not developed a common strategy. They also concluded that there wasn't enough emphasis placed on security. With the convergence of the many functions involved in security as described above, many companies have considered establishing a single position to head up the different duties and assume responsibility for coordinating all the effort.

According to CSO Online, "the role of chief security officer (CSO) has exploded onto the corporate scene in North America and Europe in the last five years." Security has evolved into an essential, shared service within most organizations, and the head of security is also becoming a critical leadership position. The head of security has responsibilities not merely to Physical Security and IT, but to improving the operational efficiency of the business and implementing cost-effective risk management measures. For example, employees need to be identified at all times by wearing a photo ID credential that may serve as a timekeeping device, parking structure admission card, building and room access card, and a token to use along with a password for access to the computer system. Security can change facility access rights of employees depending on the threat level, by upgrading or downgrading data privileges immediately. Human Resources can process new employees and departing employees quickly granting and eliminating physical and data access rights in a single transaction. Another example is using a single corporate network to connect and run all the IT functions as well as connecting all the security devices such as card readers, CCTV cameras, and duress alarms. As a result, the organization achieves better security and incurs lower costs.

These types of bottom line improvements come most easily when companies treat security as a strategic business process, assigning a single individual to coordinate the various risk management functions of the organization.

DUTIES OF THE CSO

The CSO position is intended to be analogous to that of a Chief Financial Officer or Chief Information Officer. The CSO coordinates all security responsibilities throughout the organization and is accountable to top management and the governing board. With a single person accountable for security responsibilities, the many separate functions involved in security operations can be better coordinated, and information can be disseminated more efficiently throughout the corporation. The CSO concept hinges on the perceived need to integrate security concerns into corporate strategy. In theory, the position gives security issues a place at the table whenever high-level decisions are being made about the location of facilities; protection strategies for facilities and data; supply chain sources; choice of corporate partners; and procedures to ensure the safety of an organization's products and stakeholders. The CSO can concentrate on the "big picture," delegating routine oversight of physical security to managers at the operating level.

With regular access to the C-suite, the CSO will be better able to redirect organization policies quickly in response to an emergency or perceived threat. Finally, the CSO will control the security budget for the corporation as a whole so that security spending can be managed more efficiently.

As listed in WORK.CHRON.COM, "A CSO is the executive whose ultimate role is to ensure that an organization's security function adds value and gives it a competitive advantage. A major part of a CSO's role within an organization is to help forge strong and secure connections between departments. A CSO who can reduce friction between departments thus adds value to an organization.

They must identify organizational protection goals and objectives, ensuring they are consistent with their organizations' strategic plans. Part of a CSO's job is to work with other executives to decide on the priority of security needs and then spend according to an organization's financial constraints and directives. CSOs also oversee a network of security directors, managers, and staff and work with local, state, and federal law enforcement and other security agencies." We have attached a sample job description (Attachment 1).

QUALIFICATIONS OF THE CSO

Before the professionalism of the security manager to the CSO, those employed in the security department tended to be mature, retired people with military, police, or government law enforcement agency background. Many did not have education at the university level, experience in business,

or experience as a manager. For many it was a second career after retirement and they were not looking for a challenge.

Skills

- The CSO must be technically oriented, with a keen understanding of an organization's assets and systems.
- CSOs must have in-depth knowledge of risk assessment and vulnerability analysis techniques, how hackers and intruders might penetrate their defenses, and how to defend against attacks.
- CSOs must be organizationally skilled in carving out the security budget, in influencing other verticals within the organization, and in earning the trust of top executives.
- The CSO must understand how to detect, contain, and remediate any cyber-attacks and physical intrusions that do occur.
- The CSO must be a crisis manager, adept at handling the type of breach that spills onto the front pages of the newspaper, solving the problem while projecting calm, and keeping the public informed.
- The CSO must be able to inspire confidence when speaking to reporters and the public when an inevitable breach occurs.
- The exponential expansion of human knowledge, the growing demand for a broad range of complex and customized security systems, and the evolution of worldwide competitive markets for security products and services has driven the development of project management techniques in the security industry (Patterson, 2013). The CSO must be able to manage technical projects involving the implementation of sophisticated PPS.

THE BUSINESS CASE FOR SECURITY

Security has a traditional disadvantage of being viewed primarily as a cost rather than as a source of business value to an organization. Given that a direct link to the organization's revenue generation is at the root of much corporate decision making, the absence of any such link for security makes it a difficult sell to management. The notion of a "Triple Bottom Line," (a term coined by Elkington, 1997) reflecting economic, social, and environmental impacts, might one day benefit thinking about corporate security in the way that it now guides thinking in citizenship and sustainability. Security organizations can also achieve recognition from management for reducing losses.

One example that comes to mind is how the discipline of safety came to be a mainstream business concern. Today, safety is entrenched in any organization that aspires to best practice levels of performance management. If

security is going to arrive at a similar level of corporate operating recognition, then new ways of describing it may have to be formulated. In contrast, if there is no solution to this language barrier, it becomes much harder to buy the "business case" for security as a value-adding activity. Thus, the language of security and the perception of its value are interconnected. Whatever the ultimate approach may be, security executives agree with peers in other areas of business that defining the business case for security is the key factor in making security a higher priority for corporate managements. Articulating the business case requires a thorough appreciation of the relevance of security to corporate reputation and business opportunities.

Determining the "return" on security investments also requires a framework to measure the value added to the organization through such investments. At present, security managers find it difficult to analyze security spending in these terms. They lack the tools and staff resources to perform such an analysis. It is true that at least insurance is one area in which security spending yields tangible financial results; many insurers will reduce premiums if an organization can demonstrate that it has instituted procedures and implemented security systems that lower risk exposure. However, there is a lack of tools, metrics, or staff resources to measure other aspects of security investment in an equally straightforward manner. Ultimately, the value of security spending will be demonstrated to the extent that it becomes a proactive management tool, and not merely a reaction to incidents or disasters. Some security managers tend to think of their jobs in terms of responding rather than initiating. There is a common sentiment that security's access to the "C-suite" was inadequate to these times and that a change of mindset would be a prerequisite to enhancing the priority accorded to security in corporate operations. We recommend organizations formally define a framework such as that shown in Fig. 1.1 using the following definitions:

- Security Vision and Strategy—A formal statement of the purpose of the Security function. The security organization's goals include developing a comprehensive security vision and the development of a security strategy document that aligns the organization's security activities with business objectives and communicates this strategy throughout the organization.
- Senior Management Commitment—Senior management supports security efforts through policy, directives, and resource allocation. The security organization's goals include the development of policies, procedures, and standards that clearly define the business need for security services to be integrated throughout the business areas of the organization.
- Security Management Structure—Roles, responsibilities, and organizational groupings assigned for security functions and activities.

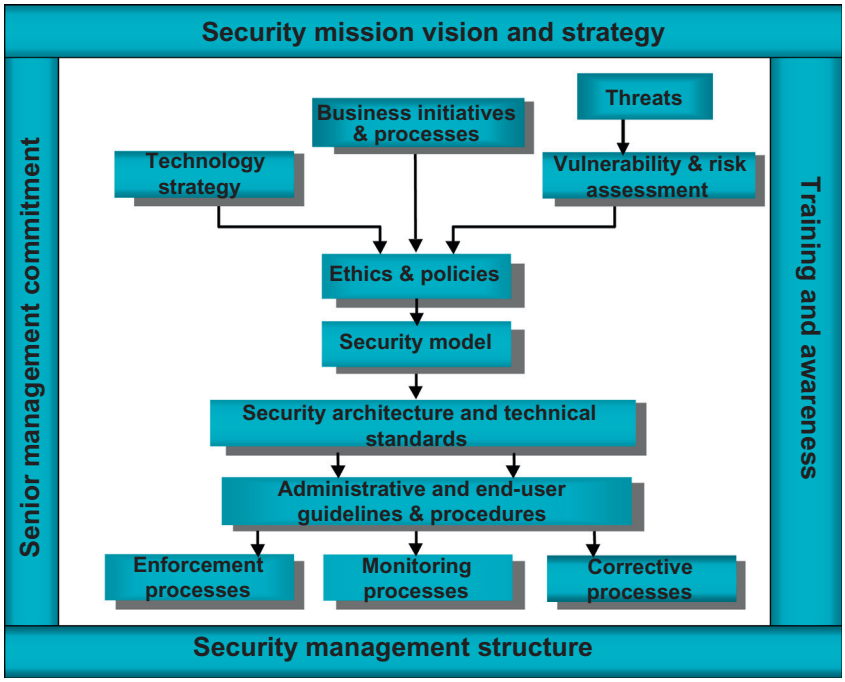


FIGURE 1.1
Security framework.

The security organization's goals include eventually developing an enterprise-wide centralized security management function that is built to ensure the security and protection of the organization's assets.

- Training and Awareness Program—Ongoing security education program for all employees. The security organization's goal is to develop and disseminate a global training and awareness program that makes everyone within the organization aware of their individual responsibilities concerning assets protection and security.
- Technology Strategy and Usage—A linkage should exist between the types of security technology being implemented throughout the organization and the security solutions and processes in place to protect assets. The security organization's goal is to be a team member of the various technology planning, architecture, and steering committees within the organization and work to ensure that security services are clearly defined, understood, and available as required.
- Business Initiatives and Processes—A linkage should exist between the business strategies and directions being pursued by the organization and the security solutions and processes in place to protect the

information assets of the organization. The security organization's goal is to understand the key business drivers that are occurring within the organization and help to design and build security solutions that complement these initiatives.

- Threat, Vulnerability, and Risk Assessments—Identification of threats, vulnerabilities, and risks facing the organization is a vital part of the security framework. The security organization's goal is to participate in identifying those threats and vulnerabilities that affect the organization and work to build risk mitigation strategies.
- Policy—Written statements of management's expectations for the protection of the organization. The security organization's goal is to ensure that the policies are complete and up-to-date while researching new security areas that may eventually impact the organization.
- Security Model—Asset ownership and classification processes designed to structure organize and focus security efforts. The security organization's goal is to work with asset owners and knowledge management resources to ensure that an adequate asset ownership and classification scheme is defined, and corresponding processes and systems are developed.
- Security Architecture—A document that maps security needs, business initiatives, business drivers, and regulatory requirements for security solutions, security practices, and security policies of the enterprise or a particular economic cycle.
- Technical Standards—Specific office types and technology-specific control standards implemented to achieve security policy objectives. The security organization's goal is to work with the various office managers and to review and develop appropriate security standards.
- Administrative and End-User Guidelines and Procedures—Day-to-day, operational procedures for implementing security policies and standards. The security organization's goal is to work with the various office managers and review and develop appropriate technical administrative and end-user security procedures.
- Enforcement Processes—Processes, procedures, or activities designed to ensure security policies and standards are implemented. The security organization's goal is to work with the office managers to put into place appropriate enforcement processes and systems.
- Monitoring Processes—Processes, procedures, or activities designed to detect conditions of noncompliance with security policies and standards. The security organization's goal is to work with the office managers to put into place appropriate monitoring processes and systems.
- Recovery Processes—Processes, procedures, or activities designed to recover facilities back to normal operations. The security organization's

goal is to work with the office managers to put into place appropriate recovery processes and systems that protect assets during the recovery process.

CONCLUSION

Advances in technology have benefited the world in many ways, but unfortunately, there is a portentous side; technology can be used against us. Hackers can activate baby monitors to spy on families; thieves are analyzing social media posts to plot home invasions; criminals can control security cameras to determine when homes or businesses are vulnerable, and stalkers are exploiting the GPS on smartphones to track their victims' every move. We all know today's criminals can steal identities, drain online bank accounts, and even attack our national infrastructure. The security organization of the future is evolving, and the CSO is a core part of making the transition to being an essential component of the business. The answer to making the organization successful is to embed security into the business fabric So if an organization's task is "selling shoes online," it is the CSO's job to convince the organization that the task is now "selling shoes online securely" and to get the organization moving quickly in that direction.

ATTACHMENT 1 JOB DESCRIPTION OF THE CHIEF SECURITY OFFICER

The following job description of the CSO is from SecurityDreamer, https://securitydreamer.wordpress.com/2007/03/15/job_description/ (accessed February 17, 2016).

Overview

The CSO is the leader of the corporate/physical security function to include responsibility for overall corporate security strategy, security architecture development, and global functional oversight. The scope of this role covers all utilized security technologies and services, including protection services, perimeter defenses, physical and logical access control, and profile management of all employees, contractors and visitors. As the organization's senior security officer, this person also has enterprise-level responsibility for all data/information security policies, standards, evaluations, roles, and corporate awareness.

This person will work with user and technical groups and Internal Auditors in the development and implementation of a security strategy designed to provide a high level of security over physical facilities and data processing while preserving and enhancing facility and system usability. This person must be able to develop and implement flexible security solutions, dictated by the needs of a hybrid and rapidly evolving decentralized business environment. The individual must be a results-oriented person who can achieve tangible improvements in the corporate security arena. Excellent technical and communications skills are a must, as well as proven security leadership experience.

(*Continued*)

(Continued)

Role and Function

The CSO will be responsible for directing the activities of the security function. Responsibilities will include:

- Work closely with corporate executives, business managers, audit and legal counsel to understand corporate requirements related to security and regulatory compliance, and to map those requirements to current security projects.
- Develop, implement, and manage the overall enterprise process for security strategy and associated architecture and engineering standards.
- Develop and implement policies, standards and guidelines related to corporate security.
- Oversee the continuous monitoring and protection of facilities, personnel and information systems.
- Evaluate suspected security breaches and recommend corrective actions (including incidents involving outside vendors).
- Serve as the enterprise focal point for security incident response planning and execution.
- Define and implement an ongoing Risk Assessment program, which will define, identify and classify critical assets, assess threats and vulnerabilities regarding those assets, and implement safeguard recommendations.
- Assist Internal Audits in the development of appropriate criteria needed to assess the level of new/existing applications and/or technology infrastructure elements for compliance with enterprise security standards.
- Establish and monitor formal certification programs regarding enterprise security standards relating to the planned acquisition and/or procurement of new applications or technologies.
- Assist in the review of applications and/or technology environments during the development or acquisitions process to (1) assure compliance with corporate security policies and directions and (2) assist in the overall integration process regarding organization's own technology environment.
- Oversee the development of, and be the enterprise champion of, a corporate security awareness and training program.
- Manage security functions related to corporate information systems or data centers, working closely with the information security team.
- Evaluate changes to the corporate environment for security impact and present findings to management.

Reporting

- The Chief Information Security Officer will initially report directly to the Chief Operating Officer and will serve on the Executive Planning Council.
- The CSO will have direct reports including an administrative assistant, the manager of security architecture and engineering, and various other staff.
- The CSO will have dotted line reports including the VP of Information Security, The VP of Internal Audit.

Qualifications/Experience

The candidate will have

- A college degree (BA/BS)
- Excellent staff management skills
- Ability to interface with top management
- Eight to ten years of management experience at least five of which were in a security-related area in a leadership capacity
- Certifications as Certified Protection Professional (CPP)
- Certified Information Systems Security Professional

(*Continued*)

(Continued)

Other desired qualities include:

- Consensus-builder, while still results-oriented and commitment focused
- Network-based security experience
- Business-based attitude, i.e., the recognition that no policies can be implemented w/o demonstrable business benefit
- Customer service experience
- Awareness of and strong experience in:
- Vulnerability testing in addition to penetration testing
- Developing security practices as a people problem vs a technical problem
- Standards-based architecture with an understanding of how to get there, including compliance monitoring and enforceability

References

ASIS Saint-Blanquat, H., 1986. The First Settlements. Trans. A. Ridett. Silver Burdett, Morristown, NJ.

Dalton, D.R., 2003. Rethinking Corporate Security in the Post 9/11 Era. Butterworth Heinemann, New York.

Elkington, J., 1997. Cannibals with Forks: The Triple Bottom Line of Twenty-First Century Business. Capstone, Oxford.

Greer, W., 1979. A History of Alarm Security. National Burglar & Fire Alarm Association, Washington, DC.

Grosvenor, E.S., 1997. Alexander Graham Bell. The Life and Time of the Man Who Invented the Telephone. Harry Abrams, New York.

Holmes, E., 1990. A Wonderful Fifty Years. Holmes Protection, New York. (Originally Published 1917.)

Kovacich, G.L., Halibozek, E.P., 2003. The Managers Handbook for Corporate Security. Butterworth Heinemann, United States.

Mahoney, R.W., 1995. Diebold, Incorporated: From Safes to Software. Newcomen Society of the United States, New York.

Parker, D.D., 1976. Crime by Computer. Scribners, New York.

Patterson, D.G., 2013. Implementing Physical Protection Systems—A Practical Guide. ASIS International Improving Security Awareness-Inside Homeland Security-IHS, Washington, D.C, http://www.abchs.com/ihs/SPRING2013/ihs_articles_1.php (accessed February 22, 2016).

Schell, B.H., 2004. Cybercrime: A Reference Handbook. CA: ABC-CLIO, Santa Barbara.

"Triple Bottom Line". The Economist. November 17, 2009.

Further Reading

Gill, M., 2006. The Handbook of Security. Palgrave Macmillan, London.

Thomas E. Cavanagh. (2004) *Corporate Security Measures and Practices—An Overview of Security Management Since 9/11*.

WEB SOURCES

http://www.scmagazine.com/a-brief-history-of-internet-security//article/149611/

The Need for a Chief Security Officer (CSO) has arrived, http://www.csoonline.com/article/2113130/data-protection/the-need-for-a-chief-se (accessed February 17, 2016).

Roles & amp; Responsibilities of a Chief Security Officer | Chron. com, http://work.chron.com/roles-responsibilities-chief-security-officer-19479.html (accessed February 17, 2016).

Job Description of the Chief Security Officer | SecurityDreamer, https://securitydreamer.wordpress.com/2007/03/15/job_description/ (accessed February 17, 2016).

CHAPTER 2

Organizing

What You Will Learn

- How to recruit, evaluate, select, and hire job candidates.
- How to organize the work activities of security department employees.
- How to determine work tasks, assign them, provide resources to the people being tasked, and monitor their performance.
- How to terminate an employee.
- Understand the nature and purposes of organizational structures.

INTRODUCTION

In this chapter, we will discuss the role of the Chief Security Officer (CSO) in determining knowledge and skill requirements for a security position, and when the position is vacant, the tasks of the CSO in recruiting, selecting, and hiring a replacement. We will examine setting objectives for individual employees and for the security organization as a whole, and monitoring performance. Termination of employment is the outcome when an employee's performance does not meet established job standards, and during the termination interview the CSO should expect to encounter a range of emotional reactions. Finally, we will look at types of organizational structures and how they influence the organization's work processes, particularly as they relate to security operations.

STAFFING

The hiring process in a mature organization is almost always under the exclusive ownership of the human resources (HR) group. Hiring tends to be more formal than flexible and moves through stages arranged and monitored by HR staff. (Note: Here, we are not discussing the hiring process for security guards employed under contract. The CSO can specify in the contract that certain preemployment standards must be met for guards assigned to the

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00002-5

contract, but the CSO has no direct part to play in hiring the guards.) Although HR controls the hiring process, many administrative tasks must be performed by the CSO. The sections that follow describe how the process works.

Justify the Position

A position opening occurs when a new position is created or when a job incumbent leaves an existing position. The principal duties of the Chief Investigator are presented in a series of statements such as the following:

- Conduct investigations of felony crimes committed against the company, and workplace violations involving theft, drug trafficking and abuse, assault, harassment, and other matters selected by the CSO.
- Collect physical evidence.
- Interview witnesses and suspects.
- Prepare investigative reports.
- Testify at administrative and legal proceedings.
- Coordinate with legal entities concerning restitution.
- Advise the CSO on weaknesses in the organization that contribute to crime and/or violations of workplace rules.
- Establish and maintain working relationships with industry peers and persons in the criminal justice system.

The job description states where the job fits into the organization's formal hierarchy; that is, the position to which the incumbent reports, the positions that report to the incumbent, and the positions that are equivalent to the incumbent. For example, a job description may state that the Chief Investigator in the corporate security group reports to the CSO, supervises two investigators, and is at the same organizational level as the Chief of Physical Security in the corporate security group. The grade level of the job, spending authority, and size of budget commanded are specified in the job description. For example, the description might state that the incumbent is at grade level 9, can spend up to $1000 without prior approval, and manages the investigation office's annual budget of $250,000. The required experience, education, and training are stated. For example, the American Society for Industrial Security (International) awards three certificates: Certified Protection Professional, Physical Security Specialist, and Certified Professional Investigator. The first certificate recognizes competence in security management generally; the second recognizes technical abilities in identifying and correcting physical security weaknesses related to a protected asset; and the third recognizes competence in conducting investigations in the corporate sector.

In the information security field is the certified information systems security professional (CISSP). This certification is governed by the International Information Systems Security Certifications Consortium and is universally recognized as a key component in the selection process for management-level information security positions. The Cisco Certified Security Professional is an advanced-level certification for information technology (IT) professionals who are actively involved in developing business solutions and designing and delivering multiple levels of security departments.

Here is an example of a statement for a full-time corporate investigator: "The job incumbent must have worked in a responsible investigative position for at least 5 years and possess at least a baccalaureate degree, preferably in business management, accounting, criminal justice, or similar major area of study. The Certified Professional Investigator certification is desirable but not mandatory."

When the vacant position is an already-established position, the CSO updates the existing job description. In the main, we are talking here about a full-time employee position in a security department. However, the same principles apply when hiring a part-timer to fill in for a full-time employee called away from the job; a permanent contract employee such as an investigator in the direct employ of Pinkerton's or other private security firm; an independent consultant or private investigator with a skill not present in the security department and who may be needed to work on a large and complicated investigation; an investigator working as a team member on a project that has a beginning and ending date; or an investigator directly employed by an outsourced company that has completely or partly taken over security department functions. In all cases, the CSO prepares the job description.

Identify Relevant Skills and Knowledge

A thoughtful examination of a job's tasks will reveal the skills and knowledge that must be applied by the incumbent to operate at the desired level of performance. If the incumbent's job includes conducting investigations of felony crimes, he/she must be skilled at collecting evidence, interviewing witnesses and suspects, writing reports, and testifying at judicial proceedings. These particular skills require, among others, knowledge of forensic sciences, criminal psychology, rules of writing, and criminal trial procedures.

If the task is to network with peers in security and law enforcement, a relevant skill is verbal communication. The supporting knowledge includes understanding the structure and workings of the criminal justice system. Unfortunately, and damaging to the hiring process, it only rarely happens

that a job description will define skill and knowledge requirements to the level of specificity needed to search for and sift through qualified candidates.

Search for Qualified Candidates

Several avenues of search are available to: the CSO and HR staff, headhunters, and advertisements placed in newspapers such as the Wall Street Journal. Notices placed in and found in security profession newsletters and similar publications and networking databases, plus websites such as the company's Internet and Intranet, Craig's List and Monster. Also, tweetering may produce results. Finally, and most importantly, are word-of-mouth searches.

The nature of a search is dependent on the nature of the job: low-end jobs are advertised in low-end publications such as ordinary newspapers, security profession newsletters, and the Internet. High-end job openings are placed in business-oriented newspapers, and with headhunters.

Choosing a search avenue is not nearly as complicated as traveling the avenue. Complications arise in the way the job and the qualifications of the candidate are described. Help-wanted ads that contain descriptors such as "Ivy League type" or "energetic individual" imply discrimination on the basis of class and age. Sex-biased descriptors include "Gal Friday" and "salesman." Other discriminatory references might be "former military officer" or "retiree."

Legal challenge can be avoided by explicitly describing the required job skills and knowledge. Jacob says a security investigator, for example, writes reports, testifies, and respects Constitutional rights. The appropriate descriptors could be "capable writer," "good verbal communicator," and "knowledge of state and Constitutional law."

Compare Candidates against Job Requirements

This stage in hiring is not as simple as it sounds. Valid comparisons rely on having two sets of data that can be matched one against the other. The data sets are well-defined job requirements and clear evidence of qualifications that correspond to the requirements. The matching process becomes unworkable when one data set is apples and the other is oranges, and complicated when minor job requirements are included. The idea is to make the data sets fit nicely with each other and to not bother with lesser job requirements. An example of a good match between a key job requirement and a clear qualification is the statement "The candidate's knowledge of criminal investigative methods can be demonstrated by presentation of a transcript or certficate showing completion of a course in criminal investigation. An example of

such a certificate would be the Certified Professional Investigator certificate awarded by the American Society of Industrial Security (International)."

A commonly used method, but not the only method, is administering a job-related test, the answers to which can reveal the candidate's weak and strong attributes. A test of this type is usually administered after the candidate is determined to be one of the best candidates.

Interview the Candidates

Candidate interviews are a minefield to be treaded carefully. The mines to look for are discrimination for age, gender, sexual orientation, religion, political perspective, disability, national origin, ethnicity, pregnancy, race and color, prior convictions (but not arrests), and retaliation that may be based on information uncovered up to that point in the selection process. Mistakes in any of these areas can lead to a complaint filed with the US Equal Employment Commission, and failing a satisfactory resolution through the Commission, the claimant is free to file a civil suit.

It helps to use a script that avoids the mines and concentrates on the candidate's competency in respect to job standards. Every question posed to a candidate during the job interview must be the same question posed to all candidates. The taking of accurate notes is essential.

In a mature organization, three interviews done in sequence are common. The first is usually by the HR representative who is working with the CSO. The second interview is technical in nature and done by the CSO or the person that will directly supervise the hired candidate. The third is an interview by the person holding hiring authority. In some cases, the hiring authority for the security department is held by the CSO.

Identify the Apparent Best Candidate

At this point, the search has been narrowed considerably. The applicants still in the running are on what is called the "short list." The one or two candidates that look best for the job are moved to the top of the list. This is not the moment to tell the top candidate that he/she appears to be the winner. It is a decision-making moment to be shared by a select few, such as the CSO, the incumbent's direct supervisor, and the HR representative assisting in the selection. The next step is to ensure that the best candidate has honestly presented the facts.

Conduct a Background Inquiry

Time and expense are involved in the process of verifying a candidate's credentials. Instead of conducting background checks on all candidates prior to or immediately following job interviews, it is sensible and cost-conscious to wait until the list of candidates is down to one or two and then begin the process of validating representations that were made in writing on an employment application and verbally during the job interview. In smaller companies or companies that feel they get better results from an outside agency, such as a private detective agency, will place the background inquiry in the hands of the outside agency. A background inquiry is said to be confirmatory when the employer seeks only to confirm that the job candidate has been truthful in providing information. The confirmatory inquiry is almost always limited to information provided by the candidate. Of special interest are previous employment, education and training, and criminal history.

A background inquiry is said to be investigative when the employer looks for information that a candidate may be concealing such as information relating to a cause for termination from a previous job or the commission of a serious crime. King points out that an investigative background inquiry will often be initiated when a confirmatory inquiry reveals possible deception by the candidate.

Test the Apparent Best Candidate

Alcohol and drug testing are common procedures for evaluating a candidate for a security job, or for that matter any job that involves protection of human life or sensitive assets such as nuclear material and secret information. The negative effects of alcohol and drugs on human performance in the workplace are widely known. They include lost productivity, absenteeism, high accident rates and medical costs, theft, and violence.

Human behavior can be assessed also through psychological testing. Test content may be directed to almost any facet of intellectual or emotional functioning. Among the aspects of greatest concern to a CSO are honesty, propensity for violence, personal traits, values, and attitude. Test results are obtained by comparing the individual's responses against standard responses, with the standard responses having been developed previously by commonly accepted scientific methods. A test score can predict an individual's behavior in a narrowly defined set of circumstances, and is said to have predictive validity when it yields consistent, reliable measurements. For example, an honesty test has predictive validity if persons who score high are later shown by their behaviors to be honest. When accurate in

predicting a job applicant's future behavior, psychological tests can be valuable hiring tools.

Proficiency tests can be used to select job candidates and to determine their suitability for particular jobs. Aptitude tests predict future performance in a job for which the individual is not currently trained. If a person's score is similar to scores of others already working in a given job, likelihood of success in that job is predicted. Some aptitude tests cover a broad range of skills pertinent to many different occupations. The General Aptitude Test Battery is an example. It not only measures general reasoning ability but includes measures of perception, motor coordination, and finger and manual dexterity.

Intelligence tests measure the global capacity of an individual to cope with the environment. Test scores are generally known as intelligence quotients. Objective personality tests measure social and emotional adjustment. Responses that briefly describe feelings, attitudes, and behaviors provide a profile of the personality as a whole. The most popular of these tests are the Minnesota Multiphasic Inventory and the California Psychological Inventory.

One cannot discuss preemployment testing without reference to their critics. The major criticisms stem from two interrelated issues. The first is technical shortcomings in test design. Because technical weakness to some degree is inescapably present in all forms of preemployment testing, the sharpest of critics demand that such testing not be used at all. The mainstream view is that test results represent only one piece of information about an individual, and as such should not be used as the sole criterion for selection or rejection.

The second criticism deals with interpretation and application of results. Opponents argue that testing can under- and overvalue job candidates, and employers who use testing often place an inappropriate reliance on tests. These arguments have been particularly loud in the case of intelligence testing. Psychologists generally agree that using intelligence tests to bar individuals from job opportunities, without careful consideration of other relevant factors, is unethical. Critics have taken their views to the courtroom. A chief argument is that certain tests emphasize skills associated with white, middle-class functioning, resulting in discrimination against disadvantaged and minority groups.

Offer the Job

At this point, the final stage of the hiring process, the job is offered. If accepted, the new hire may be required to sign a confidentiality agreement.

In the following anecdote, the new hire is a security group employee. The CSO will likely require the new hire to undergo an orientation that identifies prohibited behaviors, penalties for violations, and the methods used to assess and enforce compliance with rules. It is at this point that the Federal Trade Commission, acting under the authority of the Fair Credit and Reporting Act (FCRA), comes into the picture (see Chapter 14: Preemployment Screening for the full text of the FCRA).

CRITICAL THINKING EXERCISE

Larry's search for a security group investigator narrowed to two candidates: Cynthia Castillo and Brendan Murphy. Details in the job applications for both candidates had been verified. Cynthia had a degree in business management and seven years of work experience as a credit card fraud investigator. Brendan had a degree in criminal justice and 22 years as an agent in the Bureau of Alcohol, Tobacco and Firearms. Although Larry was careful in final job interviews to ask each candidate the same set of questions, the conversation tended to stray. With Brendan, for example, the matter of his age came up, as did his Irish descent and Catholic upbringing. Cynthia mentioned that she had a child by a previous marriage and was engaged.

Larry selected Cynthia. He was sold on her education, her prior work experience, and her enthusiasm. A month later, Larry was informed that Brendan had filed a discrimination complaint. Brendan alleged that he had been denied the position because of responses he made to questions that were illegal to ask. He also alleged that Cynthia had been preferred over him because she was female and Hispanic.

INDEPENDENT CONTRACTORS AND CONSULTANTS

Independent contractors and consultants typically work for more than one client, operate out of their own offices, set their own hours, and work according to their own methodologies. The contractor is generally engaged to work for several months such as to repair or replace an entire IT system. The consultant is engaged for a shorter period of time, perhaps days or a week, and would be a choice to evaluate an ongoing or completed project such as the one just mentioned.

Unlike regular employees, consultants are not entitled to overtime, vacation pay, and time off to deal with family and medical emergencies. Consultants may or may not be accorded protections against discrimination based on race, gender, religion, disability, or age. The legal obligations of a client to a consultant are not nearly as demanding as those that apply to regular employees. CSOs employ consultants when:

- The work to be performed requires technical expertise not available in the security group or not readily available in the larger organization.

An example is the use of a so-called "tiger team" to conduct computer penetration tests.
- The need for the work is occasional or periodic. For example, a risk management consultant may be hired once per year when annual security audits are conducted.
- The cost of the consultant is less than the cost of performing the work in-house.
- Contingencies arise that make it impossible or difficult for the security group to effectively carry out its mission. The CSO, for example, may engage the services of freelance investigators to augment security group staff during a major investigation.

ORGANIZE ACTIVITIES

In the routine course of business, the CSO engages in a variety of practices loosely called organizing. According to Rorty, these practices include:

- Establish job positions
- Hire people to fill the jobs
- Assign work
- Delegate responsibilities
- Acquire materials and tools
- Manage time
- Counsel and guide employees the organizing activities of the CSO reflect the business processes of the company.

A manufacturing company will work differently than a company in lending, banking, retailing, or mining, as will a government agency in educating, regulating, or enforcing. The CSO will of necessity operate in harmony with the processes of the company no matter what they are. Although the CSO might incorporate practices found reliable through personal knowledge and experience, the overriding imperative is to meld group operations with the needs of the larger organization. For this to succeed, the security group must operate in harmony with itself and with other groups. The CSO understands that security operations are but one part of a large and complex mosaic.

ESTABLISH OBJECTIVES

The organizing function operates at two levels: group and individual.

Group Objectives

Group objectives are subparts of the organization's goal. If the goal is to be a profitable competitor in the mining of silver, one of the objectives of the security group will be to prevent theft of silver extracted from ore. Group objectives, then, are consistent with the needs and nature of the company's business. The fulfillment of group objectives is a major consideration when senior management rates the CSO's performance.

Individual Objectives

The objectives of individuals working in the security group are employee performance targets that are set annually, monitored periodically throughout the year, and evaluated impartially at the end of the year. The targets are sometimes negotiated between the CSO and the subordinate. Once agreed upon or set, performance begins or continues from the previous target period. From time to time, such as monthly or quarterly, the CSO and subordinate meet to discuss progress.

Individual objectives fall under group objectives. They are extensions of the major tasks, duties, and functions defined in an individual's job description. These objectives state what the individual is expected to do in his/her job and establish measurable criteria as to volume and quality. Imagine that it's the duty of the security group's physical security specialist to conduct security vulnerability assessments of the company's six manufacturing plants. The CSO establishes an objective for this duty: perform one security vulnerability assessment every quarter of the calendar year and produce from each assessment a written report that meets established criteria for content, format, and readability.

The outcomes of group and individual objectives are often measured with a yardstick called "value derived versus cost," a fancy name for a concept that poses a simple question: Was the delivered service worth the expenditure? Organizing by objectives allows answers that are rational and impersonal.

ORGANIZE CONSISTENT WITH POLICIES

The company's statements of missions and goals are found in its policy or policy set, and security is one of the matters addressed. A company's management may choose to express its security philosophy in an overarching policy that addresses a range of issues such as preemployment screening, substance abuse, and workplace violence. In addition or alternatively, the company may choose to create a number of standalone policies, each covering a fairly discrete issue such as preemployment screening only. In the latter arrangement, the security group would likely own a policy of its own and share ownership in other policies. In whatever form, the ideal security policy is

endorsed by management at the highest level and understood by all parties affected by it.

The point here is that security policy carries with it commitments that must be met. If the policy pledges to obey laws, respect the rights of people, and establish a safe work setting, the CSO must ensure that the manner of protecting company assets must not violate the law, must not violate anyone's rights, and must not create safety risks.

Provide Physical Resources

Ideally, resources are determined by objectives but the reality is that objectives conform to resources. A security group objective can make perfect sense, but if the resources are not available it makes no sense at all. It is accurate to say that resources entrusted to the CSO derive from the dictates of senior management. If the chief executive officer (CEO) issues a policy that requires the security group to prevent unauthorized entry to a manufacturing plant, funding must be made available to meet the policy's requirement. The CSO may judge that fencing, lighting, and access control equipment will need to be installed and more guards hired. The plant superintendent, however, may disagree with the CSO's thinking. He may say, "A fence and guards checking passes will slow people down when they come to work. Plant productivity will drop. I don't like it." The financial officer at the plant may say, "Since we're providing the funds for this project, we think we can get by without access control equipment and with three new guards instead of five." If the CSO cannot negotiate a level of funding adequate to meet the policy requirement, he/she may have to appeal to the CEO and in the process alienate the plant superintendent and financial officer.

It may not matter what the CEO or executive management want to do. Occupational Safety and Health Administration, Environmental Protection Agency, internal and external auditors, Homeland Security, and other regulatory bodies may require, limit or proscribe certain features. For example, Homeland Security may require that perimeter fencing be stronger and higher than normal, certain sensors be removed and replaced by enhanced sensors, and a closed circuit television system be installed.

Perception is also a determinant in the allocation of resources. When senior management perceives that the CSO and the security group are effective at what they do, there is a greater chance that security operations will be adequately funded. This is a fickle reality because the perceptions of senior managers are based on "snapshot" views of security: "The guard at the main entrance was alert and smiled as I drove by," or "The moron at the security desk didn't even know my name." Sadly, resource allocations can be based on such perceptions.

Provide People Resources

The resource most important to the CSO is competent people. A security group can have a state-of-the-art assemblage of equipment and a full complement of personnel yet be incapable of meeting group objectives when human competence is lacking. Competence is a mix of knowledge, skill, and attitude. The first two can be taught and learned without much difficulty. The last of the mix, attitude, can be taught but for some people not easily learned. Consider the following scenario.

CRITICAL THINKING EXERCISE

A motorist driving on a lonely country road sees ahead of him a red octagonal sign bearing in the center large white letters that spell STOP. The driver understands that motor vehicle law requires motorists to come to a complete and full stop at the intersection where the sign is posted. The driver has just demonstrated knowledge. The driver removes his foot from the accelerator, applies the brakes, and maintains steering. The driver has just demonstrated a skill. The driver notices that the intersection ahead of him is clear. There's no other vehicle in sight. The driver proceeds through the intersection without stopping. The driver has just demonstrated an attitude. A CSO's efforts to organize the security group can be successful when the group possesses and applies a correct mix of knowledge and skill, accompanied by a positive attitude.

ORGANIZE BEYOND BOUNDARIES

The security group supports and works in concert with other company groups. Although it can serve important support functions, it cannot do everything related to security. For protection to prevail, every employee must pull his/her own weight: the executive secretary locks the safe before going home, the scientist removes data maps from the conference room wall, the janitor locks doors, the Chief of Operations (COO) does not discuss sensitive matters over the telephone. The catalyst is the CSO.

Some employees hold more responsibilities than others. This is especially true of employees in line management. Company assets, such as vehicles and desktop equipment, are signed out to managers and supervisors. Even though a group's assets are in the custody of subordinates, the group leader is responsible for their care. The responsibility is often spelled out in a policy statement such as the following.

"Managers and supervisors at all levels are responsible for protecting the assets entrusted to them, ensuring that subordinates do likewise, and meeting security standards and practices necessary to maintaining a secure, safe, and productive work environment for our employees, guests, and the customers we serve. The matter of assets protection will be an element in the annual

evaluation of managers and supervisors and may be a factor in determining individual pay raises, bonuses, and promotions."

A policy statement that links security responsibilities with pay and advancement can be a powerful motivating tool. Because few managers and supervisors have a firm understanding of protective measures, they must turn to the CSO for guidance. It is in this regard that the CSO plays an organizing role outside the boundaries of the security group.

The CSO is expected to create a "culture of security" or a "culture of vigilance." Examples of such cultures in action might include employees asking strangers the nature of their presence in a protected facility, alerting security of suspicious strangers in the parking lot or circling the building, questioning why a truck is parked close to the building in violation of security, reporting that a coworker has a lethal weapon in the workplace, or informing a supervisor when a coworker's behavior suggests an early stage of violence.

The CSO does not provide security but rather helps others discharge their security responsibilities by offering expert counsel. Counsel can take many forms: face-to-face discussions, presentations at line management meetings, alerts and advisories by e-mail, and memoranda. The arrangement can work very well, provided the CSO is not stretched thin. This can happen when the company is very large, operates in many geographical areas, and works in partnership with other organizations.

Assign Tasks

The total work in a security group is the sum of all tasks. A single task can be thought of as a combination of elements: a physical or mental action (e.g., directing vehicle traffic), the place of action (e.g., the exit gate from the company's parking lot), conditions affecting the action (e.g., inclement weather), and equipment needed to perform the action (e.g., a traffic vest, traffic baton, and rain slicker). Tasks in written form are seen in many venues.

Two other elements are highly determinative of task performance. First is the importance or criticality of the task. Some tasks have greater impact and consequences than do others. The task of directing traffic is less critical than the task of preventing unauthorized entry. A second determinant of performance is the training that precedes and facilitates task execution.

Tasks are arranged in groups according to jobs. The security officer holding the job called console operator will perform a set of tasks unlike the set of tasks performed by a gate guard.

Monitor Performance

Inside the CSO's organizing tool kit is a practice called monitoring. The following are examples of monitoring:

- Looking at tasks as they are being performed to detect mistakes, small and large, that can lead to problems
- Examining the output of task performance such as general correspondence and incident reports
- Visiting guard posts
- Observing tests of fire detection and suppression equipment, backup power supplies, and other equipment kept in readiness for emergency responses

Many will liken the process to "management by walking around," whereas a few may call it "making a nuisance of one's self." Whatever the label, monitoring is an indispensable part of organizing. Monitoring in the sense used here is essentially inward (i.e., it is focused on security operations). Monitoring that is focused on operations outside the security group is discussed later, particularly in the chapter dealing with risk management. The following anecdote makes the point that routine monitoring can identify the need for change.

CRITICAL THINKING EXERCISE

The CSO for a minerals extraction company made it a point to monitor daily reports of security incidents. He noted an upward trend in the number of incidents that appeared to be drug related. He visited the HR director and the company's head physician. The HR director pointed out that the company had a workplace rule that prohibited use of illegal drugs on company property. The CSO pointed out that the rule had no teeth because without drug testing there was no way to determine if a given incident resulted from a violation of the no-drug-use rule. The physician suggested starting a random drug testing program, with testing by a certified lab using the urinalysis method. Agreement was reached and approval given by the CEO. On the first day of urine collection, the CSO appeared at the collection site to monitor how things were going. He observed a worker in line who appeared to be intoxicated. The CSO confronted the worker, and after smelling alcohol on his breath asked him if he had been drinking. The worker affirmed that he had been drinking and admitted he was under the influence, and then said, "But I'm here for a drug test. I don't do drugs. I only do whiskey." The CSO sent a report to the CEO, with copies to the HR director and the head physician. The CEO ordered that the new random testing program be changed to include testing for alcohol as well as drugs.

TERMINATE UNACCEPTABLE EMPLOYEES

For two reasons the CSO needs to be knowledgeable about termination interviews. First is the need personally to inform a subordinate that his or

her services are no longer desired. Second, the CSO is often asked to be present when trouble is expected at a termination interview of someone else's subordinate.

The sagacity of Solomon is required to anticipate the range of potential reactions in a termination interview. Certain typical responses, however, can be expected. These include stunned reaction, psychological trauma, sorrow, and belligerence.

Stunned Reaction

In this case, the termination notice is received as almost good news, the employee seems to be fully composed and in control, the session is proceeding well, and the CSO is gaining confidence there will be no problems. The fact may be that the employee is stunned by the news and unable to respond in a manner that reflects true inner feelings. People who react this way may lack the capacity to vent, and if they hold back the stress—which tends to build over time—they can explode hours, days, or weeks later. To the CSO, this is a concern because the explosion can be directed at the company.

It can also happen that the employee will be so taken aback by the termination notice that he/she will not mentally process the implications and, in effect, act is if the interview is nothing more than a routine meeting. The employee simply chooses not to hear the bad news.

Psychological Trauma

Employees who react to termination with uncontrolled weeping, absolute silence, or what appears to be shock are probably incapable of reacting. It can be very unnerving when the employee clearly appears to need help and the CSO, who would like to give help, lacks the capacity to do so.

It occasionally happens that the CSO, motivated by a desire to help, will hint at or promise to assist the employee in some way that is not permitted by the terms of the discharge. This is clearly not a good move for the employee because the offered help cannot be delivered, and for the CSO the result may be a complaint on the grounds of a breach of promise.

When the employee cannot be returned to a normal state, the CSO should bring a treatment professional into the picture. A company, whether making multiple or single terminations, should have a third party present such as a counselor or HR representative. If the terminating person becomes violent or appears to be in the early stage of violence, a security officer should be close by. Having the security officer in the room can be a trigger for violence. The officer should be near enough to intercede if necessary.

Finally, and very importantly, the interviewer, without making a physical search, should not conduct the interview if the terminating employee possesses or appears to possess a weapon of any type.

Sorrow

Many employees will respond initially with expressions of disappointment and hurt. A lesser number will express anger, betrayal, and resentment. These are all natural reactions that can be healthy because they are venting mechanisms. The CSO can expect the employee to move from normal expressions of sorrow to practical questions about what happens next.

Belligerence

The CSO will be apprehensive about encountering an employee who overreacts when informed of termination. Although it is true that violence is possible, experience indicates that the odds are low that it will occur. Experience also indicates that when the CSO approaches the situation primed to respond with stiff resistance, the odds change greatly in favor of a confrontation.

The critical factor, then, when confronted with a potentially belligerent employee is to maintain self-control and not escalate the hostility. On the other hand, the CSO should not be defensive to the point of agreeing with the employee. Calmative gestures—such as a smile, a shrug, an open posture, and soft silence—may be useful in helping a belligerent person regain composure. A positive outcome is enhanced when the CSO proves to be an empathetic listener.

Disparaging comments against the CSO and the company are in the realm of normal behavior and to be expected. But certainly there are limits to the abuse the CSO should tolerate. Threats of harm and intimidating physical contact are unacceptable, and should they occur the CSO has three options: (1) warn the employee that the behavior must cease immediately, (2) call for assistance, or (3) conclude the interview.

Manage the Termination Interview

Preparing for the termination interview increases the probability of producing the desired results, reduces stress placed on the CSO, and helps keep the process on a professional level. Preparation means reviewing the reasons for terminating the employee, anticipating the range of reactions that may be exhibited, and determining a strategy and a set of tactics for controlling the reactions.

- Schedule the interview at a suitable place and time.
- Ensure that the employee will appear, even to the extent of personally escorting the employee to the interview.
- Know what should be collected (e.g., keys, credit cards, files, portable laptop, and so on).
- As soon as possible in advance of the interview, remove the individual's computer access to company files and to files held by others such as the company librarian. This rule is especially important when sensitive company information has been available to the individual.
- Arrange in advance security officer assistance that may be needed to counter a belligerent reaction.
- If emotional reaction is expected, consult with HR for advice and on-the-spot counseling for the individual if needed.
- Set up a procedure for the employee to leave the work site as quickly as possible with personal property in hand and with as much dignity as possible.

ORGANIZATIONAL STRUCTURES

Rubinstein holds that organization theory is an attempt to explicate and predict human behavior in an organization. The theory presupposes that the design or shape of a business organization will influence human activities. In the vertical organization, work processes are directly influenced by instructions passed down from bosses to subordinates and by lateral coordination among the bosses and the subordinates.

Vertical Model

The vertical organization is sometimes called the classic or pyramidal organization. At the top of the pyramid is the head of the organization and at the bottom level are the least influential of the rank-and-file employees. Status and authority increase as one moves up. Closely related functions are tied together in vertical chains, and hence the term "chain of command." A single chain might start one or two levels from the top, beginning with the CSO. One level below might be positions for the head of investigations and the head of guard operations. Below each of those might be three or four positions representing the functions of preemployment screening, credit card fraud, and physical security inspections.

At the top of the vertical organization is the senior executive and/or executive team. An executive team typically consists of the CEO, COO, and Chief Financial Officer. At the level immediately below are usually found the Vice

President for Human Relations and the Head of Information Technology. If the CSO is not at the second-down level, he/she will typically at the next lower level. At that lower level are likely to be found The Chief Information Officer and the Property Manager.

Perhaps more important than level is access to the important decision makers, i.e., the people who make the company run. The CSO is an ideal position when he is accorded an "open door" to the CEO's office.

As an organization grows in size and complexity, the chains multiply and lengthen.

Another in the variety of organizational form has pyramids on top of pyramids. The pyramid at the very top is corporate management. It is here that goals are established and major decisions made that affect operations in all the underlying pyramids.

Below corporate management are pyramids that can represent subsidiaries, major functions, business streams, or geographical locations. Each of these second-level pyramids has a senior management team that directs its enterprise in accord with the dictates of corporate management. The very lowest level of pyramids is operational management. These pyramids are arranged in sets that correspond to and support a senior management team.

Network Model

Humanity seems always to have organized its practices in hierarchies. Systems of top-to-bottom control have not been restricted to business but are found in the practices of religion, education, and the military. The notion of hierarchies has been enduring because it is orderly, efficient, and amenable to control. Many of us enjoy ranking things and don't feel comfortable without being ranked and knowing where we fit in the scheme of things.

The questions of today are "Does the vertical model work as well or better than other models?" and "Does the vertical model fit rapidly changing world markets?" The answers are often "no." Markets can suddenly rearrange in new and exciting patterns, calling for new business practices and human skills. The vertical model is slow to react to rapid change.

Many organizations now believe that the vertical model no longer functions effectively as a universal model.

In its place has come a model that goes by several names: flat, horizontal, open, and network. For our purposes, we will call it the network model. The network model features clusters of employees grouped according to the sets

of multiple skills they possess and which are needed to meet the organization's performance objectives. A basic tenet of Ostroff is that teams, not individuals, constitute the fundamental units of the organization and are encouraged to be self-managing.

Flexibility is a chief advantage of the network model. Consultants and contractors can offer services that do not require a full day at the company's worksite, which is a cost benefit to the company. The consultants and contractors, being independent entities, do not obligate the client to pay withholding taxes and provide fringe benefits. An advantage for the consultants and contractors is flexible work hours, which allows them to work for more than one client at a time.

Fewer layers of management are necessary because many of the managers and supervisors are either team leaders or almost "inside" the work process. In this arrangement, horizontal does not mean flat as in "flat as a pancake." Horizontal refers to work flowing horizontally. The work is performed by teams, each possessing skill sets that correspond to the nature of the work.

The network model is rooted in a plain observation that business practices based on price and economies of scale have lost their magic. Success in the new competitive environment is now believed to proceed from the possession and use of knowledge and rapid technological development. As a result, massive organizational changes are common, vertical organizations are flattening and opening up, and work is shifting from individual efforts to team efforts. Team success is often made possible by tapping into unique talent, inside or outside the organization. Human networks often form of their own accord to supplement networks of the formal organization. "Stars" of influence and technical know-how become contributors with or without management intervention.

Security Group Fit

To the CSO, the type of organizational model may not be as important as the work processes influenced by the model. The practices of control, downward supervision, and upward feedback that are part and parcel of the vertical organization diminish or disappear in the network organization. The CSO's attempts to retain and apply traditional controls are not always welcome in a company that believes in empowerment.

The mandate for the CSO is to achieve the same or higher level of results in a different manner. This is neither simple nor easy. On the one hand, the organization's management wants the CSO to embrace bold new concepts, yet on the other hand wants no dilution in the protection of assets.

Experience, whether the he has it or not, or likes it or not, the CSO is caught up in a process of learning and adapting to organizational change.

REVIEW QUESTIONS

1. Name and describe the eight steps of filling a vacant job.
2. State four reasons why a CSO might decide to hire an outside consultant.
3. Organization theory presupposes that the design or shape of an organization influences the work activities of persons within the organization. Along this line, describe and contrast the vertical and network models.

Further Reading

Jacobs, D.L., 1998. Small Business Legal Smarts. Bloomberg Press, Princeton, NJ.

King, C.E., 1993. Background checks: record searches. In: Fay, J.J. (Ed.), Encyclopedia of Security Management. Butterworth-Heinemann, Boston, MA.

Ostroff, F., 1999. The Horizontal Organization. Oxford University Press, New York, NY.

Rubenstein, A.H., 1982. Organization theory. In: Heyel, C. (Ed.), Encyclopedia of Management. Van Nostrand Rheinhold, New York, NY.

CHAPTER 3

Managing People

What You Will Learn

- The six levels of Maslow's hierarchy of needs.
- The importance of understanding and fostering employee motivation.
- Steps for appraising job performance.
- Challenges to setting effective targets.
- A technique for employee self-evaluation.
- Advantages and disadvantages to employee self-appraisal.
- The upward feedback process.
- The elements of the position description and its use in evaluating positions.

INTRODUCTION

Success at managing people rests on interpersonal skills that take the Chief Security Officer (CSO) far beyond the issue of being liked. Motivating others is not a matter of earning admiration, but of inspiring them to work individually and as a team. The CSO's principal task is to create a climate for work in which team efforts are organized and directed toward the attainment of agreed-upon and well-understood goals. But to effectively discharge that task, the CSO must comprehend the human needs, differences, and emotions of those being managed.

The willingness of subordinates to apply themselves to productive work activities is linked to how much personal value they find in the work itself. The CSO's challenge is to discover the rewards people find in their jobs and to integrate the rewards with work processes. This merging of personal desires with organizational needs is at once tricky and difficult. An understanding of motivational theory can help.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00003-7

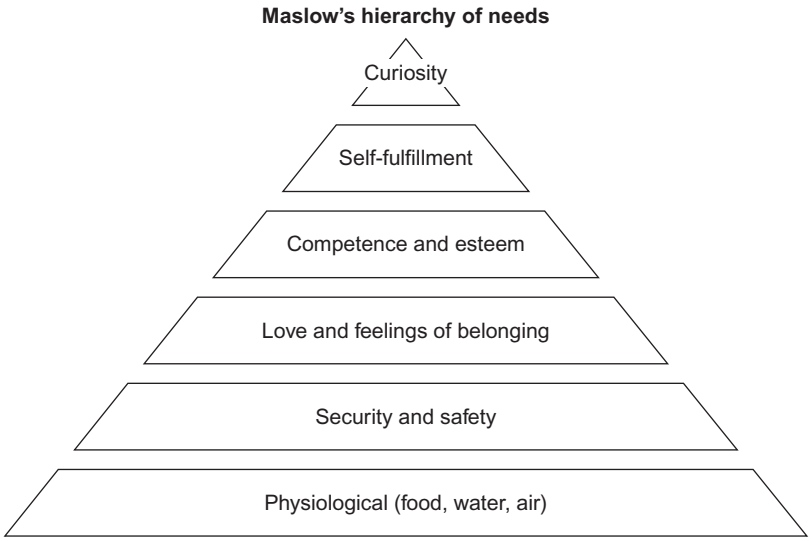


FIGURE 3.1
To the extent lower level needs are met, higher needs come into play.

MASLOW'S THEORY

Maslow's theory (1943) holds that motivation is the cause of an organism's behavior or the reason an organism carries out a particular activity. Fig. 3.1 illustrates the upward movement of human motivation. In the human organism, motivation involves both conscious and unconscious drives. Psychological theories hold that a primary level of motivation satisfies basic needs such as those for food, oxygen, and water. A secondary level of motivation meets social needs such as companionship and achievement. The primary needs must be satisfied before a person can attend to secondary drives.

The American psychologist Abraham Maslow devised a six-level hierarchy of motives that determine human behavior. According to Maslow, human needs operate in an ascending hierarchy that begins with a natural striving to satisfy the physiological imperatives. In this hierarchy, which can be abstracted as a pyramid, a higher need does not provide motivation until all lower, more basic needs are satisfied. When a need is satisfied, it ceases to be a motivator.

Physiological

The physiological needs are man's basic requirements for nourishment, water, air, and rest. A person's focus will be entirely on these needs for as

long as he or she continues to be unmet. Once met, the individual's focus shifts upward.

Survival

At the next level is the requirement to be free from harm. The safety and security of the individual dominates. Like the underlying physiological needs, this level is concerned with survival and self-preservation.

Love

At the third level, the individual strives for love and belonging. Affection and human relationships are the focal points.

Self-Esteem

Competence and prestige wrapped in self-esteem come next. These needs are satisfied through personal achievement, independence, status, and recognition and are similar to love needs because both are social in orientation.

Self-Fulfillment

The fifth order of needs is self-fulfillment or self-actualization. At this level, the individual self-expresses through the exercise of personal capabilities. Satisfaction is derived through the development of one's own potential and the expression of creative urge.

Curiosity

The highest and most abstract in Maslow's order of needs is curiosity. At this level, the individual is highly curious and strives to satisfy a thirst for understanding. The individual, for example, may find satisfaction delving into the mysteries of religion, life, or the origins of the universe.

Key Tenets

The key tenets of Maslow's theory can be summed up in the following observations:

- Man is a continuously wanting animal. When fulfilled in one need, he develops desires in another.
- When a person's needs have been satisfied, he or she ceases to motivate. A person must be confronted with a need before being moved to initiate, change, or sustain behavior.
- A need can be satisfied in different ways. A person who needs money will be motivated to acquire it. The method of acquisition in extreme

cases can be irrelevant. For example, a person might meet the need for money by going so far as stealing.

- One style of behavior may satisfy more than one need. A person who works hard to earn money may want the money to buy food (physiological), pay the mortgage (security), or gain prestige (self-esteem).

MASLOW IN THE SECURITY ENVIRONMENT

A person's natural striving to establish human relationships and to experience self-esteem is present as much in the workplace as in any other setting. A security employee, whether working at the line level or in management, has social needs that include friendship with coworkers and acceptance within the work group. The extent and intensity of individual efforts will vary, however. An individual who satisfies social needs outside the workplace may exhibit less striving than someone whose entire social experience is dependent on coworkers.

Attempts to satisfy the higher needs of self-esteem are often expressed by seeking recognition as a standout performer or as a valued contributor to the attainment of group goals. Most of us never stop looking for assurance that we are held in high regard by our peers, and even when we obtain that assurance today, we will seek it tomorrow and every day thereafter. Consider the following situation.

CRITICAL THINKING EXERCISE

Jason was young, competent, and newly promoted as head of the security group's credit card fraud unit. He loved his work and admired his boss. One day he got into a heated dispute with a peer, the head of the physical security unit. Jason took the matter to the CSO, hoping for a positive intervention. When the CSO seemed reluctant to intervene, Jason remarked, "What's a person supposed to do around here?" Without thinking, the CSO answered, "A man should do what he has to do."

Jason went back to his desk in anger. The anger festered for a week. A call came in for him from a headhunter. Before the month ended, Jason had resigned and relocated to another city, and the CSO never knew why.

Did the CSO error in the way he responded to Jason's request for intervention? If you believe this to be true, does the error prove poor leadership? What does this incident show us about retaining good workers?

Basic to an understanding of human needs is the recognition that people respond to CSOs, coworkers, and situations as perceived, not as they are in

reality. Retention studies show that 70% to 80% of the reasons people leave companies are related to bosses.

The ambitious employee working for an unsupportive boss will look at the options: stay with the company and get nowhere, or leave the company and continue to pursue the personal dream. Of course, not all employees are ambitious or highly motivated. An employee may not have a personal goal or not see the job as absolutely essential to personal happiness. At the other extreme is the employee who has a goal so lofty that the job is viewed as inconsequential.

It is not enough for a CSO to simply assign work. The work has to be organized in ways that facilitate needs. If an employee has a need to belong, he or she may find reward working alongside others; if the need is for self-esteem, reward may be found in having an important job title; and if ego satisfaction is the reward, the employee may find job happiness in being recognized. The CSO in some respects acts as a broker who helps parties of differing aspirations reach a mutually satisfying agreement.

The CSO who grasps Maslow's theory will appreciate that different employees have different needs and that their needs affect their output. The CSO looks for the signs of needs and supervises accordingly.

PEOPLE DEVELOPMENT

Excellence in managing people is founded on a belief that group performance is a reflection of the people comprising the group, the point being that the effective CSO will help group members be the best they can be.

Encourage

Although a member's development is largely the result of personal effort, the CSO plays a key role by encouraging the effort and offering opportunities. Fig. 3.2 takes a humorous approach to leadership failures.

Encouragement is often a matter of letting people know where they stand at the moment, giving them a clear sense of a future that includes them, and showing that the company will help them develop so that they can participate in that future. Encouragement is also given by making decisions about people fairly, equitably, and in the context of performance. It involves communicating openly and honestly and rewarding those who excel. Subordinates worth keeping usually want to know the following:

- Where is this train going?
- What risks will I encounter along the way?

You know you are a poor leader when…

You get more fun out of working a crossword than asking your employees how they're doing.
Your idea of freedom to work is not requiring employees to clock in on holidays.
Your top reward for an employee's outstanding work is a coupon for a Big Whopper.
An interviewee for a job learns your life story but you forget to ask why he wants the job.
An assistant says he can't get time to talk with you, you tell him the world wasn't built in a day.
You invite subordinates and the CEO to a party at a posh restaurant and no one shows up.
An employee asks to know the long-range plan, you send him to a fortune teller.
At a departmental meeting, you show slides taken at your daughter's high school graduation.
You tell a subordinate to rate his own performance, and then, you argue with him about it.
You show up at the job, your card key doesn't work, and a stranger is sitting at your desk.

FIGURE 3.2
It sometimes helps to use humor when being self-critical.

- When will we get there?
- What rewards will be mine personally?

Expect Excellence

Generating momentum for the development of subordinates is often achieved when the CSO expects excellence, is intolerant of substandard work, gives credit where it is due, and shoots for the highest star. The development of people is a basic ingredient in the recipe for enhancing group performance. Some employees will seek self-development; others will avoid it. Some employees will merit development opportunities by demonstrating enthusiasm and exceptional performance; those with low enthusiasm and poor performance will not. Consider also the points shown in Fig. 3.3.

PERFORMANCE APPRAISAL

Performance appraisal is the ongoing process of setting objectives and assessing individual and collective achievements during a finite period of time. It is primarily about counseling and feedback on ways to improve performance at an individual and team level and the quality of work relationships. Performance improvement results from people being clear about priorities and objectives, what skills need to be enhanced, and which types of behavior can help to this end. Clarity of purpose relies on open, positive, and constructive discussion between leaders and individuals and agreement on how to do the job better.

In the appraisal process, a CSO evaluates, coaches, counsels, and develops subordinates on a continuing basis throughout the reporting period, usually

People management standards

All employees must be taught the business context and their individual roles as team members.

The leader will

- Have primary accountability and authority for leading, deploying, developing, coaching, and rewarding people.
- Show commitment and competence through active and visible participation in teamwork, openly communicating with employees, and networking with others.
- Continually build personal capabilities.

The company will have a bias toward retention of skills and protecting its investment in people.

The leader will

- Systematically select and place competent employees.
- Use a variety of practices and methods to transfer skills and experience.
- Advertise employment opportunities.
- Utilize external resourcing after internal resourcing has been exhausted.
- Build relationships with, and maintain access to, external suppliers of specialized support and expertise.

Development of people is essential for improving business performance.

The leader will

- Describe the performance contract and competitive position to individuals and teams with clear and agreed objectives.
- Ensure sharing and learning from others including those outside the company.
- Assess individual and team performance. Provide clear feedback on performance delivery and improvement actions.
- Seek feedback from subordinates and peers via upward appraisal. Prioritize individual development objectives that improve skills and enable better performance and delivery through people.
- Identify employees with management and senior management potential early in their careers and participate in their development and deployment.
- Encourage personal development planning by individuals and coach them in their development and reality-check their plans.

The company will benefit to the extent that employees share in success.

The leader will

- Provide a competitive base compensation and benefits package.
- Demonstrate the relationship between business, team, and individual performance and reward, and ensure understanding by all employees.
- Quantify annual reward to reflect business performance, for example, pay top bonuses for top performance.

People are an asset and an investment.

The leader will

- Identify people risks, assess their consequences and probabilities, and set processes in place to address them.
- Audit the execution of people management standards to enable sharing of better practices and lessons learned and improve business performance.
- Ensure legal requirements are met.
- Support common systems to allow information to be shared and utilized.
- Identify responsibility for maintaining personnel records and systems that demand protection against unauthorized access.

FIGURE 3.3
This document is a menu for managers.

1 year. In the conduct of these activities, the leader's performance is subject to appraisal as well.

Setting Targets

Near the close or at the very beginning of the reporting period, the leader and his direct subordinates—individually or as a team—meet for the purpose

of setting performance targets. Target setting ensures the CSO and the people to be rated are in agreement as to what should be achieved.

Target Qualities

The targets are specific, measurable, relevant, and time related. Although firm when formulated, they can be amended and supplemented throughout the reporting period. Although targets will consistently correspond with business results and expected standards of performance, they can vary according to the type of work involved. They can also relate to personal development. For example, the CSO may encourage a subordinate to attain the Certified Protection Professional (CPP) designation. Although attainment of this target may not directly relate to a specific work output, few can dispute the job relatedness of skills and knowledge acquired in pursuit of CPP status.

To the uninitiated, target setting may appear to be more trouble than it's worth. Targets can be difficult to formulate and sometimes impossible to agree upon. They cause problems when the leader and subordinates can't come to terms because the targets are irrelevant, unchallenging, or overly demanding.

The leader might reject a subordinate's suggested targets on the grounds they lack sufficient work value, are not in line with business goals, or are simply too easy. The subordinate may resist the leader's targets when they are passed down from above like Moses' tablets and when they appear inflexible or laden with the risk of failure. Posing questions such as the following may be helpful to leader and subordinate alike in formulating targets:

- Does the target make good sense?
- Is it important to the subordinate, the CSO, and the company?
- Does it mesh with group or company goals?
- Does the target fall within the CSO's area of responsibility and authority?
- Does it carry risks operationally? Financially?
- If questioned, will top management support the target?
- Is the subordinate capable of meeting the target?
- Can attainment of the target be verified in a measurable way?

For most jobs, 6 to 10 targets will be sufficient, and it is possible that some or all will change or evolve as work progresses. Targets will sometimes be contingent upon factors beyond the CSO's ability to control, such as higher level approval of a planned project, availability of funds or equipment, and dependence upon the work of others outside the CSO's supervision.

Focus on Action Steps

In determining targets, it is useful to focus on the action steps required for achievement. A single target can incorporate several action steps. If the target is to "develop and administer a training module for entry-level security officers," the action steps could include writing a lesson plan, preparing or acquiring audiovisuals, constructing a test to measure learning, setting a training schedule, arranging for the place of training and needed training equipment, preparing certificates of completion, and making a record of attendance and scores. Time frames or deadline dates can be established for each action step, programmed to occur in a particular sequence, and assigned to several individuals in a team effort.

Base and Stretch

Targets can be of two types: base and stretch. A base target involves tasks that are integral to the job and sometimes routine in nature. Writing a report of investigation is a task of a security investigator's job and is fairly routine to do, at least for the investigator. A productivity gain might be possible by performing this task in a different manner. The CSO and his or her investigator may agree on a target calling for the investigator to revise the group's report writing method.

A stretch target goes beyond the norms of job expectations. It typically addresses a major problem, challenge, or opportunity, and its achievement can bring substantial reward to the organization. It may seek to raise quality, increase productivity, reduce costs, and develop new markets. Once the targets are set, they need to be put into writing, and any later changes should be written down and acknowledged by the subordinates with signatures or initials.

Performance Review

At preestablished intervals, the CSO and the subordinate meet to review progress. The subordinate is invited to comment on performance with respect to the agreed-upon targets, highlighting areas of success, improvement, and difficulties encountered. A form such as that is shown in Fig. 3.4 might be used for this purpose.

A review meeting can be a time for revising, canceling, or creating targets in light of experience. It is essential that the meeting be documented. The traditional method of documentation is use of a form or note-taking. However, new technology may make the documenting process simpler administratively such as by the use of video and voice recordings and Web-based applications.

EMPLOYEE REVIEW

Employee Name: _____ Date: _____

Department: _____ Period of Review: _____

Reviewer: _____ Reviewer's Title: _____

	EXCELLENT	GOOD	FAIR	POOR
Honesty	☐	☐	☐	☐
Productivity	☐	☐	☐	☐
Work Quality	☐	☐	☐	☐
Technical Skills	☐	☐	☐	☐
Work Consistency	☐	☐	☐	☐
Enthusiasm	☐	☐	☐	☐
Cooperation	☐	☐	☐	☐
Attitude	☐	☐	☐	☐
Initiative	☐	☐	☐	☐
Working Relations	☐	☐	☐	☐
Creativity	☐	☐	☐	☐
Punctuality	☐	☐	☐	☐
Attendance	☐	☐	☐	☐
Dependability	☐	☐	☐	☐
Communication Skills:	☐	☐	☐	☐

Comments: _____

_____

_____

_____

Employee's Signature: _____ Reviewer's Signature: _____

FIGURE 3.4

A form such as this can be helpful in considering the pertinent aspects of an employee's performance.

The subordinate may be invited to comment such as offering suggestions about how performance on particular targets could be improved. The documentation can serve as a discussion point at the next review meeting. The usual practice is to make the formal rating following the final review meeting of the reporting period.

Because business organizations vary widely, as do the preferences of the CEO or the human resources manager, performance evaluations vary widely. An analogy is the professional football team (a business organization) that follows a set of standards when drafting and hiring players (the employees) and the coach (the CSO) who evaluates a player's performance based on speed, strength, and stamina, all of which are demonstrable, measurable, and possibly capable of improvement.

In addition, performance appraisals vary within an organization according to the grade and responsibility level of the person being rated.

Self-Appraisal

Self-appraisal is sometimes a standard element in an organization's system for performance evaluation. The benefits of asking for a self-appraisal in most cases outweigh any disadvantages produced by the requirement. The form shown in Fig. 3.5 provides a means for the employee to honestly evaluate his or her performance. The following are advantages of a self-appraisal:

- The employee may be the best source of information about the quality of job performance.
- Self-appraisal increases the perception of fairness.
- Areas over which the rater and employee disagree can be highlighted.
- The process may help the employee gain personal insights as to success or failure.

The following are disadvantages of a self-appraisal:

- The employee may deliberately give a low rating in order to avoid disagreement with the rater.
- The employee may deliberately give a high rating in order to put pressure on the rater.
- When the employee and the rater disagree, bad feelings can result.
- The employee may dislike the idea of self-disclosure.

PERFORMANCE APPRAISAL CYCLE

Evaluation of performance is a process that continues uninterrupted. Although significant events relating to performance may occur at points over

EMPLOYEE SELF-EVALUATION

Employee Name: _____ I.D. No: _____

Department: _____ Date: _____

List objectives you met or exceeded during this performance review period.

1. _____
2. _____
3. _____
4. _____

List objectives that you did not meet during this performance review period.

1. _____
2. _____
3. _____
4. _____

List your key strengths.

1. _____
2. _____
3. _____

List skills you need to develop further.

1. _____
2. _____
3. _____

List your primary goals and objectives for the next performance review period.

1. _____
2. _____
3. _____
4. _____

FIGURE 3.5

When the employee self-evaluation process is taken seriously on both sides, the employee can become aware of personal shortcomings, and the supervisor can obtain insights to the employee's perception of the job and its demands.

time and are certainly worthy of consideration, they are not the only criteria for making an overall judgment. The process described here operates cyclically; that is, it transitions to a starting point from the ending point of a previous period, passes through one or more phases marked by preestablished time intervals, and moves to the starting point of the next cycle.

Starting Point

The starting point for appraisal involves CSO and subordinate agreeing on targets for the upcoming cycle, measures that will be used to evaluate performance, and meeting dates for the purpose of reviewing progress. Between quarterly reviews, the CSO observes the subordinate's performance, obtains feedback from the subordinate, and provides appropriate guidance or assistance.

Quarterly Reviews

On specified dates—usually at the end of the first, second, and third quarters of the reporting period, the CSO and subordinate meet to compare performance against the targets. The targets are revised, if needed, and the subordinate is coached and counseled, if needed. During the final progress review, the subordinate's overall performance is considered, forming a foundation for a written performance rating.

Ending Point

The end of one cycle and the start of the next tend to blur. Between the final progress review and the end of the cycle, the CSO selects a performance rating; writes the performance report and obtains the subordinate's comments and signature on the report; determines the subordinate's merit pay increase or bonus, if any; and begins to develop with the subordinate a new set of targets for the upcoming cycle.

Rating on Merit

A chief purpose of performance appraisal is to administer pay in a manner that takes into account the separate contributions of individual employees. Through a systematic rating procedure, usually called merit rating, a CSO is able to make equitable decisions regarding monetary and promotion based on appraisal records. Despite recurring complaints about the imperfections of procedures that link performance to pay and advancement, such procedures are usually objective and provide information that often cannot be obtained any other way.

Objective and Quantitative

Merit ratings are designed to replace subjective general impressions with judgments that are formed from empirically derived evidence. Generally, the evidence is quantitative in nature, capable of analysis, and collected over a period of time such as 1 year. When soundly developed and systematically administered, merit ratings can stimulate the person being rated, particularly when the rating methodology provides opportunities for CSO and subordinate to discuss ways and means for focusing performance on meaningful work outputs. This aspect of appraising is in the nature of making a "reality check."

A merit rating system requires the CSO to make objective judgments and present supporting evidence. The CSO is confronted with two questions: What is the standing of the rated person, relative to others, in terms of receiving a financial reward for work contributions? What proof is there to support that standing?

Unfortunately, the appraisal process is sometimes used only as a tool for making salary, and promotion determinations, as opposed to harnessing the process to the larger issue of improving productivity. In some organizations, supervisors have come to view the appraisal process as a necessary evil to be endured. They admit the process may have some value to the human resources staff, but believe it has little value to the tasks of supervision or to the enhancement of work output. Appraising for some CSOs becomes nothing more than filling out forms.

Conducted casually, performance appraisal can be destructive. Without a clear focus and a commitment at all levels, the process can poison CSO/subordinate relationships and seriously detract from optimum productivity. The rater and the rated person can be soured on the process, and management's credibility can be damaged.

Evaluating human performance in the workplace is both essential and difficult. Evaluating is essential because it provides the data for making decisions that affect the profitability of the organization and the aspirations of employees. Evaluating is difficult because it is continuous, complex, and fraught with hazards at every turn. The negative outcomes of an imperfectly administered program can be substantial, but so also are the positive outcomes.

UPWARD FEEDBACK

Upward feedback is a mechanism for communicating between CSOs and their subordinates. The process is intended to be mutually beneficial and has the following four aims:

- Improve communication between the CSO and his or her team.
- Improve teamwork.

FIGURE 3.6
A free and honest evaluation made by subordinates of their manager can lead to better understandings on both sides. *From Burns Security Services International.*

- Identify management practices where change will result in managing people more effectively.
- Create an action plan to which all members of the team can commit.

Upward feedback is marked by open thinking, personal impact, empowerment, and networking, and can help a CSO improve personal performance by obtaining a better understanding of how to lead others. The photo in Fig. 3.6 is a depiction of a security manager and her subordinates engaged in the upward feedback process.

Upward feedback is sometimes called the 360-degree process when it evaluates the CSO with input obtained from the CSO's subordinates and peers. Tornow (1998) suggests that management and communications skills are the primary performance factors assessed. A chief feedback criterion in the 360-degree review process addresses whether subordinates are satisfied with their access to information about, and opportunities for, career advancement. A CSO interested in furthering his or her understanding of upward feedback can do so by attending seminars on the subject, reading articles on the Internet and at the local library, purchasing books online and at a bookstore, and conferring with a subject matter expert such as the specialist in the HR department who coordinates or oversees the organization's upward feedback program. The primary benefit of understanding upward feedback is to view it not as an opportunity for subordinates to criticize or "get even" with the boss, but as a sensible, reasonable mechanism for looking at one's self through the eyes of others and making adjustments in managerial style that rewards the person being rated, the persons doing the rating, and the organization that benefits from improvements in performance.

A CSO's natural instinct may be to react to what at first appears to be personal criticism. After getting past the initial surprise, annoyance, and rationalization, the CSO may be ready to listen to the feedback and agree to make changes. Change need not be attendance at an organization-mandated seminar or weekly visits to a psychiatrist. Change can simply be helping oneself through introspection and experimenting with new ways of managing people.

Obtain Subordinates' Ratings

The process usually begins by distributing a questionnaire to the CSO's direct reports. The questionnaire in Fig. 3.7 is an example. The questionnaire is anonymous and contains questions relating to management practices that are widely held to be supportive of effective teamwork. The person filling out the questionnaire is asked to rate each practice in certain dimensions, for example, the relative importance that the respondent places upon the practice and the degree to which the CSO uses the practice.

The completed questionnaires are sent to an upward feedback adviser, who is usually a third party such as an outside consultant or a specialist within the organization's HR group. The questionnaires are scored, with significant variances noted. An example of a significant variance might be that the respondent considered conflict resolution within the team to be highly important but rated the CSO very low in effectively resolving conflict. A report is generated in the scoring process. Such a report might present findings as numerical data such as bar charts and as short narratives describing outstanding strengths and weaknesses.

Questionnaires are not the only tools suitable for obtaining upward feedback. There is always the good old suggestion box, confidential meetings with all or several employees at once, and confidential interviewing.

Upward Feedback Report

The report, which provides a snapshot of team members' perceptions, is the central topic of a one-on-one meeting between the CSO and an upward feedback adviser. The CSO sizes up the report's information, raises issues and questions with the adviser, identifies areas that need to be clarified, and develops an agenda and a plan to meet with the team to review the report.

The follow-up meeting with the team is chaired by the leader, with the adviser present to ease the comfort level of the attendees. The leader actively solicits observations and examples pertinent to the feedback report, listens carefully, and probes for understanding. The desired outcomes are for the

UPWARD FEEDBACK QUESTIONNAIRE

Notice to person completing this questionnaire: Upward feedback plays an important part in the Company's performance appraisal process. The Company is now asking you to provide constructive feedback on your manager's leadership skills and abilities. Please be honest and confidential in your answers. Directly forward the completed form to the Human Resources Department.

Name of Manager: _____

Rating Scale

Strongly Agree	Agree	Disagree	Strongly Disagree
1	2	3	4

My manager:

_____ Encourages me to suggest improvements in the way work is performed.
_____ Obtains my reactions and suggestions before making a major change that may affect me.
_____ Encourages me to express my concerns or doubts about a proposal under consideration.
_____ Empowers me to do my job.
_____ Identifies clear, attainable goals and objectives by stating what needs to be done and how.
_____ Provides an environment that motivates me to achieve my goals and objectives.
_____ Provides challenging opportunities that maximize the use of my skills.
_____ Acts as a sounding board for ideas.
_____ Recognizes and rewards innovation and creativity.
_____ Enables good performance by clearing roadblocks and providing support.
_____ Gives me opportunities for professional development and improvement of my skills.
_____ Is flexible in management style.
_____ Communicates corporate and departmental goals and objectives.
_____ Acts as coach and mentor.
_____ Builds a cohesive team.
_____ Provides honest and constructive feedback about my performance.
_____ Delegates effectively.
_____ Conducts regular one-to-one feedback meetings.

Comments: _____

FIGURE 3.7
The Upward Feedback Process focuses on managerial skills important to the business.

leader to gain a true understanding of the feedback and determine a foundation for action.

Immediately following the team meeting, the leader and the adviser confer privately. They review and obtain clarity on what was said. The adviser provides objective commentary and assists the leader in "reading between the

lines." The leader is led to explore areas in which change is appropriate and to make a personal commitment for improvement steps. The leader develops a draft of a realistic action plan that incorporates personal and team objectives.

Objectives for the Leader

Finally, the CSO sets up a meeting with his or her boss to identify ways to fully support achievement of the objectives in the action plan. Included on the agenda is a discussion of the training, education, or other resources that may be needed to carry out the plan. The leader circulates the agreed-upon action plan to team members. This helps confirm that the feedback has been heard at a level higher than the CSO, and that commitments have been made to act on the key areas.

Upward feedback means exactly what the term suggests. If it were called downward feedback, the process would be used to evaluate subordinates. No, upward feedback is a method by which the persons being supervised actually evaluate their bosses.

CRITICAL THINKING EXERCISE

Sally is the CSO at a major hospital. She had been accepted into the hospital's management development program consisting of formal instruction followed by a period of applied learning on the job. She filled out a pre-entry survey that asked her to rate her leadership ability. She considered herself reasonably skilled as a CSO and thus gave herself an 8 on a 10-point rating scale. During the formal instruction, she was required to ask for feedback from her boss, peers, and direct reports. The feedback indicated she had significant leadership weaknesses to overcome. In light of what the development program taught her and what the feedback told her, Sally concluded that leadership was more difficult and complicated than she originally thought it to be. She finished the formal instruction, and per the requirements of the program set personal development goals. In the ensuing months, she noticed improvements in her working relationships and the overall performance of the security group. Then came her annual performance appraisal. A self-appraisal form asked her to rate herself on a 10-point scale. Sally gave herself a 7.

Why do you think Sally lowered her score from her previous self-appraisal? If the group's performance improved, why didn't she rate herself higher?

Making upward feedback work can be difficult and tricky but well worth the effort. Grote (1996) believes the process works best when:

- It is business driven.
- The organization needs the behaviors that are measured.

- The process can reliably measure the behaviors of the people in charge and match their behaviors against the needed behaviors, i.e., behaviors that contribute to the organization's mission and objectives.
- Conditions exist for modifying unsatisfactory behaviors and providing opportunities for improvement.

POSITION EVALUATION

Position evaluation is the determination of an appropriate grade level for a specific position or job. Evaluation is not of the individual but of the job. It focuses on the nature and conditions of the job, not on the qualities of the incumbent. Because grade level is the chief determinant of salary or wage and other job benefits, the process of position evaluation is both critical and sensitive. Certain key pieces of information are necessary to make an accurate evaluation. These include:

- The nature of the job.
- The conditions under which the job is performed.
- Constraints and factors that assist the incumbent.
- How the job fits into the organization and its importance in the achievement of organizational objectives.
- The extent of accountability built into the job, including the dimensions and quantity of accountability.

Grade Level Determination

Grade level determination makes objective what would otherwise be subjective in evaluating a position. Management, in trying to sort out and make sense of the comparative values of different work functions, recognizes that the best that can be done is to introduce a sense of order into making what are essentially human judgments. Although many evaluation schemes use numbers and other seemingly objective criteria, the process is more art than science.

Position Description

As shown in Fig. 3.8, a position description contains:

- Identifying details such as job title, department, location, and so forth.
- A description of the overall purpose and chief objectives of the position and the nature of activities such as production, maintenance, sales, or special projects.
- Organizational relationships that identify the person to whom the position reports and those reporting to the position.

POSITION DESCRIPTION

Position Title: _____

Name of Incumbent: _____

Department: _____

Location: _____

Supervisor: _____

Position Number: _____

Approved By: _____

Date Approved: _____

MAJOR DUTIES

1. _____

2. _____

3. _____

4. _____

5. _____

ORGANIZATIONAL RELATIONSHIPS

This position reports to: _____

The direct reports for this position are: _____

The organizational peers for this position are: _____

COMPLEXITIES OF THE POSITION

(Circle One) Very Simple Simple Complex Very Complex Highly Complex

IMPACT OF THE POSITION ON THE ORGANIZATION'S MISSION

(Circle One) Very Low Low Average High Very High

POSITION DATA

Number of Employees Supervised: _____ Annual Budget: _____

Education Required: _____ Years of Experience Required: _____

Training and/or Certifications Required: _____

Comments: _____

FIGURE 3.8

The essential characteristics of a job can be found in a position description.

- The annual budget of the activity performed, the number of employees supervised, the nature and amount of funds that are affected by the incumbent, licensing, education, and experience requirements, and the extent and nature of contacts maintained by the incumbent.
- Principal accountabilities performed in accomplishing the overall purpose and chief objectives of the job.

Position evaluation is the process of comparing, ranking, and evaluating jobs by the use of specific qualitative and quantitative factors that include mental and physical skills, degrees of responsibility, and working conditions. It is the job that is evaluated, not the person performing it. An evaluation acceptable to an employer and an employee is used as a basis for determining pay and terms of employment.

REVIEW QUESTIONS

1. State the six levels in Maslow's hierarchy of needs.
2. Self-appraisal is a method for reviewing an employee's job performance. Identify a major disadvantage in asking an employee to appraise his or her own job performance.
3. What is the chief purpose of performance appraisal?
4. Provide a brief description of upward feedback.
5. Evaluating a position and evaluating a subordinate's job performance are different. In what respects are they different?

References

Grote, D., 1996. The Complete Guide to Performance Appraisal. American Management Association, New York.

Maslow, A.H., 1943. A Theory of Human Motivation. Psychological Review, New York.

Tornow, W.W., 1998. Maximizing the Value of 360-Degree Feedback. Jossey-Bass Publishers, San Francisco, CA.

CHAPTER 4

Leadership and Management Skills

What You Will Learn

- The dynamics of leadership.
- The competencies of an effective leader.
- Empowerment as a management tool.
- Leadership skills essential to managing security operations.

INTRODUCTION

The experienced Chief Security Officer (CSO) knows that when threats to security increase, it inevitably follows that demands on the security group will increase proportionally. The demands can vary, yet they all require for satisfactory response a trait we call leadership.

The CSO is expected to build within the security group a vision corresponding to the primary mission of the larger organization and has to persuade peers from other functions to accept the what, how, and why of security operations. For this last demand, persuasiveness is a crucial skill. In the persuading mode, a CSO can be likened to a minister pleading with a congregation to live by a universal truth. Everyone will agree on the truth, but not everyone will agree on how it is to be lived. The same is true for the concept of security: everyone will agree that security is essential, but not everyone will agree on how it is to be done.

LEADERSHIP IN THE MANAGEMENT OF SECURITY

Some CSOs are relatively new to crossfunctional leadership and feel inadequate because historically they haven't needed to exercise leadership skills outside the boundaries of the security group. Although leadership is difficult to define, most people agree that a leader has a focus on the future; that is, a CSO prescribes the means and methods for reaching group goals. Agreement

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00004-9

on leadership starts to fragment when discussion moves to the question of how a leader is made. Yet, when the shouting has ended, widespread support will remain for the proposition that the head of security has to exercise strong leadership skills when setting the vision for the security group and obtaining approval throughout the organization.

Complex and Subtle

Leadership in the security domain is complex and subtle. It involves thinking strategically, transforming strategy into results, working well with myriad personalities and groups, managing conflict, and directing the day-to-day operations of the security group. Functional expertise, which has always been important to effective security management, is a narrow part of a much broader picture. Setting up an access control system is functionally focused and narrow; formulating a vision and moving others toward its attainment is diffuse and broad. The wide horizon also encompasses an understanding of the nature of the company's business, the industry, the marketplace, and the constraints acting upon the company, both internally and externally.

Manager Versus Leader

The top security person is always a manager but not always a leader. A significant distinction exists between managing and leading. A manager does things right; a leader does the right things. Each role is critical to the success of the organization, yet the roles differ greatly in execution and impact.

Axelrod (1999) recalls a statement by General George S. Patton, one of the great teachers of leadership. He said, "You young lieutenants have to realize that your platoon is like a piece of spaghetti. You can't push it. You've got to get out in front and pull it."

A common problem in many security groups is that the person at the top spends too much time managing and not enough time leading. Some of the fault lies in a Peter Principle which holds that an employee who excels technically should be moved up to a supervisory or managerial position, even when it is apparent the employee lacks leadership skills. Partly to blame may be an absence in the organization of education and training systems that teach leadership skills.

BUILD A VISION

Building a vision is a first step in creating a reason for others to follow. A leader is able to draw the attention of others through an uncommon expression (e.g., Martin Luther King, Jr.'s "I Have a Dream") and a

prescription for change. The leader communicates a powerful commitment to break new ground and to go where others have feared to tread.

An outcome, a goal, a sense of direction is articulated. Attention is shifted to the leader, and people are drawn to the vision and are consequently enrolled. The vision is imprinted in the minds of followers, which involves 1% explicating and 99% creating a mental picture. The leader will be adept at using metaphors to transform words into tangible ideas and at reducing complexities with phrases, slogans, and models. The meaning of the vision is molded into a form that can be understood by all.

Communicate the Message

The techniques for communicating a message are limited only by imagination. A very common technique for communicating with people is public speaking, a depiction of which appears in Fig. 4.1.

People who would be leaders, such as candidates for elected office, look for innovative ways of getting their messages into the public psyche. A sign on Harry Truman's desk said, "The Buck Stops Here." That simple slogan conveyed a great deal about Truman and what he stood for, helping him to retain the presidency in spite of the odds against him.

FIGURE 4.1

A leader's message in the building of a vision is strengthened when followers and potential followers are able to see and hear the leader, evaluate body language, and gauge the leader's apparent sincerity and resolve. *From iStockphotos.*

Cultivate Trust

The chief component of trust is reliability. "You know where he stands" is a statement pointing to reliability. "That's not what he said yesterday" is also an indicator of reliability, although in the negative sense. People will follow an individual who can be counted on to stay the course. Reliability in the pursuit of a goal will gather followers even among people who disagree with the goal. Other components of reliability include honesty, integrity, and faithfulness. Fig. 4.2 points out the desirable traits of a leader.

Develop Oneself

Employing a correct mix of relevant knowledge and skills is a key competency. Included is the leader's nurturing and strengthening of personally held knowledge and skills, an activity carried out for the most part in the realm of experience. Leaders learn by doing, and because the doing is never perfect, mistakes occur. The pertinent point is that leaders learn from their mistakes. A mistake is often viewed as a lesson learned, as an option that proved to be less successful than another option, and as an inevitable step on the way to achieving a goal. The leader's focus is on progressing, not on losing ground. An example is the coach with a team on a long winning streak. He or she will influence the team to play to win, not play to keep from losing.

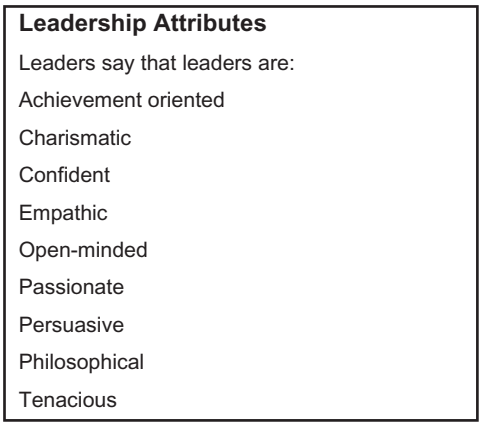


FIGURE 4.2

At a symposium sponsored by *cio* (a magazine for information technology executives), the leaders in attendance shared their thoughts on the attributes to look for in potential leaders.

EMPOWERMENT

Contributing

An effect of leadership is each employee's belief that he or she is contributing to the success of the organization. For various reasons, some employees make large contributions and others do not, yet all employees need to feel they are making a positive difference. The outcome of effective leadership is empowerment, a kinship that exists at all levels. The guard in the parking garage has the same feeling of belonging as the CSO on the executive floor. An interesting aspect of empowerment is a sense of community even among warring factions. It is quite possible for some people to dislike each other yet share a feeling of unity.

Sharing Accomplishments

The new millennium is marking a dramatic transformation of leadership. Tarnish is forming on the time-honored belief that a great organization is the work of one person. The shining new belief holds high the importance of leadership at all levels and is characterized by comradeship grounded in shared accomplishment. It is demonstrated and energized by small teams working toward common goals, and performing challenging tasks collaboratively. Understanding and managing these multiple relationships as essential partnerships is a must.

The greatest factor in the empowerment of a workforce and the ultimate determiner of which organizations succeed or fail is leadership. For as long as strategies, processes, and cultures change, the key to success remains leadership.

Energizing and Motivating

A CSO can bring excitement, challenge, and enjoyment to security jobs. These attributes develop out of vision and ideals that energize and motivate with little or no impetus from the promise of material reward or the threat of discipline. A pat on the back at the right moment can be more valuable, both to the security group and to the individual, than a raise in pay. An encouragement to improve performance can sometimes yield better results than a written admonishment.

Conflicting Values

When the CSO's vision fails to inspire, the reason is likely to result from a conflict of values. If the CSO adds or changes tasks, and as a result reduces

the quality of a service, some task performers will not want to follow because their core values prevent them from delivering a shoddy service.

Quantity Versus Quality

Interestingly, quantity is viewed objectively—such as the number of security guard hours sold per month—whereas quality is viewed subjectively—such as the morale of the security guards providing the services. A good leader understands both dimensions and is aware of the interplay between the definitive bottom line and the amorphous human soul.

Love of Work

Intimately connected with the concept of quality is love of work. A person who loves work will not be motivated by the desire for reward or the fear of rebuke. Love of work may lead the employee to improve output without prodding. The employee may discover a better way to perform a task, which can be the exact opposite of (and a great improvement to) the work system mandated by management. The following anecdote is instructive in this regard.

CRITICAL THINKING EXERCISE

One morning while passing through the lobby of the corporate headquarters where he worked as CSO, Andy observed a long line of impatient people waiting to be issued visitor passes. A few hours later, after the morning rush had subsided, Andy made it a point to stop at the visitors counter to ask the security officer why the early morning processing of visitors had taken so long. The security officer put his finger on a memo in his post orders and replied, "My supervisor told me to exactly follow this memo—the one you wrote."

Andy went back to his office and read his copy of the memo he had recently sent to the guard supervisor. It prescribed in great detail the procedure for issuing a visitor pass. Although long, Andy could see nothing wrong with the procedure. He called the officer on the phone and asked him what he had been doing before the new procedure went into effect.

"I was doing it my way," the security officer replied, and then, he described his way. The officer's way was faster and made perfect sense, Andy realized. He thanked the security officer for doing a good job and rescinded the memo.

FOLLOWERS

It is inescapably true that a leader cannot exist without followers, and writings on leadership give the impression that good leaders create good followers. Although a leader may attract and recruit people who are willing to follow, the followers may not be good at following.

Taking Directions

Becoming an effective subordinate is not all that easy. A first requirement for the follower is to take direction. A second may be to suspend an opposing belief or abandon a personal principle. Abstaining from dissent may also be an expectation. Over a period of time, small divergences can become large holes in the fabric of the group.

Telling the Truth

The most important characteristic of a follower may well be a willingness to tell the truth. As work accelerates and complexities multiply, a leader is increasingly dependent on subordinates for good information. Followers who tell the truth and a leader who listens can be a formidable combination.

Providing Feedback

An effective CSO looks for good people from many backgrounds with different points of view and encourages thoughtful dissent when decisions are due. Disagreement forces the CSO to closely examine a wide range of options that can lead to improved choices and better results. A leader is poorly served when his or her ideas are the only ideas or when the ideas are met with a unanimous yes or an acquiescent silence. A good leader will understand that dissent in the decision-making process, when cultivated and usefully channeled, is very healthful. Whatever annoyance a leader may experience at the moment of receiving contradictory feedback can be outweighed by the value of having made the best calculation possible. The soothing balm to the leader's damaged ego can be the expectation of group success and personal advancement.

LEADERS ADD VALUE

A leader's greatest contribution to a business organization may be to add value. Imagine that the head of marketing in a national contract guard company develops a unique method for selling services over the Internet. The method succeeds so well that the company improves its market share by 20% and raises profits to an all-time high. The head of marketing has added value by enabling the company to excel in a crucial aspect of the business.

It may be well to note that interesting things can happen in the aftermath of the event described previously. The head of marketing might be seen from the top as a brilliant and well-rounded leader who deserves admittance to the company's inner sanctum. On the other hand, the innovative marketer might be labeled a narrowly skilled specialist lacking the vision required to

perform at a higher level of management. The manner in which the head of marketing engineers the innovation and handles the success will affect his or her personal career.

COMPETITION AMONG LEADERS

A CSO is invariably in competition with other leaders, all of whom may have the same upward mobility aspirations. An organization can benefit greatly from competition among coleaders seeking to impress the powers that be. In the contract guard company described previously, a long-standing accession practice was to move the head of operations into the next higher position on the totem pole. The success of the marketer, however, altered the script. Faced with a threat to advancement, the operations man shifted into high gear and found opportunities to reduce the company's turnover ratio, which in turn helped fill new jobs created by the marketer's innovation.

Ambition

Do not doubt for an instant the ambitious nature of the CSO. Although hard work behind the scenes may be a condition of the job, it is in the natural order of things for the CSO to aspire to a higher position. The lure of advancement and status is a powerful narcotic that draws people to positions of power and leadership.

Loyalty

There is an irony in the truth that a leader in the making is a follower and that following requires loyalty. Loyalty is steadfastness, a trait that is often called "hanging in there." Steadfastness is not blind devotion and fawning adulation. Loyalty the follower shows the leader can be justifiably withdrawn when the leader takes a seriously wrong turn. For example, a CSO's loyalty to the CEO can entirely disappear when it is clear that a serious crime—personal or corporate—has been committed and that the CEO is a guilty party and actively engaged in its concealment. The CSO is no longer a willing follower and may have just one option: blow the whistle and move on.

A CSO will move on for other reasons as well. He or she may decide that the time is right to advance, either by hiring on with another organization or by creating an organization. The decision to leave may also result from a realization that advancement in the current organization is simply not attainable or not worth continuing the effort. Behind such a decision may be the deterioration of the relationship between the CSO and the boss. More than a few talented people have said adios because of "philosophical differences."

PRICE OF LEADERSHIP

Then, there is the price of leadership. The demands of a top position can cause a CSO to sacrifice family, friends, and the simple pleasures of life. Staying at or moving toward the top can have price tags: divorce, alienation, physical breakdown, and mental aberration.

A society that adulates and disproportionately rewards athletes is also a society that focuses on organizational leaders. Just as a premium athlete can quickly fall from grace, so can a CSO. The head of a security group will be removed from the helm with the same speed as the manager of a cellar-dwelling baseball team.

LEADING IN THE 21ST CENTURY

The reader by now should have grasped a key point in which the hero form of leadership has given way to a new form in which the leader is a catalyst and facilitator.

Build and Manage

The CSO is expected to build and manage a network of personal relationships that goes beyond direct reports and subordinates. The CSO has to initiate and cultivate relationships throughout the organization and in the external environment. This personal network cannot tolerate dead wood. Fulmer (2000) expresses a belief that failing relationships have to be abandoned and replaced with new relationships. Associates inside and outside the organization belong in the CSO's personal network to the extent that they contribute to the security group's goals, and the vendors of security products and services who are long on promise and short on delivery need to be weeded out.

Know the Landscape

The CSO has to know where true power resides in the organization, understand the nuts and bolts of the organization's business, and understand where the organization fits into the larger picture such as the industry or the regional and national economy. Very demanding and essential is the perception of patterns and trends occurring in the organization, in the customer and supplier bases, and in the political and legislative arenas. What do the trends mean to the security mission now or in the future? How can these insights be turned to good advantage? Knowing the landscape requires face-to-face exposure to insiders and outsiders, hence reinforcing the importance of building and managing a personal network.

Expect the Best

The CSO in pursuit of exemplary achievement is self-challenging. He or she sets personal goals that are higher than prior achievements, yet attainable. This attribute is conveyed by example to subordinates.

Do Not Micromanage

A common failing is to be personally active in every facet of security group activity. Subordinates lose interest in their work when the boss is continually looking over their shoulders and telling them how to cross the *T*s and dot the *I*s. A command-and-control approach may have value in military and training settings but not in a fast-paced business setting, especially in a security group staffed with capable people.

Be Accessible

Staying out of the way of people at work is one thing; being available to help is another. Accessibility can be as simple as inviting questions, giving prompt answers, listening, and letting subordinates know that "the door is always open" or giving them a contact telephone number or e-mail address.

Focus on What Is Important

Certain of a security group's activities will be more important than others. Important activities are those that have high relevance to company goals and those of an exigent nature. Sometimes, the exigencies occur with such great frequency that the CSO is forced to focus almost exclusively on putting out brush fires. Part of being properly focused is choosing the correct yardsticks for measuring security group performance. To illustrate, a traditional focal point of a cost-conscious CSO is the amount of money spent on guard services, especially for overtime. In being overly concerned with controlling overtime, the CSO may miss the more important issue of providing adequate protection. A better measure of performance might be dollars saved through reduction of loss.

Point the Way

The ability to communicate a clear direction is essential. Every person in the security group should be able to articulate exactly what they do and why. The CSO has to help subordinates understand their individual roles and how those roles contribute to the goals of the group and to the larger organization. This is essential for the same reason it is essential for the CSO to know his or her landscape.

A CREDO FOR THE SECURITY LEADER

Decide what you do best and then do it: Identify your strengths and apply them where they are likely to yield the greatest return. Look for opportunities that correspond to your strengths; improve your ability to do work you presently cannot do well.

Anticipate change: Know the business of your employer. Anticipate that the business will evolve and be prepared to evolve with it. Don't be content to merely hold your job; look for ways to be come better. You can be certain that the way your business operates today will not be the way it will operate a year from now.

Self-assess continually: Never stop asking, "What are my goals and am I on the right track? How can I improve the services I provide? Do I have operating costs that can be reduced or eliminated?"

Maintain a dialog with the users of security services: Deliberately and actively strive for open communications with the employees at all levels. Ask them what they want; pay attention to the answers; deliver what they want, if you can. If you can't deliver, say so. Be honest, even when there's a risk that the listener will be unhappy with what you have to say.

Think partnership: Be more than just another manager. Get into the employees' mind to learn needs, wants, and expectations. Devise new ways to deliver. Be proactive in suggesting better ways to do the job.

Act like a winner: Display confidence. Emphasize the positives and don't hide behind excuses. Be determined to do what it takes. A good motto is "I will not fail." The flip side of deciding not to fail is making business decisions unemotionally. When a course of action under your control shows signs of certain failure, have the courage to shut it down quickly.

Think long-term but concentrate on today: People have concerns about what you are doing for them today, not what you think you will be able to do for them next year.

Show the value: People are willing to buy into security programs when they understand the value derived. Demonstrate how security programs contribute to the bottom line. For example, a new access control system will enhance control of entry and reduce the cost of guard services. Explain these advantages. Use real-life examples to drive home your points.

FIGURE 4.3

Many skills go into the making of an effective CSO.

CONCLUSION

Effective leaders are persons who get things done. They become leaders by attaining knowledge, gaining experience, and learning from mistakes. They remain leaders by inspiring their followers to work together in pursuit of common goals. For some people, leadership is elusive; for others, it comes naturally. It may appear that some people are born to be leaders, but the truth is that leaders are made, and by their own efforts. Fig. 4.3 points out aspects central to the effectiveness of the CSO.

REVIEW QUESTIONS

1. An organization's CSO is always a manager but not always a leader. What is the import of the statement?

2. Define and give an example of empowerment.
3. In the delivery of security officer services, a distinction can be made between quantity and quality. Describe the distinction.
4. A Chief Security Officer is expected to "know the landscape." What is the meaning of the statement?

References

Axelrod, A., 1999. Patton on Leadership. Prentice Hall, Paramus, NJ.

Fulmer, W.E., 2000. Shaping the Adaptive Organization: Landscapes, Learning and Leadership in Volatile Times. American Management Association, New York.

CHAPTER 5

Strategy

What You Will Learn

- The difference between policy making and planning and the interaction of the two.
- The three factors that cause change in business operations and the effect of those factors on security operations.
- The six imperatives placed on the Chief Security Officer to align security operations with company goals.

INTRODUCTION

Business strategy shapes the overall configuration of the company and the core and support activities that support company goals. Helping but sometimes interfering with the company's business processes are developments that demand change such as restructuring the company or outsourcing noncore functions. The effects of strategy on security management are many and complicated, particularly the effect of technical knowledge on security operations. With strategy comes risk that is difficult to anticipate and fully understand. More than that is the need to craft countermeasures designed to eliminate and mitigate the threats that create the risk.

Policy and planning cannot be separated. Policy statements, which are written at the very top of the organization, are generally short and sometimes vague. They describe what is to be done, i.e., the organization's mission. Planning is detailed, sometimes unnecessarily so, and a function of bringing policy to life. It establishes plans, such as a plan to evacuate a building in case of fire, and assigns responsibilities to specific people that perform as commander, coordinators, and responders.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00005-0

BUSINESS STRATEGY

Three observations about security management are in order. First, the Chief Security Officer (CSO) operates in a rapidly changing business world. Fahey (1999) has recognized that the fast-paced and highly competitive nature of business is forcing companies to continually find new ways to be productive at lower cost. The new ways of doing business bring new security risks.

Second, every important decision made by the CSO depends on having accurate information, the sources of which are numerous and disparate. Sources that contribute to effective decision-making can include industry counterparts, consultants, representatives from the law enforcement and intelligence communities, advisory reports, such as those published by the Department of Homeland Security, State Department, federal bureau of investigation (FBI) and central intelligence agency (CIA), and from the security group's history, as reflected in its files and the experiences of its members.

As described in a later chapter, the CSOs of major corporations with activities in the 18 sectors of the nation's critical infrastructure coordinate their security programs with the government.

Important security decisions are never risk free, and possessing or having access to the best information available is a critical factor in arriving at the best possible decision. Fig. 5.1, a photo of the World Trade Center Towers in

FIGURE 5.1
The terrorist attack on the World Trade Center Towers impacted the nation's financial infrastructure. *iStockphotos.*

the aftermath of the 9-11 attack, demonstrates the consequences of an attack that had been shrouded in tight secrecy and carried out with extensive planning and preparation.

Third, international terrorism is on the scene in a very serious way. As of the writing of this book, our nation has not been attacked a second time, but people in the know tell us that another attack, or multiple attacks, is certain to occur. The only questions are: when, where, and with what. The European experiences are indicators of what may happen on our shores.

CORE AND SUPPORT ACTIVITIES

Nearly every business of size is organized along lines that permit simultaneous management of two main activities: the core activities at the heart of the enterprise and the support activities that contribute to the core. The core work, being essential to the business and having value that demands protection, is usually assigned to proven and trusted employees. The support work, while important to some degree, usually does not produce a significant or sustainable advantage to the business. The support staff tends to be varied, running the gamut from unskilled to highly skilled.

OUTSOURCING AND THE SECURITY GROUP

The manner of staffing in large companies has always been driven by economic imperatives. Company leaders endlessly look for ways to cut costs, and in recent years, outsourcing has been a principal cost-cutting tool in the management of human resources. A main theme of outsourcing is to lower labor costs by replacing higher paid permanent employees with lower paid contract employees. Another form of outsourcing is to move jobs to other countries where the cost of labor is lower than that paid to American employees.

Business leaders who opt for outsourcing embrace the notion that support work is mainly done in-house for reasons of convenience and that transferring support work to vendors will not affect the critical core of the enterprise. They wish to realize the full value of less-important activities at a lower overall cost and at the same time attain greater flexibility and a sharper focus on improving the core.

Beginning in the early 1980s, major company after major company fell head over heels in love with outsourcing. In short order, they brought in outside companies to take over jobs in accounting, payroll, purchasing, property management, mailroom operations, food service, shipping and receiving,

transport, secretaries/clerks, and so on. By transferring noncritical work to outside providers, managers believed their valuable time was freed up to concentrate on generating revenues. Added advantages included transferring frontline supervisory responsibilities to vendors and holding them to high service standards. The really big incentive to outsourcing was cost reduction. In more than a few cases, outsourcing did not deliver the advantages sought.

A central tenet of outsourcing is to retain the core functions. "Are security functions core functions?" This is a good question for the CSO to internalize. A management that does not perceive security to be a core function is more likely than not to outsource security. A security group that demonstrates competency in the services it provides is less likely to be replaced because management may not be convinced that an equal or better level of competency can be found at a lesser cost by going outside the company. It is fair to say that a management's perception of competency in the security group is the perception it has of the CSO's competence.

Companies that manufacture expensive products at risk during production, such as aircraft manufacturers, or companies that spend huge amounts of money on research and development of new generations of products, such as manufacturers of personal computers (PCs) and software, have no choice but to view security as indispensable, and therefore a core function.

In a fast-evolving market where new technologies are emerging, the knowledge and skills of employees are essential. Greaver (1999) believes that an organization holding exclusive rights to an emerging technology, and at the same time has a workforce strong in technological knowledge and skills, has a huge advantage over competitors.

A management often seeks to link the outsourcing process to the aims and success factors of the business. The idea is to take into account the company's drivers and market position, commercial and customer values, and the culture of the workforce. Decisions about retaining functions versus outsourcing them involve considerations as to efficiency and effectiveness, as well as to cost. Also considered are opportunities to regroup functional tasks in lieu of outsourcing and to unbundle tasks so that some can be kept and some outsourced. After those decisions have been made, the management identifies potential providers; tenders, negotiates, and awards bids; and manages the transition.

Outsourcing of the security function is familiar because it is common. A great number of organizations hire contract guard companies. The main driver in choosing a contract guard force over an in-house guard force is cost. A minority of organizations prefer having their guards on the payroll. The main drivers for these organizations are direct control of guard operations, loyalty, and low turnover.

Protecting Assets Under Altered Circumstances

The CSO's duty in outsourcing involves developing and implementing new procedures for protecting assets in rapidly changing circumstances. The duty is not easily met. The company's most valuable assets (such as entire computer systems and sensitive databases) are frequently placed into the direct and unrestricted control of vendors. The vendors, while happy to accept the assets, are not always enthusiastic about following the CSO's assets-protecting guidance, even when the outsourcing contract calls for the vendor to safeguard the entrusted assets. Adding to the general misery of the CSO can be the unwillingness of the company's department heads to intercede. Many tend to see security as counterproductive, especially during the start-up phase when they are anxious to make outsourcing succeed. Failure to make outsourcing work may adversely affect the department head's performance evaluation, an outcome to be avoided. The CSO's warning that assets may be at risk is often muted by the day-to-day bustle of launching the project.

CRITICAL THINKING EXERCISE

The XYZ Company sold merchandise on the Internet and by catalog. The critical core of the business had always been marketing, processing orders, and paying attention to customers. Receiving goods from manufacturers, storing them in a warehouse, and shipping orders to customers from the warehouse were considered noncritical support functions. After hard negotiations that were kept secret from employees, including CSO Bill Booth, XYZ outsourced the support functions to a low-bidding vendor. The XYZ inventory was transferred to the vendor's warehouse, a much larger facility where orders were shipped for other mail order companies, some of which were in direct competition with XYZ.

Nearly 90% of the XYZ receiving, warehousing, and shipping employees were let go and the company's smaller warehouse sold. Near the end of one year, XYZ was not happy with the vendor. Orders had been consistently lost, misaddressed, and filled improperly; large quantities of goods in storage were missing and not accounted for, and there were indications that the vendor had released an XYZ customer list to an XYZ competitor. Bill Booth went to the vendor's warehouse to make recommendations for improving the security of XYZ goods and its sensitive information. Booth was turned away.

XYZ announced to the vendor the intent at the end of the next 90 days to cancel the contract. The vendor demanded to be paid in advance for the final 90 days. When XYZ refused, the vendor closed its doors to XYZ representatives and stopped all work in support of XYZ. Not having access to its own inventory, XYZ became a nonfunctioning business.

A civil court restored XYZ's rights, but by then, the business had been badly damaged. The vendor's defense to the judge was that XYZ had made unreasonable demands, insulted the vendor's employees by telling them how to do their jobs, and offered only criticism in the resolution of problems.

Was there anything Bill Booth could have done to prevent this situation? What is the interaction here between business strategy and asset protection?

Due Diligence

A number of lessons can be found in the Critical Thinking Exercise. First is to learn all that can be learned about a vendor before awarding a contract. A particularly good learning device is a due diligence inquiry. Due diligence is a formal, overt investigation conducted by a company contemplating doing business with another company. The company making the due diligence inquiry seeks to verify representations made by the other company and to generally assess suitability, integrity, and financial strength. The inquiry includes gathering credit reports, searching records of criminal and civil courts, and making background checks of principal officers.

Ambiguous Specifications

Ambiguous specifications can lead to problems as well. An example is, "Vendor will provide a reasonable level of security for client assets entrusted to the Vendor." The vendor is free to provide security to any degree it wishes, at least until a clear definition is made of "reasonable level of security."

But the outsourcing companies are learning from their mistakes. A service level agreement (SLA) is now a standard. An SLA defines terms susceptible to interpretation; clearly spells out the scope and nature of work to be performed, the skills required of people assigned to the work, the methods for assessing the quality of output; and specifies steps to be followed if either party believes the terms of the SLA have not been met.

EFFECT OF STRATEGY ON SECURITY MANAGEMENT

Anticipate

An often under-appreciated skill is the anticipation of the effect that a particular management strategy will have on security services. In the development of a company strategy, the CSO can be a key contributor by proposing measures to eliminate or mitigate security-related exposures that may arise when the strategy is implemented. For example, if the strategy includes outsourcing the company's electronic data processing function, the CSO may see a possible compromise of sensitive proprietary data. Identifying the exposure is important but much less than half the chore. The difficult work comes in developing a countermeasure that will offset the risk while not sidetracking the strategy.

Exposures

While potential exposures are not easy to detect and even more difficult to prevent or mitigate, the CSO can at least rely on the common sense

observation that security risks rise when adjustments are made to the manner of work performance. A shift in strategy can move through the organization like a slow-moving earthquake. Formal and informal controls on people performance that have been set in place by tested practice can be shattered. Tiny fissures on the surface signal large disturbances below, foretelling eruptions that carry high risk. Loss events are waiting to happen, and it is the CSO's function to anticipate and prevent them.

Magnitude

The magnitude of potential loss tends to rise relative to the nature of the work. Think, for example, of the potential loss linked to a strategy shift that brings temporary filing clerks into the accounts receivable department. Now compare that shift to one in which the secret formula for the company's best-selling product is placed into the custody of a vendor.

Complexity

Complexity of the work is also a factor. The possibility of a security-related loss will rise relative to the complexity of the work. A CSO is not or does not have on staff an expert in every area of the company's total operations. Information technology (IT) is a good example. In an outsourced situation, there may be few, if any, individuals remaining in the core workforce who have a level of IT expertise sufficient to notice an exposure in a complex operation. Even after a loss occurs, the company may not have in-house resources able to properly diagnose the exposure and prescribe the correct remedy.

TECHNICAL KNOWLEDGE

Although it is unreasonable to expect the CSO to possess a comprehensive range of technical knowledge, it is quite reasonable to expect him or her to know where to find it and have it available on demand. Technical knowledge can be viewed as a dimension of business and operating in three human competencies: access, quality, and teamwork.

Access

Access refers to knowing where to find the right information, service, or product at the best price. It often means building sound relationships with actual and potential vendors and networking with peers. The transfer of "best practices" among security practitioners is an example of sharing technical knowledge.

Quality

Quality is the optimal balance between cost and technical excellence. Consistency in quality rests on quality control and quality assurance. Quality control is the responsibility of the supplier; quality assurance derives naturally from confidence in the relationship. In a mature connection between client and vendor, cost and quality will occur together, to the advantage of both parties.

Teamwork

Teamwork is the bringing together of people who each contribute from complementary specialties. It is a collective competency which gives to the players what they need to get the job done right. The needs might be information, a service, or a product. A team or teams may be the security group or the security group in tandem with various product suppliers and consultants. Team composition will vary according to the mission, with each member contributing a different set of skills and abilities. Teamwork calls for sustained leadership and goal orientation.

In a single sentence, these three competencies operate to obtain access to the essential information, services, and products that fuel the security function, assuring quality through mutual cooperation.

STRATEGY AND RISK

The ability to predict and quantify a full menu of risks is the CSO's highest mark of excellence.

Predict

To predict risk, which is restricted by the limitations of human understanding and available technology, is to identify the nature of threats confronting the organization and assessing the probability of their occurrence.

Quantify

To quantify risk is to measure potential consequences through the application of science and experience. To control risk is to logically and flexibly manage resources in ways that offset threats.

The genuinely competent CSO will obtain through continuous self-development an ability to deal with evolving threats, know where to find the technical assistance sufficient to counter them, and be positioned to acquire assistance when it is needed.

IMPERATIVES

The reader may detect the outlines of a security strategy taking shape. Integral to it are six mutually reinforcing imperatives:

- Improve on quality and cost.
- Forge close links to customers.
- Establish close relationships with suppliers.
- Make effective use of technology.
- Operate with minimum layers of management.
- Continuously improve the security staff.

Improve on Quality

The measuring stick of security performance is high quality at reasonable cost. The facets of quality are excellence, reliability, and speedy delivery of services. Successful security operations are those that strive to be the "best in class" in all the main performance venues. A characteristic of the leading performers is an emphasis on competitive benchmarking, i.e., comparing personal and unit performance with the industry's leaders, and setting goals to measure progress.

Forge Close Links with Users

Successful CSOs make concerted efforts to develop close ties with the users of security services. Who are the users? They are all of the persons within the organization, a fact forgotten by too many CSOs.

Forging a link is less like making friends through public relations and more like getting into "the mind" of the user. It can happen the CSO will know the user's concerns before the user becomes aware of them. Having that mental connect allows the CSO to respond quickly and appropriately.

Strategy in any business context is meaningless without reference to customers. The dominant aim of strategy is to deliver superior value to customers in exchange for a benefit. For the operator of a contract security company, the benefit is that elusive thing called profit. For the CSO, it is the recognition that follows on the heels of superior service. A persistent and unavoidable challenge of the CSO in the battle to sustain superior value is to stay a step ahead of those in a position to judge if value is present. Said another way, the evaluator is seeking to determine if the service provided returns a value in excess of cost. The CSO is seeking to maintain an image pleasing to the evaluator.

A standard practice by CSOs in corporate security is to compare the quality of the CSO's group against that of a security group in an equivalent

corporation. The practice is called benchmarking, a term that implies the highest mark is the goal for all others to meet. There is a fallacy in the concept because the highest mark may not be high enough. Simply emulating what others do cannot lead to superior performance.

Establish Close Relationships with Suppliers

Too often, cooperation with suppliers is achieved through the coercive power of the buyer. The alternative described here, however, is the creation of partner relationships in which price is not always the most important factor. Coordination with external vendors is crucial to a CSO in acquiring technical assistance in whatever form that assistance might take, e.g., electronic countermeasures, forensic examinations, surveillance, and undercover operations.

If a key element of strategy is to position the in-house security group to be a leader in using technical services in support of the mission, it follows that the CSO will be active in developing partnerships with the suppliers of technology. The idea is to select a small number of capable suppliers and work with them. A partnership arrangement has little room for second-guessing and beating suppliers down to the last penny.

When a vendor provides contracted guard services, the CSO should forge a positive working relationship with the guard company's account manager. An understanding between them can help both parties find a balance between assuring high guard performance and recognizing the guard firm's right to supervise its own employees. If guard performance is inadequate, the CSO has a duty to offer constructive direction, and the account manager has an obligation to listen and respond within reasonable limits. None of this is possible without a solid working relationship.

Make Effective Use of Technology

A security strategy linked to technology will require the CSO to have knowledge of work-enhancing technologies available in the marketplace and a skill in using them wisely. Being wise about technology involves recognizing that newer is not always better, and even when a technology is in fact superior, the final payoff has to exceed the costs of the technology and applying it. In short, technology must earn its way.

In looking for a technological solution, the CSO should not try to reinvent the wheel but at the same time not have a closed mind to a technology simply because it does not perfectly match the situation. Common mistakes are to reject a technology that is not totally applicable but is workable in all the important tasks and to expect more than a technology can deliver. Very

important also is to get the solution right the first time because retrofitting can be costly.

Another consideration is the working relationship between the security employees and the equipment or routines that make up the technology. This is not so much a matter of ergonomics but of the symbiotic linkage of man and machine. In companies where technology is routinely applied, the security employees are better able to adjust when a new or more complicated technology is acquired for their use.

Operate with Minimum Layers of Management

Organizational structure, specifically the horizontal distribution of departments and the vertical arrangement of managerial layers, varies considerably from company to company. Today's trends favor greater functional integration and fewer layers of management, both of which promote speedy delivery of services and a strong responsiveness to customer needs. These are virtues to be cherished by any prudent CSO.

Execution of the security strategy in a flat, lean organization will in most cases rely upon a small, yet well-rounded staff of the highest quality, working in partnership with suppliers who bring to the arrangement a broad array of technical competencies. The competencies that stand out are in the job domains of computer security specialists, antisurveillance technicians, auditors, questioned document examiners, access control specialists, and so on. The security profession, although very broad and mature, can be surprisingly innovative when it comes to harnessing the special talents of little-known experts.

Continuously Improve the Security Staff

The first five strategy elements require departures from the conventional way of dealing with employees. The changes call for developing a new mindset, a new commitment, and strong leadership. Progress will seldom be comfortable when old ideas are refashioned or cast off.

The improvement of security staff depends on the infusion of large doses of meaningful, useful knowledge. The modes of teaching can include counseling, formal classroom instruction, and on-the-job coaching. The constant in the process is unending development of employees, not merely development to get the strategy up and going, but development throughout the employees' working lifetimes.

The outcome of staff development will be technical competency, quality output, teamwork, and a flexibility that permits acceptance of daunting challenges.

STRATEGIC PLANNING

In most of the previous century, planning carried out by senior management was called long-range planning. In today's high-tech environment, it is deserving of a fancier name: strategic planning. Large companies everywhere plan strategically, and smaller companies in increasing numbers are following suit. Indeed, it can be said that in the fast-paced and intensely competitive marketplace of the new millennium, any corporation worth its salt cannot afford to operate without strategic planning. According to Hoenig (2000), a leadership guru, an organization has no choice except to engage in strategic planning. The real issues are how much planning to do, how to do it well, and when to apply it. Fig. 5.2 provides examples of how not to plan or operate a business.

Strategic planning underscores a point sometimes forgotten, i.e., that a business organization has two types of management. That which is done at the top is called strategic management. Everything else is operational management. Planning done at the top is long-range in nature, and planning below the top is the now of short-term planning. The CSO is always a developer of operating plans, but is only sometimes involved in the development of strategic plans—not because the CSO is regarded as a poor team member in

Murphy's Law

Nothing is as easy as it looks.

Everything takes longer than you think.

Anything that can go wrong will go wrong.

If there is a possibility of several things going wrong, the one that will cause the most damage will be the one to go wrong.

If there is a worse time for something to go wrong, it will happen then.

If anything simply cannot go wrong, it will anyway.

If you perceive that there are four possible ways a procedure can go wrong, and circumvent these, then a fifth way, unprepared for, will promptly develop.

Left alone, things tend to go from bad to worse.

If everything seems to be going well, you have obviously overlooked something.

Nature always sides with the hidden flaw.

It is impossible to make anything foolproof because fools are ingenious.

Whenever you set out to do something, something else must be done first.

Every solution breeds a new problem.

FIGURE 5.2

Murphy's Law provides a tongue-in-cheek guide for security planners.

strategic planning. The reason is topic matter such as relocation of a plant, introduction of a new product or service, a change in the organization's mission and objectives, and similar issues. When the topic involves security, the CSO is most usually invited to participate.

The proposition that a CSO should have a basic understanding of strategic planning rests on a number of simple observations. One is that strategic planning is a consistent element in companies that are successful. Another is that strategic planning is clearly a part of managing. Every leader is expected to understand the nature of planning and to be comfortable in its elements and execution. Yet it's a fact that some leaders have a fuzzy understanding of planning or feel threatened by it. Some indications of the unknowns associated with planning can be found in Fig. 5.3, strategic planning elements.

The gains to be made to a leader personally and to his or her subordinates can be lost when the leader is excluded from strategic planning. A leader who shies away because of poor understanding or dislike of the process is apt to be viewed as a nonplayer. The effect of nonparticipation can be hurtful when the planning involves the leader's sphere of operations.

Strategic Planning Elements

Measurable goals

Specific tasks that lead to measurable goals and assign personal accountability.

Incentives

Rewards that make people want to carry out the plan.

Realistic estimates

Ambitious outcomes grounded in reality.

Incremental efforts

A division of work that organizes a big plan into achievable chunks.

Landmarks

Results-oriented milestones that signify progress according to plan.

Flexibility

A forward view that allows alternative paths and modified expectations.

Focus

A keen eye on the course and a steady hand at the wheel.

Value perspective

A view that looks at the cost of plan execution as an investment.

FIGURE 5.3

These elements characterize effective strategic planning.

Policy and Planning

The relationship between policy development and strategic planning can be described as totally intimate. You can't have one without the other, and although the functions are distinguishable, they are at the same time inseparable.

A policy establishes the arena in which the actions of the business are to occur. It provides a vision for the business and serves as a guide for action. Planning, on the other hand, is the architecture of the arena; it is specific and detailed. To illustrate the difference, the chief executive officer in a retail company might say: "It is our policy to be a main player and tough competitor in the retail industry." One tier down the vice president of sales might say of his or her operation: "Our objective is to meet projections each year of our five-year plan to market new and highly desirable products for customers," and the purchasing manager might say: "Our objective is to acquire the latest in fashions that will appeal to men, women, and teenagers." The CSO might say: "Our number one job is to protect against loss in all its forms such as cashier dishonesty, shoplifting, cargo theft, and internal theft by employees working in all facets of the organization." The company's manager of retail stores might set an objective such as "We will operate with a high degree of customer service relations, maintenance of a reliable inventory, and full stocking of shelves."

All of these statements are likely to include modifiers like "at least possible cost," with "maximum assurance to safety and the ecology," and so forth. But the main point here is that a policy broadly defines the universe of action, whereas planning is concerned with what happens inside the universe.

The reader at this point may want to thump these pages and vigorously point out that a CEO's policy-making function involves more than just issuing a simple pronouncement. And the reader would be right. Policy making is more complicated than that. Policies virtually abound in the corporate environment. They cover staffing, growth, planning, managerial authority, conflicts of interest, marketing, production, finance, facilities, compliance with rules of regulatory boards, termination practices, and many more. Then, too, are the qualitative differences in policies. Some are simply more important than others, giving credence to the term "high-level policy."

The badge of honor in the corporate environment is often the extent to which a leader is involved in policy development. The higher the policy and the extent to which the leader sets it, either entirely or by contribution, is a determinant of status in the formal, corporate organization. In the security field, we see evidences of this concern for status in the number of questions asked of CSOs by senior management, peers in the industry, and salesmen

wanting to market products and services. The inquirers seem to believe that policy decisions go hand-in-hand with the CSO's decision-making powers. These assumptions are not always true, but true often enough for them to be widely held.

It may help to think of policies as many trees in an orchard. The gardener is the CEO. The roots of the security tree spread deep into the organization. Each root is a separate element such as security officer operations, physical security, and investigations. All roots collectively draw nutrients from the soil in the form of funding for labor and equipment. The CEO-gardener is ever watchful for blooms that produce the fruit. If the security tree does not bear fruit, the gardener will investigate and, where appropriate, change the composition of the soil, prune the unproductive limbs, or remove the tree entirely and plant another. When the security services fruit does not bear a sufficient amount of fruit to justify cultivation, the result is replacement of the tree.

The CSO and Strategic Planning

Strategic plans send ripples throughout the whole of the organization. Ripples that impact the CSO negatively can be lessened to the extent that the CSO participated in developing the plan. The degree of involvement by a CSO tends to be determined by three factors. First is where the CSO sits on the organizational chart. If at the lower end of the pecking order, he or she won't have much input. Second is the shape of the organization. If it is a flat organization with only few levels separating the chairman from the frontline workers, the chances for the CSO to contribute are increased. Third is the personality of the CSO. If the CSO is perceived as being inept or uncaring about strategic planning, he or she won't be invited to participate, no matter where located on the organizational chart and no matter the shape of the organization. If perceived as having something meaningful to contribute and willing to contribute, the CSO stands a better chance of being invited into the upper realm.

CRITICAL THINKING EXERCISE

Eighteen months ago, Patrick was hired to be manager of loss prevention for a computer store chain. The first objective of the job was to reduce warehouse thefts. At first, Patrick was the major player in developing and implementing security plans. But as the warehouse theft rate began to decline, the chief operations officer began to complain. The new security measures, he said, were cumbersome and costly. Unfortunately for Patrick, his boss happened to be the chief operations officer. For six straight months, Patrick was not invited to planning meetings. He learned of security-related decisions only after they had been made.

What, if anything, can Patrick do? Create a detailed plan of how you think Patrick should approach this situation.

Business Is Like War

A critical duty of senior management is decide how to efficiently use the company's resources. This duty is not easily discharged under any circumstances and is especially fraught with difficulty in turbulent times. In one respect, business is like war. If the general's grand strategy is correct, any number of tactical errors can be made, yet in the end the war can be won. A tactical error, such as the inefficient use of a company resource, can hurt the company's competitive effort but won't necessarily result in the other side winning. But if the grand strategy is faulty to begin with, even the most efficient use of internal resources will not prevent losing. The ideal situation is to have a correct strategy and to implement it with tactics that are efficient and effective.

If we carry the war analogy a little further, we can say that the general's first order of business is to decide the mission. Are we going to destroy the enemy entirely or do we hurt the enemy to a certain level? What resources do we have at our disposal? This thinking process leads to developing a strategy and a plan, setting objectives and evaluating the effectiveness of planning decisions. These are not matters for men in the trenches; they can only be decided at the top. In the theater of operations, the field commanders carry out the general's orders. Occasionally, the field commanders are called to the general's command post and asked to provide their input. The parallels between war and business are clear.

No Absolutes in Strategic Planning

Strategic planning has common elements in all competitive human endeavors, yet there is no such thing as a standard or universal system for strategic planning. It's not possible to transfer the strategic planning mechanism of one company to another and expect it to work properly. Business organizations, even when in the same line of work, will be different in many key respects, including differences in the nature and the how of planning.

Neither is it sensible to expect that CEO Smith and CEO Jones, given the same premises, will develop closely similar operational plans. Smith may want guards in lieu of sensors, and Jones may prefer sensors over guards. At play also are costs and the preferences of management.

It is no accident that geniuses often occupy senior executive chairs; these are leaders whose intuition and intelligence bring them like cream to the top. Their success is seldom the result of developing a written plan and sticking to it without deviation. They tend to fly on the seat of their pants and make snap decisions intuitively, often relying on a gut feeling, or a flash of brilliant insight. If an organization is managed by a genius, and there are many

examples in high-tech businesses, formal strategic planning will likely suffer, and that may be just as well. But if the CEO is not the intuitive type, strategic planning can be "set in stone." This is not altogether bad, especially for mature organizations. Planning will be formalized, highly documented, based on research and input from many sources, and involve the participation of many people.

Strategy and Change

A change in strategy precipitates changes in policy which precipitates changes in plans which precipitate changes in work practices. The strategy change begins as a snowball that gets larger and larger as it rolls downhill, producing change all along the way.

The CSO must anticipate resistance to change in the security group. "But we've always done it this way" is a common cry heard when work practices change. The old ways of doing things may be so entrenched that even the best-laid preparation will falter. Managing change even under the best of circumstances is hard work. It requires imagination, analytical ability, and fortitude.

To sum up, strategic management occurs at the top and operational management occurs below. Strategic plans are extensions of policy. Policy and plans should be, but are not always, created with input from the CSO, but without exception, the CSO is impacted by strategic plans.

CONCLUSION

Strategy is the direction and scope of an organization over the long term. Its purpose is to achieve advantage through its configuration and deployment of resources to meet or exceed the successes of competitors and gain a deserving share of the marketplace.

A strategy tells employees where the organization should be in the long term; it targets the organization's market and the activities for hitting the bulls-eye, how the organization can perform better than its current status, and what resources are needed to make the strategy succeed. Those resources are often found in finance, resources held, and the technical competence of the workforce. Operational strategy is concerned with how a business competes successfully in a particular market. It makes decisions about choosing between what products or services are to be offered, meeting needs of customers, gaining advantage over competitors, exploiting current assets, creating new opportunities, and containing costs. It is concerned with how each part of the business is organized to meet the goals of strategic direction.

Operational strategy therefore focuses on issues of resources, processes, and people.

The CSO is involved in policy and planning decisions, but more at the operational level than the strategic level.

REVIEW QUESTIONS

1. A CSO operates in a rapidly changing business world. Name and describe three factors causing the change.
2. Explain the concept of due diligence.
3. The CSO is the principal architect of a security strategy that aligns with company goals. The day-to-day execution of the strategy relies for its quality on six imperatives. Name and describe the six imperatives.
4. A policy is broad while plans are detailed and directional. A security group cannot function without a policy and without plans that carry out the policy. Describe the interaction of policy making and planning.

References

Fahey, L., 1999. Competitors. John Wiley and Sons, New York.

Greaver II, M.F., 1999. Strategic Outsourcing: A Structured Approach to Outsourcing Decisions and Initiatives. American Management Association, New York.

Hoenig, C., 2000. The Problem Solving Journey. Cambridge, MAL: Perseus.

CHAPTER 6

Budget Management

What You Will Learn

- Three purposes of budgeting.
- The three tasks that follow the preparation stage of a budget.
- The purpose of a budget audit.
- The role of the budget director.
- Zero-based budgeting.
- The cost/benefit ratio.
- The differences between traditional budgeting and zero-based budgeting.

INTRODUCTION

Heyel (1982) defines a budget as a forecast of all the transactions of an organization for a stipulated period, organized in such a way as to bring to the attention of specific managers the financial results over which they have control and to enable the preparation of financial statements such as the budgeted income statement, balance sheet, and cash-flow statement.

Because a budget sets priorities and monitors progress toward selected goals, it is a basic planning tool. A budget helps a Chief Security Officer (CSO) make informed decisions on the management of people and assets in the security group. Typically, the CSO prepares the budget on the basis of estimates to meet priorities for the next fiscal year. The estimates reflect inflationary pressure and current year spending.

The budget is presented to the CSO's supervisor, who may modify the estimates and rearrange priorities. The supervisor delegates to the CSO formal authority to enter into financial obligations at certain agreed dollar levels. An independent body within the company, such as a financial control group, generally monitors security expenditures to ensure they are consistent with organizational objectives. In any operation of size and complexity, budgeting will be a routine, yet essential, element of planning from year to year.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00006-2

Three purposes of budgeting stand out:

- Estimate the costs of planned activities.
- Provide a warning mechanism when variances occur in actual costs.
- Exercise uniformity in the matter of fiscal control.

BUDGET PREPARATION

An annual budget places on the CSO the responsibility of preparing security group estimates and coordinating them with overall company planning. The CSO and his or her supervisor meet, sometimes with key security group staff present, to discuss planned activities. It is not unusual to begin as early as 6 months in advance of the next fiscal year.

Security budget preparation begins with targets and ends with binding commitments. Outlays and spending authority are usually categorized by functions such as labor, office supplies, travel, estimated costs of investigations, and physical security inspections. New spending requests, even when approved at the next higher level, tend to be critically examined.

Preparation includes obtaining buy-in from groups dependent on or affected by security group activities. Garnering buy-in is typically informal: phone calls, e-mails, memoranda, and one-on-one meetings. The CSO's objectives are to identify essential security services that have not already been addressed and identify objections that may surface later, when the time for patching up has passed.

AUTHORIZATION

Authorization begins by obtaining supervisory approval. Preceding approval may be meetings with peers. Peers head up groups and report to the same supervisor. It is very likely that a peer will be a security services customer and therefore will have a stake in the security enterprise and a right to offer input.

The next step is to present the proposed budget to a budget review committee composed of specialists from the company's finance group. The review committee typically asks to receive the proposed budget for study in advance of one or more discussion meetings to follow. The CSO's budget proposal is detailed item by item and thoroughly documented. Details address objectives, projected activities, purposes and benefits, and likely consequences if activities are not funded adequately.

When the CSO presents the proposed budget in person, he or she uses a combination of negotiation and persuasion. Several such meetings ensue before the budget review committee sends the proposed budget to a higher level for a final decision. The decision will certainly involve the Chief Financial Officer (CFO) and possibly others on the executive team.

CRITICAL THINKING EXERCISE

Jeff Reynolds, CSO of IT Enterprises, worked diligently to prepare his security budget for the upcoming fiscal year. Jeff had noticed that each year he was met with resistance when it came to increasing his group's budget, yet the demands on his staff seemed to be growing exponentially. He felt strongly that without increased financial resources, he would not be able to adequately ensure protection of the company's assets: the employees, the products they produced, or the building itself.

During his first round of peer meetings and phone calls, Jeff cajoled and urged his peers to understand how important it was for his group to gain a larger share of the overall company budget. While his colleagues claimed to understand his plight, they too were jockeying for increased resources for their own departments. Jeff feared he was fighting a losing battle and that his security group would be unable to adequately ensure everyone's safety.

As you read through this chapter, consider what steps Jeff should take in preparation for meeting with a budget review committee. What specific information will they want to see? How can Jeff garner the support of his peers for his security budget?

EXECUTION

The budget process generally begins at the start of the next fiscal year. The CSO's responsibility is to ensure effective and efficient performance of security group functions while at the same time keeping costs in line with the budget.

At some point, the CSO may find it necessary to amend the budget, for example, when an unanticipated event requires the expenditure of unbudgeted funds or when an unusual opportunity presents itself. In the business of security, unanticipated events are the norm rather than the exception. The CSO will send a funding request up the chain of command.

Other amendments can occur. An allowed practice may authorize the CSO to move unspent funds in one account to another account short of funds. However, the transaction must be justified and documented. The practice is not unlike a family that moves money from one planned activity to another. Although formal and closely managed, a budget is in a constant state of change, and not all changes bring added funds. In times of economic stress, the CSO may be required to cut spending.

AUDIT

A budget is audited during execution by the CSO and the company's accounting group. The CSO keeps track of spending almost as it occurs. Every invoice or bill signed by the CSO is copied and placed in a file. Auditing by the accounting group is largely a matter of recording payments made to fund security group activities. A record is prepared monthly. Fig. 6.1 depicts an audit checklist.

When significant variances appear, the accounting group informs the CSO. When variances increase or are not corrected, the accounting group notifies the CSO's supervisor. The security group's budget can also be examined by the company's audit office for one or two reasons: as a routine control measure or as a formal investigation of suspicious irregularities.

THE BUDGET DIRECTOR

A budget director brings all group budgets into a comprehensible whole called the master budget. Heyel (1982) states that a budget is an overall forecast of transactions. These are transactions that occur within a preestablished period and are presented at intervals to senior management in time for decisions to be made to change or remain on course. The master budget is the principal tool for enabling the preparation of financial statements such as the income statement and balance sheet.

The process of budget preparation at the group level adheres to a methodology specified by the budget director. Group leaders identify and justify their planned activities and estimate costs. The format and dollar figures of proposed budgets are developed according to a common framework. Without it, the auditing function would be hampered and the master budget difficult to comprehend.

FIGURE 6.1
The auditor's checklist can provide indications of variances in the security department's budget. *iStockphotos.*

The prescribed methodology of the common framework and the actual budget are two different things: the first is a tool and the second is the object crafted by the tool. A budget is purpose-driven and function-conscious. The form of budgeting specified by the budget director will correspond to organizational goals and functions necessary to reach them. Selection of the budgeting approach can be influenced also by history and experience tax implications, and the preferences of the executive team and the board of directors. Major spending decisions can be made at the board level but are most often made by the executive team. The budget director reports to the CFO, a member of the executive team.

ZERO-BASED BUDGETING

Zero-based budgeting starts with an assumption that zero dollars are available. Dollars become available when proof is presented that an activity is necessary to the business. Implied in the approach is a requirement to explore alternatives for achieving less effective results at a lower cost. Group leaders, including the CSO, make their case by answering three questions:

- What is the purpose of the activity?
- What will it cost?
- What is the added value?

Benefits that can be derived from the activity are weighed against cost. The CSO makes the argument that benefits will be lost or that undesirable consequences will come about if an activity is or is not funded at a lesser level.

Zero-based budgeting forces the CSO to look at different levels of effect associated with carrying out an activity such as the options described in Fig. 6.2. The levels may range from minimum to optimum. At each spending level, the CSO would show the costs of the activity, the predicted value, and the effects likely to be experienced by increases or decreases in spending. The CSO could be required to describe the probable outcomes of operating a guard force at different spending levels. The manager's description to the budget committee might appear as shown in Fig. 6.2.

Not shown in Fig. 6.2 is an option to eliminate the security program entirely, which the executive team could very well consider.

Sennewald (1998) adds that whatever the changes required by growth or budget, the point of organization remains to service the interest of the department in getting the job done through an intelligent division of tasks and the establishment of clear lines of authority.

Guard Force Operations

Option 1: Operate at an Optimum Level of Security

This level of activity for guard service at the Corporate Tower includes coverage on a 24-h basis with guard positions as follows:

- Security supervisor.
- Console operator.
- Front desk officer.
- Office area patrol.
- Garage patrol.
- Cleaning crew patrol.

Guard service functions at the optimum level of activity include the following:

- Immediate response by an experienced supervisor to serious incidents such as fire, bomb threats, injurious accidents, illness, and violence.
- Uninterrupted monitoring of console equipment (such as CCTV monitors, access control and intrusion detection alarm systems, and fire alarm systems) and the initiation of immediate requests for assistance from fire and law enforcement departments and emergency medical treatment agencies.
- Prompt processing of visitors to the Tower.
- Prompt opening of locked offices and conference rooms with use of the security officer master key.
- Identification and immediate correction of safety and security hazards in the offices areas, such as electric heaters and coffee makers left on and access control doors propped open.
- In building evacuation situations, assistance to fire wardens such as directing employees down stairwells, carrying incapacitated or injured occupants to safety, and directing street traffic to allow deployment of fire trucks around the Tower.
- Prevention of assault, theft, and vandalism in the Tower garage.
- Escorting contract janitors while they work on floors containing sensitive information.

The total annual cost for this level of activity is $1500,000.

The effects of operating at the optimum level are as follows:

- Security officer manpower will be sufficient to meet increasing security demands such as those now being made by the recently formed Research and Development Group.
- The company will be in compliance with City Fire Code in respect to emergency evacuation of the Tower.
- Employee complaints alleging lack of security in the garage will be reduced if not eliminated.
- The risk to sensitive information posed by unaccompanied janitors will be eliminated.

Option 2: Operate at the Current Level of Security

This level of activity for guard service at the Corporate Tower includes coverage with guard positions as follows:

- Console operator.
- Front desk officer.
- Office area patrol.

Guard service functions at the current level of activity include the following:

- On-and-off monitoring of console equipment.
- Processing of visitors to the Tower, with occasional delay.
- Opening of locked offices and conference rooms with use of the security officer master key; some delays must be expected.
- Identification and immediate correction of safety and security hazards in the offices.

FIGURE 6.2

This document reflects the relationship between security services and their costs at three levels of operation.

The total annual cost for this level of activity is $85,000. The effects of operating at the current level are as follows:

- Security officer manpower is not able to meet increasing security.
- The company is not in full compliance with City Fire Code in respect to emergency evacuation of the Tower.
- Employee complaints of poor security in the garage will continue. Assault, theft, and vandalism are possible.
- The risk to sensitive information posed by unaccompanied janitors is possible. The cost for offsetting the risk is considerably less than the loss that will be experienced if sensitive information is damaged, destroyed, or compromised.

Option 3: Operate at a Lower Level of Security

This level of activity for guard service at the Tower includes coverage on a 10-h-per-day basis, normal working days only, with guard positions as follows:

- Console operator.
- Front desk officer.
- Office area patrol.

Guard service functions at this level of activity include the following:

- On-and-off monitoring of console equipment.
- Processing of visitors to the Tower, with delays expected.
- Opening of locked offices and conference rooms with use of the security officer master key; delays expected.
- Identification but not immediate correction of safety and security hazards in the offices.

The total annual cost for this level of activity is $65,000. The effects of operating below the current level are as follows:

- Security officer manpower will not be able to maintain a reasonable level of security. Given the number and nature of security reports made in the past year concerning breaches of security (i.e., an assault in the garage, auto theft, auto vandalism, unauthorized entry, and theft of equipment), it is possible to foresee the occurrence of similar crimes, and a failure to address crime with preventive measures can result in civil liability.
- The company will not be in full compliance with City Fire Code in respect to emergency evacuation of the Tower.
- A 10-h day for security operations will very likely result in contract janitors being on the premises with no oversight except that provided by their employer. Theft of assets, including information and equipment, is a possibility.

WARNING: The differential in costs between Options 2 and 3 is insignificant in comparison to losses that would very probably result under Option 3. Also, in the opinion of the CSO, any reduction in security below Option 3 would have nearly the same effect as having no security at all.

FIGURE 6.2
(Continued).

Directions Flow Down

Directions on major budget issues flow from the top down, and requests for funding flow upward. Directions passed downward tend to deal with both administrative and substantive matters. Administrative matters provide guidance as to the format of the budget document, the placement of particular costs into particular categories, the attachment of supporting documentation, and the deadlines for submitting the documentation.

Limitations

Substantive matters can include limitations, such as no new hires, no purchases without prior authority, and no increase of the group budget beyond a certain level (e.g., not more than 5% above the total budget of the current year). Fig. 6.3 points out the differences between traditional and zero-based budgeting.

Traditional versus Zero-Based Budgeting

Traditional	Zero-Based
Oriented to a function or a department	Oriented to programs and projects
How much do you want?	How much do you need for what and why?
Focused on new incremental programs	All programs, old and new, compete for the same scarce resources
Extrapolate past spending	Programs and projects are presented as decision packages
Increment for inflation	Inflation is reflected in the decision packages
Reduce spending by trimming across the board	Eliminate low-ranked packages
Fuzzy linkages to the organization's goals and objectives	Decision packages clearly reflect organizational goals and objectives
The end product is an aggregated set of numbers difficult to understand	The end product is a lean set of ranked priorities that can be changed as circumstances warrant
Internal politics, gamesmanship, selling, and negotiating adversely influence approval	The decision packages speak for themselves
Needed trimming can be offset by deliberately inflating numbers that are difficult to verify	Inflated numbers stand out
In the scramble for scarce resources, the cogency of requests is blurred by emotions	The options are laid open for discussion and evaluation in a business-like atmosphere
At the end, the management decides who gets how much	The end is determined by the persuasiveness of the decision packages
Corporate infighting leads to low morale, turnover, decreased productivity, etc	Personal feelings can be put to the side when decision packages correspond to the organization's goals and resource limitations
Spending is easily monitored and controlled	Spending is easily monitored and controlled. More importantly, decision packages can be evaluated according to results achieved

FIGURE 6.3

Note the differences between traditional budgeting and zero-based budgeting.

A down-and-then-up-again pattern is usually the case before a group's budget is set in stone. The CSO meets multiple times with multiple functionaries. At one meeting, the budget is okay; at the next meeting, it is not okay. At every meeting, the CSO pleads his or her case. Nearly every meeting is called the "final" meeting, which turns out to be not the case. Because the CSO never knows if the next meeting will be the final meeting, he or she has to approach it as if it were a "last chance."

Cost/Benefit Ratio

A request for a major purchase such as a new Physical Protection System may require approval by a spending authority separate from the budget committee. A major purchase not reflected in a budget is called an "exception to the budget." A preparatory step in considering a large expenditure is to determine the cost/benefit ratio, a figure computed by dividing costs by benefits. For example:

- A new access control system costs $500,000 to implement.
- The service life of the system is 10 years.
- Guards replaced by the system result in a saving of $100,000 per year.
- The cost/benefit ratio is therefore 0.5:1, meaning that the cost of the purchase is half the benefits or that the benefits are twice as great as the costs.

The ratio was arrived at by multiplying the annual guard cost savings by the number of years of useful service of the access control system. This figure ($1000,000) represents the benefit and is divided into the cost of the system ($500,000). Benefit versus cost is 0.5. When the ratio is less than 1.0, it is favorable and unfavorable when it is higher than 1.0.

CONTROLLING COSTS

Regardless of the budgeting method used, cost control is inevitable. Each method has its advantages and disadvantages. The method selected is not always based on achieving a match between the method and the nature of the business. It is not unusual for a budgeting method to be selected on the personal preferences of a senior executive such as the chief executive officer or CFO. Apart from the process of budget preparation and approval is the day-to-day task of maintaining a budget folder. This folder is informal and a device of convenience. Placed into the folder are invoices, statements, price quotes, purchase orders, sales receipts, notes and memos concerning expenditures, and like items. Monthly, the accounting group sends to the CSO a computer-prepared summary that:

- Reflects spending for the previous month and year-to-date.
- Compares those figures against the budget's planned expenditures.
- Highlights variances. The CSO is expected to take action when actual spending exceeds planned spending by a significant amount. The action is to put a brake on spending, if possible; if not possible, the CSO submits a request to increase the budget, a request that is never warmly received.

OVERSPENDING

Overspending is frequently the result of poor planning. Failing to anticipate rises in the costs of essential products and services or incorrectly calculating how many and how much of each will be needed is somewhat forgivable. Underspending for a budget item is rarely a problem; overspending is an indication of poor money-managing skills. Figs. 6.4–6.7 show various forms used to track and control spending.

Overspending is occasionally unavoidable, for example, a major investigation comes up. Although a reasonable amount of money is included in the budget for meeting normal investigation costs, that amount is not nearly enough to cover anticipated costs to pursue the new and large investigation. The CSO would go back up the budget line of command to request added funds. If the CSO is smart, he or she will ask for approval to spend whatever is necessary. The answer is likely to come back: "An increase in the amount of X dollars is approved. If you need more at a later time, apply again."

On the following pages, you will find examples of common budget reports.

CRITICAL THINKING EXERCISE

Kurt Kruger is the lone security professional employed by Sparling Oilfield Supplies located in Odessa, Texas. Sparling is one of several US-based subsidiaries owned by a French firm that has a headquarters office in Houston. Kruger reports to Stan Holloway, head of a two-person legal department. Holloway reports directly to Sparling's CEO, a Frenchman named Pierre Duchesne.

Odessa is the center point of an oil boom. A half-dozen small to medium-size drilling companies are operating 24 hours a day, hoping to be next in tapping into a huge reservoir of crude oil that lies beneath the sandy soil of Odessa. Sparling sells drilling bits, pipe strings, valves, and other supplies to the drilling companies. One in particular is Durango Drilling.

Sparling's auditor visits Kruger and tells him documents reflecting sales of supplies to Durango and accounts receivable documents appear to be false. The dollar amount involved, according to the auditor, is in the range of $5 million.

Kruger pays all of his budgeted investigation funds to pay for the services of a private investigator (PI) who had once been the Chief of Detectives for the Midland Police Department. The PI tells

BUSINESS EXPENSE REPORT

Employee Name: Title: Department: Building:

Phone/Extension: Supervisor: Purpose of trip:

Date	Description	Tickets	Hotel	B'fast	Lunch	Dinner	Trans.	Entertain	Misc.	TOTAL
	SUBTOTALS									
									LESS EXPENSE ADVANCE AND CHARGES TO COMPANY	
									TOTAL DUE ME (COMPANY)	

Employee Signature: Title: Date:

Approval Signature: Title: Date:

FIGURE 6.4

Business expense report.

AUTO EXPENSE REPORT

Employee Name: Title:

Phone/Extension: Supervisor: Month of:

Date	ODOMETER START	ODOMETER STOP	MILEAGE X .35	GAS/OIL	PKG/TOLLS	MISC.	TOTAL
		TOTALS					
						LESS CASH ADVANCE & CHARGES TO COMPANY	
						BALANCE DUE ME (COMPANY)	

IF SUBMITTED AS AN EXPENSE REPORT, ATTACH RECEIPTS AND SIGN BELOW		
Employee Signature:	Title:	Date:
Approval Signature:	Title:	Date:

FIGURE 6.5
Auto expense report.

WEEKLY TIME SHEET

WEEK ENDING:

Employee Name: Title:

I.D. No: Status (Temporary, nonexempt):

Department: Supervisor:

DATE	START TIME	END TIME	REGULAR HRS.	OVERTIME HRS.	TOTAL HRS.
		WEEKLY TOTALS			

Employee Signature: Date:

Supervisor Signature: Date:

FIGURE 6.6
Weekly time sheet.

Kruger he has learned that Duchesne is transferring large amounts of drilling supplies to Durango "on the cuff." When Durango reaches the oil reservoir and begins production, it will pay for the supplies at the usual prices, plus 50%. The 50% will go into Duchesne's pocket. In order to verify the PI's findings and gather evidence to establish a case, Kruger needs funds. He goes to Holloway, his boss and head of the legal department, briefs him, and asks that funds be added to the security budget to pay for the services of a certified forensic auditor and further out-of-house work by the PI. Holloway refuses because Kruger had not asked approval of a budget increase before hiring the PI and admonishes Kruger for not properly managing his department's budget.

Without tipping his hand, Kruger talks to nonsupervisory employees in the sales department and accounts receivable office. They believe something is wrong but have been afraid to speak out and will not do so now, but they give Kruger copies of questionable sales and payment receipt documents.

Standard practice in Sparling's budget management practices is to allow unspent funds in one budget category to meet expenses in another category. Kruger uses unspent funds in the office supplies

MONTHLY BUDGET REPORT

Spending By Category	Actual This Month	Projected This Month	Actual Year-to-Date	Projected Year-to-Date
Salaries/Benefits/Payroll Tax/Overtime				
Temporary Labor				
Contract Labor				
Monetary Awards				
Travel Expenses				
Rent				
Personnel Development and Training				
Moving Expenses				
Office Supplies				
Office Furniture and Equipment Purchases				
Furniture and Equipment Rentals				
Software Purchases and Maintenance				
Computer Supplies				
Computer Services (Vendor)				
Freight and Express				
Telephone				
Philanthropic and Miscellaneous Contributions				
Professional Memberships and Certifications				
Subscriptions and Publications				
Professional Meetings				
Recruiting and Relocation				
Totals				

FIGURE 6.7
Monthly budget report.

and equipment category to rehire the PI to find out what he can about Durango's purchases and account payables. The PI obtains document copies, plus sworn written statements from two Durango employee-witnesses that confirm the irregular practice. Kruger takes the documents to the Midland Chief of Police and asks for a police investigation. The Chief refuses by saying that the matter is internal to Sparling and Durango and that any investigation by the police would be improper.

Kruger contacts the CEO at Durango and is stonewalled. That same day Kruger is terminated by order of Duchesne for not following standard budgeting practices.

What has Kruger done wrong, if anything? What can he do now? Do you think Holloway informed Duchesne of the matter?

CONCLUSION

A budget is a list of all planned expenses and revenues. For the most part, it is a plan for saving and spending. A budget will illustrate trade-offs between expenditures and services or products received in turn. In other words, a budget is an organizational plan stated in monetary terms.

The budget of a company is compiled annually, but not always on time. A finished budget, usually requiring considerable effort, is a plan for the short-term future, usually 1 year ahead. Traditionally, the finance department compiles the company's budget using modern software and technological equipment that allows managers of various departments to list their expected expenses in the final budget.

If the actual figures delivered through the budget period come close to budget figures, this suggests that the managers understand their business and have been successfully driving it in the intended direction. On the other hand, if the figures diverge wildly from the budget, this sends an "out of control" signal.

Zero-based budgeting is a technique of planning and decision-making which reverses the working process of traditional budgeting. In traditional incremental budgeting, departmental managers justify only increases over the previous year's budget. No reference is made to the previous level of expenditure. Zero-based budgeting requires budget requests to be justified in complete detail by each manager starting from zero dollars. Zero-based budgeting also refers to the identification of a service and then committing dollar resources to deliver the service.

REVIEW QUESTIONS

1. Explain the relationship between budgeting and performance targets.
2. Name and describe the three purposes of budgeting.
3. How early might a CSO begin planning the next fiscal year's budget?
4. List two categories that might be found in a security budget.
5. What is a master budget?
6. Describe a zero-based budget.
7. How is the cost/benefit ratio computed?

References

Heyel, C. (Ed.), 1982. The Encyclopedia of Management. third ed. Van Nostrand Reinhold, New York.

Sennewald, C.A., 1998. Effective Security Management. third ed. Butterworth-Heinemann, Boston, MA.

CHAPTER 7

Managing Change

What You Will Learn

- The characteristics of change.
- Teamwork in effecting change.
- Technology and change.
- Organizational politics and change.
- Change on a personal level.

INTRODUCTION

The pace and magnitude of change can be overwhelming at times, according to Bamford (1996). Demands on Chief Security Officers (CSOs) to transition to new ways of getting the job done seem to arrive unexpectedly, often with short deadlines and high expectations of success. Change, like the redesign of the organization's structure and the adoption of advanced technology, also seems to arrive during periods of constrained resources. Although natural and inevitable, change has taken on dimensions of size and complexity not seen before. To manage change effectively, the CSO has to recognize certain truths inherent to change. Among these are the following:

- Change defies the status quo and creates dynamics that have to be managed.
- The processes of change are predictable and transferable as knowledge.
- Change in work practices cannot be achieved without the commitment and willingness of those who perform the work.
- Consultation and collaboration are more effective in carrying out change than is the case with traditional approaches such as issuing directives and monitoring for compliance.
- Change must not be judged by occurrence but by consequences.

Change is a permanent feature of modern management. This may be generational in the sense that older managers have difficulty with change;

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00007-4

younger managers do not. As the older leaders leave, it can reasonably be expected to presume that change will accelerate. Change, then, is part of the competitive fabric.

Impact and Context

Although these truths stand firm, change varies in impact and context. When the Justice Department ordered the breakup of AT&T into "baby Bells," a great shock rippled through the organization, the communications industry, Wall Street, and telephone customers. In contrast, a barely perceptible ripple would follow a decision to switch from employing personal secretaries to employing secretarial pools. Both actions represent change, but change of markedly different magnitudes. The contexts in the two examples are also very different. In the first case, the rules of the game were altered; in the second case, the manner of work was altered. Varying impacts and contexts call for varying approaches. An analytical question-and-answer drill for finding an approach that might work.

- What is the problem that is to be solved by the change? What is the change exactly? What are its dimensions, how amenable is it to implementation and control, and what impact will it have on work processes?
- Who are the significant people? Who will do the implementing and controlling, and who will be most affected by it? Who will be the willing participants? Who will oppose the change? Who are the organization's gatekeepers?
- What other changes are in progress that will impact this change? Will the impacts be positive or negative? Can other changes be incorporated by or linked to this change?

Analysis along these lines can be very helpful in mapping out action steps to engineer the change. The map, or plan of action, is updated as the change evolves. This is because the goal of change is not to attain change for the sake of change but to solve problems. This explains why change is not a one-time event but a process of constant improvement. Rarely can we perfectly solve a problem. Just getting to the 80% level of improvement can be a marvelous reward. But the change process does not stop there; it evolves in form, striving to attain the last 20%.

Working through People

Change can occur only through people willing to accept it and make it work well. The CSO, who is constantly affected by change and who is sometimes the engineer of it, works by necessity through people at all levels of the

organization. Today, it might be a physical security safeguard installed here and a planning idea planted there; tomorrow, it might be counseling caution at one place and recommending action at another. The CSO's influence in the organization is deep and broad, yet at the same time sharply focused on the security group. Discussion with team members (e.g., direct reports and supervisors of key functions) and within teams (e.g., security officer operations, investigations, and physical security) is essential to building a consensus. Fig. 7.1 depicts a meeting between a CSO and a subordinate.

In respect to the organization as a whole, consensus building is much more complicated. Assume for example that parties representing two separate organizations wish to reach an agreement on a mutually beneficial project. Opposition arises when one party is in an autocratic organization and the other is democratic in nature. The gap between "for and against" can reflect management philosophies that are sometimes called "Old School and New School." In some venues, a more recent term is "expectations management."

A meeting to forge the outlines of the project will typically begin with arguments for and against, move to a common ground for agreement, and end with clearly understood objectives and individually accepted responsibilities. The outcomes of the meeting are understood by all to be group owned. Consensus can take time and requires interpersonal skills, which are often possessed by the person slated to be in charge of the project.

FIGURE 7.1

A method for gaining consensus for change implementation usually involves face-to-face meetings. *Istockphotos.*

However, not all meetings will end with agreement. If the gap is large, i.e., both parties are at opposite ends of the spectrum, agreement may never be reached.

Consider, for example, the following anecdote.

CRITICAL THINKING EXERCISE

Security analyst Jim Smithers listened carefully as Alex Harcourt, the company's venerable head lawyer, complained that changes made to reports prepared by security group investigators were omitting facts that he had always relied upon. Harcourt said, "The reports are nothing but blocks, some filled in, some not. Also, my secretary has trouble with the new format and she dislikes it as well."

"I'll take care of it," Smithers replied. He went back to his office and drew up an investigative report form similar to the previous form but still inclusive of the objectionable blocks. Smithers reported Harcourt's unhappiness to and shared the revised report form with Terry Allen, the CSO. Allen was new to the company, was in his twenties, and his prior job was security supervisor at Microsoft.

Allen arranged a meeting with Harcourt, with Smithers present. Harcourt made his position clear: "I like a narrative report. It is easy to read and from it I am able to make judgments of a legal nature. The blocks are confusing and they have to go."

Allen handed Harcourt the revised form and said, "Please take a look at this. It has a narrative section that will summarize in words what the block entries mean."

"I still do not know why you need all those blocks. They are simply confusing."

"Sir," Allen said, "The company has moved to a greater reliance on information technology. All departments are required to make the change. In our case, the blocks allow a person to quickly and easily place the data in a computer where it can be arranged to show current and past histories of offenses by type, assets stolen or lost, loss amount, frequency of losses, and so forth. The blocks are a great time-saver."

Harcourt and his secretary had placed their desktop IT assets in a storage room and had no intention of learning a new method. On the other hand, Harcourt was aware of the company's commitment to IT. He looked at the form again before saying, "Well, the blocks can stay but I want to see more space for a narrative of the incident."

Allen looked at Smithers and asked, "Can the form be arranged as Mister Harcourt suggests?"

"Yes, it can. Also, anytime Mister Harcourt needs an explanation, I will be most happy to talk with him over the phone or visit him in his office."

Harcourt rose from behind his desk and said, "Well, that's it then."

Consider the story in the context of change. Do you believe the agreement will be observed by both parties. If not, who do you think will break the agreement and why?

ADJUSTING TO CHANGE

Teamwork is essential to managing change, and the CSO engenders it via the following:

- Creating an atmosphere that encourages open discussion.
- Persuading, listening, reflecting, and demonstrating flexibility.
- Ensuring that the people who have accepted change-creating tasks possess the requisite knowledge and skills.
- Empowering people to act, giving them trust and encouragement, and supporting them logistically.
- Helping people improve performance of their change-creating tasks by affording developmental opportunities.
- Addressing conflicts fairly and openly and resolving them with integrity.
- Allowing people to learn from their mistakes without fear of punishment.

Team confidence is a natural by-product of the constructive exchange of ideas and assurance that conflicts can be raised and resolved fairly. High confidence and high morale are not by themselves guarantors of good results, however. Success in managing change requires three attributes. First is the ability to create a sense of teamwork and functionality. This involves helping team members do their individual jobs well and in harmony with one another. It also means delegating authority to make task-related decisions. A second attribute is the ability to create within the team a high expectation of service delivery. Excellence is the sole criterion; good work is not good enough. Third is an ability to correctly evaluate team performance. Note also that feedback from the team to the CSO is useful. Security officers, for example, are superb conduits for obtaining evaluations from the users of security officer services. "How are we doing?" is an easy-to-ask question that can produce valuable insights.

Familiar But Not Understood

CSOs as a class are quite familiar with change. Outsourcing, downsizing, and terrorism are but a few of the major changes that in the past three decades have impacted security operations, and the pressure for change continues unabated. Yet, for all of their experience in dealing with change, CSOs do

not commonly share an understanding of it and have not developed a uniform approach to managing it.

In some cases, very necessary change is avoided. For example, the public's demands for high standards in the selection and training of security officers are largely unheeded. A majority of the major companies in the security officer industry resist standards despite the success of initiatives to establish standards. Upgrades in security officer standards have been minor, long in coming, and driven for the most part by exasperated legislatures. Even when change is crucial, it is often resisted, and for the wrong reasons.

Change driven by professional values can enjoy wide acceptance, whereas change driven by forces external to the profession—such as law making bodies and regulatory agencies—is apt to be regarded as impossible to reconcile with professionalism. Whatever the source and however regarded, change demands an understanding of how to make things work for the better.

Poor Approaches

Not knowing how to manage change, the human inclination is to use rewards and punishment. In this approach, the change is announced, implemented with operating procedures, periodically evaluated, revised, and driven by a system of rewards and punishment. This approach rarely works because it ignores the need for workers to understand why the change is needed and how it can impact them personally.

Change is sometimes attempted by running a pilot project. After the bugs have been worked out, the project is launched and propelled at full speed.

Scant attention is given to collateral effects; all that matters is to move forward. The occurrence of change is evidence of success. The consequences of change are forgotten.

Another poor attempt is the copycat approach, which is to replicate change processes used by like organizations. This essentially quick-fix approach overlooks the complexities of change management. Fig. 7.2 points out some dos and don'ts of managing change.

TECHNOLOGY AND CHANGE

Technology has always been a primary driving force of business change. An organization's market, mode of operation, and competitive climate can be radically altered by the emergence of a new technology. Wallington (2000)

Tips on Managing Change

Don't try to control everything all the time.

Focus on the purpose of change.

Avoid changing more than necessary and changing the wrong things. Unnecessary change increases the probability of unintended consequences.

Expend more effort working through cooperative people and less effort overcoming resistance.

Do not rely on structural change to obtain practice change.

Change has value only to the extent that it solves a problem.

FIGURE 7.2

These tips on managing change can be helpful in easing doubts of subordinates.

provides a gloomy scenario. As an agent of change, technology can be called disruptive because it disturbs the status quo, in some cases to the point of threatening an organization's survival. The printing press, steam engine, horseless carriage, flying machine, and personal computer are examples of technologies that were highly disruptive when first introduced.

It is also evident that a technology can be affected by the way in which an organization uses it. Assume, for example, that the CSO purchases a software application that tracks the status and makes a record of each incident handled by the security group. The application works well except that it does not categorize incidents by type, frequency, and amount of loss per category. The CSO learns that other security groups have the same need. The CSO communicates the need to the software manufacturer. The application is modified. This is an example of an organization affecting a technology. Fig. 7.3 depicts new technology affecting an organization with the organization in turn modifying the technology to meet its particular needs.

Technology, whether it precipitates change or affects other aspects of the business, can be profound. Technology places downward pressure on labor. Work done by electronic processes equates to less work by employees. A trend well underway is distributing IT output digitally and directly to the end-user with little or no involvement of workers. Also, the process provides self-service mechanisms to the end-user, which also diminishes the need for labor. Experts point to productivity numbers as proof.

The end-user need not be a business. We see in our daily lives, apart from work, the increasing use of technology to perform functions as simple as opening a can or more complex such as determining the location of children, detecting hazards, and driving automobiles that warn or brake when detecting a possible collision.

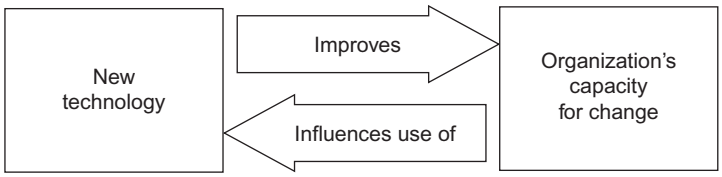


FIGURE 7.3
New technology and the organization interact.

Change induced by technology can be seen as a complete restructuring of how work is performed in this country. It can also be seen as the cause of major national problems such as putting people out of work when unemployment is high, filling technical positions with people from other nations because our educational systems fail to produce people skilled in scientific disciplines, and creating animosity between low-paid, nontechnical employees, and high-paid technical professionals. For the CSO, changes in technology increase the frequency and magnitude of security problems such as theft of valuable information, sabotage, and workplace violence.

POLITICS AND CHANGE

Change at the front end is not like change at the back end. What was first contemplated may bear little resemblance to the final result. The cause can be politics, the process by which people exercise and resist power. We tend to think of politics as an adversarial game played between Democrats and Republicans, which it is, and are unmindful of politics in the business venue. Politics inside a business organization can be invisible yet enormous in effect. It can be a force for driving change, as well as thwarting it. The practice of politics is not limited to the corporate boardroom. It is practiced by people and groups throughout the entire organization. The following is a case in point.

CRITICAL THINKING EXERCISE

Mike Cascio is the Chief Security Officer of Kwal-Buy, a company that owns and operates a thousand convenience stores in a 10-state area. The stores are located in urban areas and are open for business 18 h a day. In the previous five years, more than two-thirds of the stores were burglarized, robbed, or had an assault incident on the premises. Inventory shrinkage by reason of employee and customer theft was a loss producer in all stores. Before Mike was hired as CSO, Kwal-Buy had urged store operators to install anticrime equipment such as drop safes, CCTV, and alarms for duress, robbery, and burglary. Kwal-Buy treated each store as an independent profit center, meaning that if a store chose to purchase security equipment and services the costs came out of the pocket of the store.

In Mike's periodic visits to stores, he noted that many had no robbery and burglary alarms at all, many had partial systems, and some had inoperable or faulty systems. Some stores had overpaid for the equipment and almost all were being charged higher-than-average fees for alarm monitoring services. Mike also noted problems in lighting, obstructed views, and security training of store employees. A common sentiment of the store operator was, "I know that security is important but I don't feel like I should pick up the tab for it."

After comparing security-related loss numbers against security-related costs, Mike was convinced that even a modest improvement in security would more than pay for itself. He consulted with alarm equipment manufacturers and learned that by purchasing a standard system (CCTV/robbery alarm/burglary alarm) in a quantity of not less than 250, the per-system price would be half the average price being paid by store operators. Mike also priced the cost of purchasing, installing, and operating alarm monitoring equipment, for which there was plenty of room in the security center at Kwal-Buy's corporate offices. Quotes obtained from three major alarm installation and maintenance firms revealed that the security center and every store could be serviced uniformly and cost effectively.

The plan that unfolded in Mike's head involved a change outside Kwal-Buy's experience. It went like this. Kwal-Buy would make an initial purchase of 250 alarm systems plus one central alarm monitoring system. Kwal-Buy would hire a firm to install the central alarm monitoring system at the corporate offices and to install the alarm systems at stores that wished to have them. Annual troubleshooting and service would be included. Store operators would not pay for the equipment, installation, or service. They would, however, pay a monthly fee to Kwal-Buy for alarm monitoring.

Mike's calculations showed that if he could institute his program (i.e., the change) in 150 stores in the first year and 100 more stores in the second year he would generate revenues from alarm monitoring services equal to the costs of the equipment, the installation, and the labor involved in manning the central alarm monitoring system. In the third year, the program would generate revenues sufficient to begin returning added value to store operators in various forms, such as purchases of drop safes, improvements to security lighting, security signage, counsel on security practices, and training store employees in loss prevention techniques. Before the end of eight years, accumulated revenues would be sufficient to update/replace existing equipment. Best of all, Mike concluded, Kwal-Buy and the store operators would reduce losses linked to robbery, burglary, assault, and theft.

How will Mike make the change happen? He has had no experience as a change maker but he has watched others engineer change, particularly in the political arena. Mike decides to proceed as if he were a candidate for public office. Winning the office will be his metaphor for effecting the change.

Mike's platform for election is his vision to provide security to stores in a way that rewards everybody. He describes a new practice that will reduce costs and therefore enhance profits. His campaign is the combined efforts he makes to sell the vision. He sells by conferring one-on-one with store operators and corporate managers, making presentations at company meetings, forming and steering a task force, and taking advantage of every opportunity to explain his vision. He develops a standard speech, a highly focused bullet-points memo, overhead transparencies, slides, posters, newsletters, and e-mail messages.

Mike's campaign identifies the supporters and the detractors. He concentrates on eliciting the help of people who are willing and in a position to champion his cause. He gets people involved to a degree that they take a proprietary interest.

Mike has to overcome a natural tendency of people and organizations to cling to the past. The unproven nature of Mike's vision is unsettling to some and downright heresy to others. Election day is around the corner, and Mike is concerned. He conducts a poll by talking personally to his constituents, many of whom he has calculatedly pursued from the start. They were targeted early on because they held authority, either formally or informally. These are the movers and shakers and influence makers. Mike worries some will lose their enthusiasm.

Election day arrives and, hallelujah, Mike gets the nod to move ahead. He has planned for this day. Potential problems in execution have been anticipated and put to rest. Mike knows, however, that a single misstep can be fatal to the attainment of his vision and thus he treads carefully. Contingency options are in place to sidestep obstacles. He worries most of all about the candidates he has defeated. Will they continue to oppose him? Mike knows he will be watched and that some of his opponents may be looking for opportunities to sabotage his efforts, but he takes none of this personally.

He decides to move slowly at first and pick up speed gradually. He will know when the time has passed for the go-ahead to be cancelled. He wants to get to the point of no return quickly, but not at the risk of losing the support that has brought him this far. He will need to enlist more allies and not be stalled by detractors.

What comparisons can you make between delivering change in a business environment and delivering on campaign promises. Mike has detractors. How are they likely to undermine Mike's efforts? In your opinion, what is the organizational structure of Kwal-Buy? Explain what brought you to that opinion.

CHANGE ON A PERSONAL LEVEL

A CSO deals with change on a personal level by first recognizing three immutable characteristics of change: it is a fact of life, unpredictable, and not controllable by any one individual. Dotlich and Cairo (1999) hold that without an understanding of these characteristics, the CSO's career might be in jeopardy. Getting out of the way of change may be the CSO's best or only choice. In other cases, there may be opportunities to be a part of the change by influencing it. If the change involves altering the way a security group operates, the CSO has (or should have) an opportunity to influence the nature of the change and how it will be implemented. This is certainly better than watching from the sidelines.

Reality Check

The CSO should make a serious reality check when faced with change. He or she has to know the answers to questions such as "What do I believe in?" "Does this change impact my belief system?" and "How do I fit into this change and do I have a positive part to play?" Coming to grips with the personal implications of change can be traumatic.

When not able to substantively control the personal consequences of change, the CSO can at least control his or her personal reaction to it. A career-damaging change can occur despite the best efforts to the contrary. A change perceived incorrectly as career damaging may turn out to be career damaging simply because of the perception. When looked at free of exaggerated fear, change may look more like a bump in the road than the end of the road. The message here is to take control of the things that can be controlled, such as one's personal response.

Blame Shifters

The people most affected by change on a personal level seem in many cases to be blame-shifters. The usual laments include, "The boss had it in for me. The company deceived me. Lady Luck was against me." They are self-doubters who end up failing because they fear success. They tend to undervalue their talents and destroy their chances of getting ahead. The losers in change are sometimes people who are so locked into their own identity they cannot tolerate working differently. Change to the job is unacceptable because the job and the person are one and the same. "They wanted me to be the fleet manager when I was already the head of security. They can't do that to me." But they did.

Survivors

The survivors are people who have come to grips with change in a healthy way. They see it as a discovery, a renewal, and a challenge. They manage to retain their visions of personal success while accommodating the demands of the new situation. Theobald (1997) says of survival: "We've got two choices: to move into this new system, or to let things get worse. The one thing excluded is the middle—we're not going to stay where we are."

Action Coaching

A means of bringing individual talents and skills into harmony with change is action coaching, a technique favored by Dalton (1998). What differentiates action coaching from other forms of coaching is its emphasis on behavior modification. Performing below expectations and interacting poorly with team members are examples of behavioral problems that can be addressed by action coaching. The broad objectives in action coaching are as follows:

- Bring personal goals into line with company goals.
- Help employees adapt to changes in work procedures.
- Encourage employees to achieve their full potential.

FIGURE 7.4
Action coaching is a means for surfacing employee problems and finding solutions. *Istockphotos.*

A beginning step for the action coach is to determine the modification needed and to assess how the modification fits into the big picture. Fig. 7.4 depicts the action coach and an employee engaged in a discussion involving a change in behavior. In shorthand, determine the change and the context. Assume, for example, that Harry Blake works for you and supervises five people. You detect a tension between Blake and his subordinates. The tension results in the main from Blake's lack of skill in dealing with people generally. That is the problem. You know that the CEO is committed to establishing and maintaining harmony in the workforce. That is the context.

Questions naturally pop into your mind: What is it that needs to be done to modify Blake's behavior? How long will it take? How difficult will it be? Will the modification be worth the effort? What opportunities are available to make the modification?

You decide you need more information and therefore meet with the manager of the HR department. You learn that the company offers an intermediate-level supervisor course that includes training in team building. Blake is eligible to attend and you have the funds in your budget to pay the attendance fee. The HR manager urges you to confer with Blake, inform him that he is not meeting the company's expectation in respect to working in harmony with others, obtain his feedback, and then develop with him a plan for correcting the problem. You are advised to insist that Blake take personal responsibility for improvement, which would include successful completion of the training course. Be sure also to document everything the HR manager

counsels, including details in Blake's performance that first brought the problem to your attention.

Back at your office, you work up a script you intend to use when you meet with Blake. Included in the bulleted points are the following:

- Ask him to state the personal goals he hopes to achieve through his employment with the company.
- Ask him if he feels the company has helped him in the pursuit of those goals.
- Ask him if he feels the company has given him the training and coaching he needs to be effective in working with other people.
- Ask him what he has done personally to develop his people skills.
- Be open-minded. Listen carefully. Think before talking.
- Get in touch with his mood and tone. Get him to restate his responses. Use phrases such as "I guess what you are saying is. . . ."
- Keep the focus on him. Make sure he understands he has a problem and that the solution belongs entirely to him. Offer help, such as the training course.
- Get him to commit to modifying his behavior. Use phrases such as "What are you going to do to turn this situation around?"
- Establish milestones and a deadline for correcting the problem.
- Look for red flags such as the following:
  - Reluctance to commit to a plan of action.
  - Insistence that the problem does not exist or is minor or will go away of its own accord.
  - Blaming others.

The meeting with Blake turns out to be nonconfrontational. He is shocked at first and then mildly angry with himself for not recognizing the problem. He agrees to self-evaluate during and after transactions with coworkers, readily agrees to attend the training, and expresses confidence that he will do better. An action plan is developed and he commits to it.

After Blake leaves, the CSO considers the need for involving other people. He asks himself: "Will it be helpful to Blake and to the correction of the problem if I brief the boss?" The CSO thinks yes. "If a complaint is lodged against Blake over my head, the boss will understand that the problem is in a correction stage."

The CSO is pleased overall. He prepares a file folder on the matter and adds to it a reminder to monitor Blake's performance to ensure the plan is carried out. He will look for specific changes in Blake's behavior that indicate improvement and decide as events move along if further counseling and motivation will be needed.

REVIEW QUESTIONS

1. Six "truths" are said to be present in the management of change. Briefly describe each of them.
2. What is "group ownership?"
3. Name and describe the three broad objectives of action coaching.
4. How can a CSO deal with change personally?

References

Bamford, T., 1996. Managing Social Work. Tavistock Library of Social Work Service. Tavistock, United Kingdom.

Dalton, D., 1998. The Art of Successful Security Management. Butterworth and Heinemann, Boston, MA.

Dotlich, D.L., Cairo, P.C., 1999. Action Coaching: How to Leverage Individual Performance for Company Success. Jossey Bass, San Francisco, CA.

Theobald, R., 1997. Reworking Success: New Communities at the Millennium. New Society Publishers, Gabriola Island, BC.

Wallington, P.M., 2000. Total Leadership: Making Change. CIO Magazine, April 2000 Issue, Framingham, MA.

CHAPTER 8

Making Decisions

What You Will Learn

- The six stages of framing an issue.
- The five stages of implementing a decision.
- Using feedback to compare results against achievement.

INTRODUCTION

Leadership, certainly effective leadership, is all about making good choices. When the stakes are high and a consequential decision required, business leaders place a greater reliance on logical processes than on instinct and intuition. Diving headlong into the fray fits the leader-hero image but is rarely practiced in modern business. A more accurate image may be the jet liner pilot who relies on a standard process involving flight charts, electronic instrumentation, a copilot, and a navigator.

Sennewald (1998) is highly critical of leaders who are unwilling to make decisions clearly. Doing so reflects a lack of self-confidence or a fear of making the wrong decision. A key leadership responsibility is to give direction. Failure to act, let alone act in a timely fashion, is a serious deficiency that breeds frustration and a "don't give a damn" attitude among subordinates.

Not all important decisions are made by upper-level leaders and are often made "spur of the moment." An example is US Airways pilot Captain Sullenberger deciding to land his failing aircraft in the Hudson River, saving hundreds of lives.

It happens sometimes that several decisions may need to be made to resolve a single issue. A fire chief may need to make "on the spot" decisions about whether to send firemen into a burning building or extinguish the fire with hoses deployed outside of the building. An information technology manager faced with a problem of protecting back-up media may have

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00008-6

to decide on what types of media require storage, where the media is to be stored, and how it is to be retrieved when needed. A Chief Security Officer (CSO) faced with the problem of ineffective intrusion detection will need to make a combination of decisions relating to types of fencing, types of security lights and placement, types of sensors and their placement, type of closed circuit television (CCTV) system, composition of a security guard force, and a strategy for responding to suspected intrusions. To compound the problem, the CSO will need to decide how to make all these elements work in harmony with each other.

These types of decisions are important but are tactical in nature. This chapter will deal mostly with strategic decisions that affect the business as a whole.

A DECISION-MAKING STRATEGY

Harris (2009) makes the point there are often many solutions to a business problem, and the task is to choose one of them. The task can be simple, complex, or somewhere in between. The number and quality of decision alternatives can be adjusted according to the:

- Importance of the problem.
- Time available for solving the problem.
- Cost involved with each of the alternative solutions or combinations of them.
- Availability of physical resources and knowledge of persons tasked to provide input and the person tasked to make the final decision.
- Personal psychology, preferences, and values of the decision maker.
- This is a strategy of choosing the best possible solution to the problem, discovering as many alternatives as possible, and choosing the very best among them.

When the consequences of a decision are high, a good business leader will set aside personal judgments in favor of a process utilizing the analysis of facts. Many such processes exist in the modern business world, yet all of them include six basic stages. Fig. 8.1 lists the stages:

- Frame the issue
- Collect information
- Analyze information
- Decide
- Implement
- Examine feedback

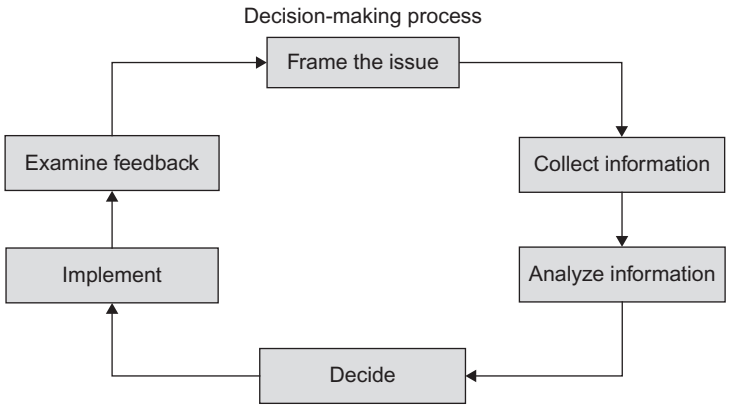


FIGURE 8.1
The six stages of the decision-making process move in a cycle that by theory does not end.

Frame the Issue

The process begins with defining what must be decided. If the decision involves solving a problem, one starts by investigating the essential nature of the problem. The questions to be preliminarily answered include the following:

- Does a decision need to be made at all?
- What is the crux of the issue? What are its dimensions?
- What impact will a decision have on other issues?
- Is the issue real or imagined?
- Who are the persons or groups best able to contribute to the best decision?
- How long will it take and what will it cost to arrive at and implement a decision?

Plunging in and trying to solve the wrong problem is a common error, and one that can be avoided by taking time to look at the issue from several angles and through the eyes of people positioned to understand the facts. The diagram in Fig. 8.2 abstractedly depicts criteria that can affect a decision. Some criteria will reach the decision-making point and some will not. We can equate all the criteria to assumptions. Some assumptions will reach the center of the web and some will not. Theoretically, the assumptions that get there are those that will shape the decision. The decision may turn out to be bad, suggesting that the assumptions were not accurate after all and that some of the discarded assumptions may be worth considering again.

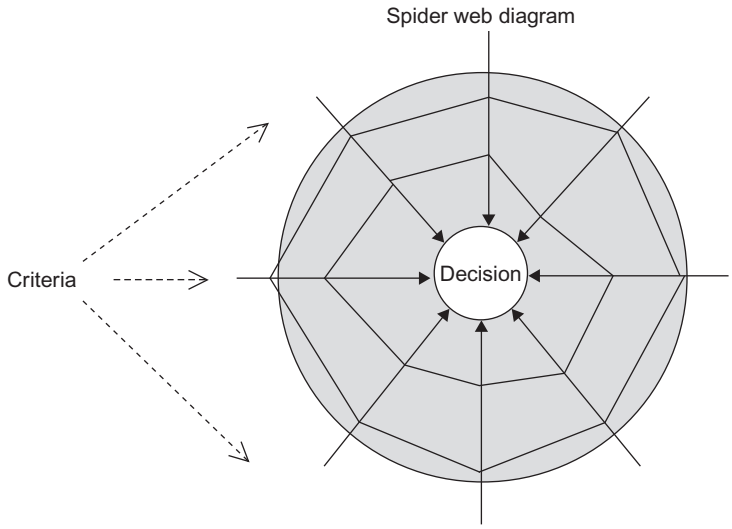


FIGURE 8.2
The Spider Web Diagram can help the decision maker visualize the many variables that can go into a single decision.

It is not too early in the decision-making process to think of possibilities. A good method for generating new ideas and assumptions is brainstorming. When properly conducted, a brainstorming session will encourage creative ideas and bring to the surface assumptions not identified in the usual manner. A lively and uninhibited session can bring out opposing views which can become supporting views or rejected out of hand. Putting innovative and contrarian minds to work can help clear away the fog of uncertainty.

Collect Information

The second stage of the process involves gathering information, including the hard facts and the best estimates. The good decision maker will draw a clear line between what is known and not known and seek to obtain the missing information.

Decision trees and hypothetical scenarios can be used to identify missing data and search for mental blind spots. Estimates of variables can be made and then challenged such as estimating a cost and then critically examining it. Tabletop exercises and hands-on practical exercises can be used to surface information that is needed but missing.

All avenues should be explored for collecting relevant information. If relevancy is in question and subsequently shown to be irrelevant, the information should be shelved or discarded. Information deemed to be relevant should be correlated or grouped in a common subject area such as topic, source, reliability, or other criteria.

Analyze the Information

At this stage, all the obtainable relevant information will be on hand and ready for analysis. For analysis to be accurate, the information has to be in a common data set. It is confusing to compare apples against bananas. The most common data set is dollar values. With a common data set established, the data are quantified and then systematically evaluated.

The methods of evaluation vary according to the nature of the information and the practices and resources of the decision maker. Analytical tools include linear modeling, sensitivity analysis to highlight uncertainty, value and probability analysis, decision trees to display relationships between alternatives and outcomes, and ranking of probable outcomes. Mistakes at this stage of the process typically include the following:

- Taking mental shortcuts such as giving greater credence to the most recent or most loudly voiced opinions.
- Wasting valuable time by considering irrelevant information.
- Being overly confident about the quality of information.
- Relying on information that confirms predetermined expectations.

Emerging from the results of the analyses are the outlines of alternatives, singly and in combinations, which if carried out correctly can achieve the decision-maker's objectives. Said another way, the problem is described by its solution.

Decide

In this stage, the solution is described by the corrective actions (i.e., options deemed capable of solving the problem). An option consisting of corrective actions is selected, and a decision is made to proceed with implementation. However, the decision should not be rushed.

We may think that decisions are consensual, but the truth is they are made by individuals acting alone. Yes, the decision maker may by relying on facts provided by others, but in the final analysis, it is his or her call to make.

Implement

The selected option is put into effect. Implementation of a major decision is rarely made all at once. It typically proceeds in stages, with each stage building on previous stages. The first stage is likely to be preparation.

- Developing a plan of action.
- Establishing milestones and deadlines.
- Acquiring and assembling needed equipment and supplies.
- Selling the option to employees.
- Training employees in the knowledge and skills necessary to smooth implementation.

Examine Feedback

Feedback, meaning information arising from the effect of carrying out the option, is carefully examined in light of the anticipated outcomes. In other words, implementation is compared against results. When the results are less than satisfactory, the decision maker can modify implementation or decide to go with an entirely different option.

Assumptions and reasoning are confirmed or invalidated by feedback, allowing new insights. The nature and dimensions of the problem may turn out to be different than first perceived, and the criteria that went into shaping the option may have been off target. Feedback naturally leads to a reexamination of the problem and the facts that were relied upon to solve it.

When the results of implementation are significantly poor, a natural tendency of the decision maker is to transfer guilt by refuting mistakes and rationalizing choices. The decision maker can go into a state of denial that if not overcome will be an obstacle to finding the correct answer.

Another common misstep is to settle for minimally acceptable outcomes instead of returning to the drawing board for another try at getting it right. Frustration of the decision maker and the bellyaching of detractors can make it attractive to put the entire issue aside and move on.

IMPLICATIONS FOR THE CSO

The decision-making process at the security group level can be, but is rarely a formal process such as that used in making strategic, major business decisions. Here is an example of the CSO using the same five-step process used by senior management.

Assume the CSO is faced with a problem of unauthorized persons entering restricted areas. The CSO needs to know who will argue there is no problem at all and who will argue the opposite, and the CSO needs to know the cost implications of solving the problem. The CSO will also want to know if solving the access control problem will cause a problem elsewhere, sort of like closing one door, and causing another door to open. Essentially, the CSO has framed the issue.

The CSO then gathers information, which may be to call a meeting of security group employees and ask for their input. A number of answers or possibilities are raised and potential difficulties discussed. The CSO has collected information.

The next step is for the CSO to analyze the collected information. He considers the possibilities, which in this case are as follows:

- Install an electronic access control system.
- Place a security guard at the entrances to restricted areas.
- Install high-security mechanical locks on doors to restricted areas.
- Do nothing.

The CSO is now at the decision point. He or she decides that placing guards at entrances than is expensive over the long term and that doing nothing is really not an option. The CSO is left with choosing between an expensive electronic access control system which he or she believes will be more effective than less-expensive high-security mechanical locks. The CSO does not particularly like the locks option because prior experience has shown that keys get lost and compromised, which in time will require the lock cores to be recombinated at considerable expense. The CSO decides to ask the chief executive officer (CEO) to make funds available to purchase and install an electronic access control system. The CEO says no because the company is facing a shortfall in revenue. The CSO then offers an alternative: high-security mechanical locks. The CSO approves. The CSO has made a decision, or more accurately, the decision has been made for the CSO.

The locks option is explained to the employees affected by it, and the locks are installed by a company chosen by the CSO, with a completion date established and a fair price negotiated. The decision has now been implemented. All that remains is to see if the decision works. Step five, feedback, will give the answer.

Some employees complain the locks slow them down and a few complain because when they leave their key at home, they must wait until a guard arrives to open the door. A majority of affected employees say nothing at all, which causes the CSO to believe the action worked, at least to an acceptable degree.

CRITICAL THINKING EXERCISE

In a sense, David was a survivor. He had kept his job as CSO after the company was purchased by another company, and he had seen change after change while managing to keep intact a security group that was largely his own creation. The core of David's group was an in-house guard force that provided security services at the corporate headquarters. David had long ago decided that an in-house guard operation was the best choice for the company, and in some respects, he was right. The guards performed very well, they were loyal, and turnover was low.

The previous CEO had agreed with David, stating that he wanted the guards to be in the corporate family. The new CEO, however, had reservations. Last week he commented that guard costs were much too high. Today he called David and said he wanted input for a decision he would make concerning the future of the security group. He specifically asked for cost estimates to outsource guard operations. He also suggested that David might want to consider forming his own guard company and making a bid for the contract.

Should David describe to the CSO the negative implications of switching from a proprietary guard force to a contract guard force? Should David suggest that he be retained in his current position and, among the other functions he performs, ensure the contract guard company meet specifications established by David. Should David form his own guard company and make a bid for the contract? Is there any other action that David might take?

CONCLUSION

As a business grows, effective decision-making becomes much more complicated. Leaders find it difficult to get all of the information they need. In addition, they are unsure as to how their decisions on hiring, firing, purchasing, and other issues will affect the morale and productivity of employees and relationships with investors, lenders, vendors—not to mention customers. The truth is leaders cannot always choose strategies that will maximize profit and at the same time satisfy everybody. Instead, they tend to take a less risky path and settle for what they consider reasonable gains. According to Simon (1999), this observation contradicts conventional economic analysis, which assumes that a company always tries to maximize profits, without regard of other factors.

REVIEW QUESTIONS

1. Decision-making can be seen as a sequential process that moves through six stages. Name and describe them.
2. Name and describe four common mistakes that can be made by a decision maker when he or she is considering input prior to making a decision.
3. What are some of the steps to implementing a decision?
4. What does "quantifiable format" mean?

References

Harris, R., 2009. Introduction to Decision Making. Virtual Salt. Retrieved from www.virtualsalt.com/crebook5.htm (accessed 09.01.10).

Sennewald, C.A., 1998. Effective Security Management. Butterworth-Heinemann, Boston, MA.

Simon, H.A., 1999. Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization. fourth ed. Free Press, New York.

CHAPTER 9

Managing Risk

What You Will Learn

- Reasons to perform risk analysis.
- Ways to manage risk.
- How and why to use countermeasures.
- The value of self-assessment.
- Procedures for conducting a security audit.
- Procedures for conducting a security review.
- Actual and potential threats confronting critical assets.
- The seven steps of risk assessment.
- Five opportunities for managing risk.

INTRODUCTION

The view of Daniell (2000) is that we are now living in a world of rising risk and increasing volatility. Everywhere, we seem to encounter increasing and intensifying risk. Risks of concern to security professionals include:

- Terrorism
- Workplace violence by disgruntled employees
- Crimes against company assets and employees by outsiders
- Theft Of Intellectual Property
- Fraud—Embezzlement Or Misuse Of Funds
- Damage To Company Physical Property

The management of risk is a fundamental responsibility of all managers, especially the Chief Security Officer (CSO). The CSO directly manages risk within the security group and indirectly manages risk in other groups by setting security standards, educating employees to meet the standards, providing counsel and advice on security matters, and helping in the development of contingency plans.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00009-8

RISK ANALYSIS

Risk analysis is a multipurpose tool that can help the CSO:

- Identify assets deserving of protection.
- Identify threats to the assets.
- Estimate the probable frequency of occurrences.
- Estimate the probability that threats will materialize.
- Estimate the impact of threat occurrences.
- Assess the manageability of threats.
- Identify countermeasures that prevent or mitigate threat occurrences.

Assets

The assets to be protected can include employees, contractors, customers, buildings, equipment, supplies, money, information, reputation, and others. Another asset is process: a rational combination of people and properties working together to produce an output. Outputs can be products, such as refined sugar, mass-manufactured automobiles, or services such as real estate sales and legal advice.

Criticality

In risk management, criticality is a characteristic of an asset in terms of loss. Loss includes destruction, damage, and deprivation of use. Loss is often expressed in dollar values. The dimensions of criticality include cost of replacement, availability of replacement, and importance to a process.

Consider the following two scenarios. A lightning bolt strikes one of 30 tanks in a gasoline tank farm. The tank catches on fire, which destroys 50,000 gallons of gasoline and damages a connected pipeline. The facility is shut down for 2 days. Destruction, damage, and loss of use costs the company $200,000.

In the second scenario, disgruntled workers at a petroleum refinery sabotage the plant's catalytic converter, shutting the refinery down until a replacement converter can be purchased and installed. Again, we have destruction, damage, and loss of use. The destruction and damage costs at the refinery are less than $50,000 because the catalytic converter is not expensive and the cost of repairing the damage is minor. Because the converter is essential to the refining process, loss of use of the entire plant is extended until a replacement converter is acquired and installed.

The tank farm goes back on line in 2 days. The petroleum refinery does not have a backup converter and has to order one from the manufacturer. The

manufacturer promises delivery in 2 months; installation and testing require 1 month. The refinery is out of operation for 3 months. Loss derived from a complete absence of productivity for 3 months is in the million dollar range.

The cost of destruction and damage at the tank farm is significantly higher than that at the refinery. However, the overall cost for the refinery is much higher than that for the tank farm because the shutdown time is much longer. What we now see are the dimensions of criticality: cost of replacement, availability of replacement, and importance to a process. But we also see variations in those dimensions.

Threats

A threat is an indication, circumstance, or event with a potential to cause destruction, damage, or loss of use of an asset is an incontrovertible view held by DePasquale (1993). Threats vary and fall into two categories: acts of nature and acts of mankind. In the scenarios presented previously, the tank farm fire was an event triggered by Mother Nature; the sabotage at the refinery was an event caused by a human act.

Hurricanes, floods, and earthquakes are events caused by the forces of nature; terrorism and crime are caused by people. All of these events are threats because they are indications of possible occurrence. The storm that sent the lightning bolt against the gasoline tank was an indication; sabotage at the refinery was indicated by employee unrest.

Terror-related threats are indicated by the history, intention, and capability of a terrorist group. History is apparent from the group's past activities, intention is shown when the group declares it will assassinate expatriate employees, and capability is demonstrated when the group succeeds in doing what it said it would do.

Probability

The essential question seeking an answer is: "How likely is it that a particular threat event will take place?" Estimating the probability of occurrence has no reliance on mathematical models, equations, or formulas. Precise numerical quantification is never possible when the factors under examination are influenced in the main by human behavior. A good deal of the analytical input comes from knowing the current nature of a threat, tapping into one's base of experience, and applying old-fashioned common sense. The CSO who estimates probability applies a broad brush to a large canvas.

Impact

The impact or consequence of the threat event is an approximation based on the organization's earlier experiences and the experiences of similar companies in similar situations. Dollars are the customary measure of impact. The rater takes into consideration the costs of replacement, repair, lost productivity, forfeit of business opportunity, cleanup, litigation, reputation damage, and degradation of customer goodwill. Even when the impact is on human life, the yardstick is dollar value.

Frequency

Frequency is different from probability. In frequency, the rater has evidence of event occurrences such as the number of reports filed in a single year by employees whose laptops were stolen. Some events will not have a history. For example, in the matter of a trade secret compromise, the event may not ever have happened before, but the chance of it happening and the extent of loss are sufficiently compelling to regard the event as a real threat.

A relatively minor threat event, such as the theft of a laptop, can take on a serious dimension when the frequency of the event is high. A very serious event, such as the one-time compromise of a trade secret, can be less damaging in the long run than repeated theft of laptops. The cost of the event times the number of repetitions provides a dollar figure. If the cost of a laptop is $2000 and 100 laptops are projected to be stolen, the estimated potential loss is $200,000. This figure gives to management a basis for comparing potential loss against the actual cost of countermeasures. Not mentioned in this example, but extremely relevant to analysis, is the dollar loss associated with work output residing on a laptop's hard drive and the possible disclosure of proprietary data. Fig. 9.1 demonstrates a technique for estimating incident probability, impact, and frequency.

Manageability

A valuable perspective to management is the relative manageability of a threat. Manageability is the ability to reduce the probability and/or impact of a loss event. The principal methods of managing risk include:

- Avoiding the risk by placing the target where it can't be stolen or harmed. For example, a trade secret, such as the formula to a popular soft drink, can be kept in a high-security vault. Some businesses avoid crime-related risks by choosing not to operate in high-crime areas.

Incident Probability, Impact, and Frequency for a Convenience Store

Event	P	I	F
Robbery or attempted robbery	C	LI	M
Burglary or attempted burglary	L	MI	Y
Assault of employee or customer	L	HI	Y
Theft by shoplifting	C	LI	D
Employee pilferage	C	LI	W
Theft from till	L	LI	M
Theft of bank deposit	NL	MI	Y
Vandalism	L	LI	M
Arson or attempted arson	NL	HI	Y
Bomb threat hoax	NL	LI	Y

Probability Legend

PU, probability unknown;

NL, not likely;

L, likely;

C, certain

Impact Legend

LI, low impact (under $1,000);

MI, medium impact ($1,000-$10,000);

HI, high impact (Over $10,000)

Frequency Legends

D, daily;

W, weekly;

M, monthly;

Y, year or longer

FIGURE 9.1

The example used in the chart relates to the number and types of crimes committed at a convenience store during a given period of time.

- Reducing the risk by decreasing access to the target is another method. A convenience store robbery loss can be reduced by inserting into a floor safe all cash receipts above a designated amount. The store's shoplifting risk can be reduced by placing high-value merchandise in a locked cabinet and by placing easily concealed high-demand items, such as packs of cigarettes, behind the cashier's counter.
- Diffusing the risk involves the use of barrier systems such as perimeter fences; access control and intrusion detection equipment such as card readers and CCTV; locks, safes, and vaults; and standard control procedures such as property removal passes and inventory counts.
- Transferring the risk is possible by purchasing insurance or by raising prices so that the purchasers pay for the losses. Another technique is to outsource risk-heavy functions to another party. An example is the transfer of liability when an employer replaces an in-house guard force

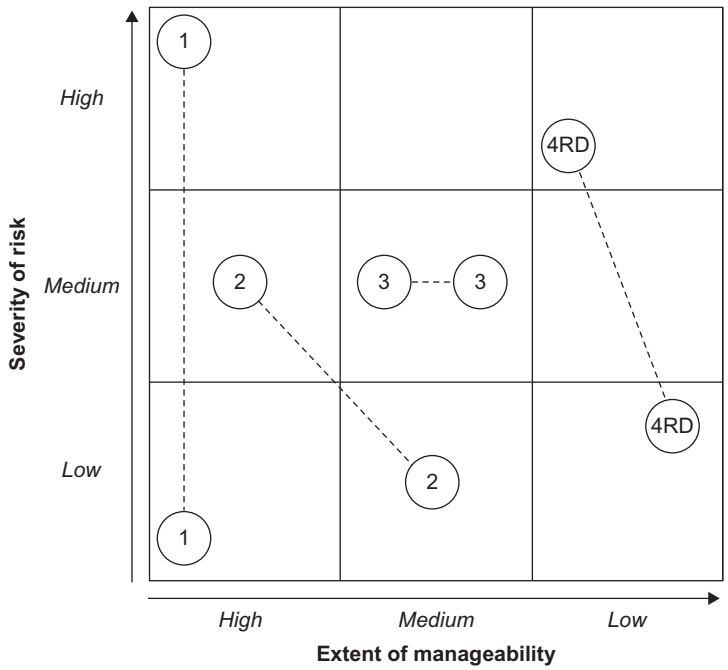


FIGURE 9.2

The Boston Square Method is a simple and commonly used device for assessing risk and management of it.

with a contract guard force. If misconduct by a contract guard harms a customer, the employer may be able to escape liability under the terms of the contract.

- Accepting the risk is also an option. A management may decide that a particular risk is worth a gamble or that the cost of loss is not large enough to justify the cost of protection. Another deciding factor may be the intractability of the risk (i.e., that despite best efforts, the risk cannot be controlled to an acceptable degree).

Fig. 9.2 can help the CSO estimate the extent of manageability of a given incident.

Countermeasures

In this step of risk analysis, security countermeasures are identified and then evaluated according to workability and cost. A countermeasure to laptop theft would be to anchor them to desks. The cost of installing anchors would be negligible compared with the cost of loss, but anchoring the laptops

would be objectionable because the countermeasure would cancel out the portability feature of laptops. An alternative might be to install lock-type anchors that can be easily detached with a key or combination dial.

Selection of countermeasures is based on two information sets. First is the information compiled from the risk-analysis process (i.e., data derived from identification of assets and threats; estimation of probability, impact, and frequency; and assessment of risk manageability).

The second information set has to do with the nature of the business, goals and operating philosophy of management, and the culture of the organization. The cultural factor can be extremely important and may explain why risk-management consultants will, in some situations, offer unworkable recommendations.

An understanding of the efficacy of countermeasures that require employee cooperation can be found in the theory of social control. The theory holds that people performance is dictated by formal and informal controls. Formal controls consist of rules and laws that coerce human behavior.

Informal controls consist of peer pressures that persuade conformity subtly and powerfully. Roper (1999) maintains that informal controls are considered more effective and longer lasting than formal control. Too often, cultural and social influences will subvert formal controls, which are main components of security safeguards. The examination of countermeasure options can lead management to address relevant questions such as the following:

- Is it always best to prevent the occurrence?
- Is it sensible to take proactive steps to mitigate the effect of the occurrence?
- Is it sensible to combine prevention with mitigation?
- Is it sufficient simply to be aware of the threat and do nothing in advance to prevent or mitigate it?
- Is prevention or mitigation cost effective?

A company's potential losses, according to Roper (1999), determine the steps taken to avoid or reduce them.

RISK ASSESSMENT VERSUS THREAT ASSESSMENT

A risk assessment is a detailed study of an organization's exposure to loss in its various forms, as well as the theoretical effectiveness of security measures that prevent loss. The assessment is the standard basis for design and redesign of security measures relative to changes in risk. A fluidity of chance is

inherent to risk. Following are examples of changes that carry risk: emergence or expansion of crime that is likely to affect the organization, social change that encourages employees to steal, increase in workplace violence, discovery of workplace drug abuse, unauthorized release of sensitive information, increased likelihood of a natural disaster such as an earthquake, and changes in the pattern of severe weather. Events such as these are called threat agents.

Many types of threat agents fall within the purview of the CSO to deal with, and many do not. Other persons in the organization share the responsibility to anticipate and prevent threats related to their areas of operation. For example, the chief financial officer has to be concerned about stock market fluctuations and revisions of the tax code; the operations officer confronts risk in myriad ways, such as the operational risk that British Petroleum took when it drilled in deep waters; and the head of human relations is concerned with risks connected to negligence in hiring, wrongful termination, and discrimination. Risks of varying natures confront the safety manager, the information technology manager, the property manager, and so forth.

Risk is a never-ending reality for businesses. A facet of a competently managed organization is an ability to make reasonable assumptions about risks. This ability is made apparent when an organization learns from past mistakes, looks into the future for threat agents on the horizon, and takes preemptive steps to negate or deflect them.

A risk is different than a threat. It may help to think of threat as the father of risk; there can't be risk without a threat. Threats are not easily anticipated but can be quite easily hypothesized. A CSO in Peoria who watches Middle East terrorism on television makes an unfounded hypothesis when he or she concludes that the organization is in imminent danger of being attacked by terrorists. However, the unfounded hypothesis can take a 180-degree turn if terrorists are observed marching down Main Street in Peoria.

Although techniques have been developed to assess terrorist threats, they are basically of a rudimentary nature. In the absence of hard intelligence, the best that an organization can do, with input from the CEO, is to characterize a specific terrorist group in terms of intent and capability.

Questions worth asking:

- Has the terrorist group identified the organization as a definite target?
- Has the group expressed an intention to act against the organization?
- Does the group possess the means to act such as possessing operational funds, weapons, and trained manpower?
- Have there been recent terrorist activities against similar organizations;
- Adjacency of the organization to other high-profile or high-risk organizations;

- Adjacency of the facility to critical infrastructure and key resources (CIKR)
- Types of tenants occupying the buildings, such as political-oriented groups, governmental agencies, mainstream media or entertainment groups, international and multinational companies, that might represent a target.
- Severe national and state crime statistics for the area
- The chronicle of security-related events specific to the site and building suggests terrorist risk
- Information provided by the government regarding operations at the organization and other properties in the surrounding area
- Comparison of operations and security practices for similar properties.

Answers to these questions will give some insight as to whether your organization may be a target.

Threat assessment relies to a great extent on fragmentary and imperfect information. Although preparation can be made certain, an accurate prediction of occurrence cannot be made certain. Three very important aspects of threat differentiate it from risk. First is magnitude. A threat can be calamitous and cause collateral damage. Second is its nature. Like risk, natural threats include uncontrollable events such as environmental disasters and accidental fires, but the threats of terrorism, crime, and kidnaping are entirely different matters, made so by varieties in type, consequences, and questionable predictability. The third difference is the arena in which the terrorist threat occurs. Terrorists operate on a world-stage, and their main targets include ethnic groups, religious groups, and governments.

An example of concern with threat size is demonstrated by the Department of Homeland Security's National Infrastructure Protection Plan (NIPP). The plan is a single national program designed to protect our nation's CIKR. A rough definition of a CIKR is a national sector that plays an essential role in maintaining the normality of life. Should a terrorist group succeed in destroying or disabling a major electrical power grid, the result would be a shutdown of factories, businesses, hospitals, communications, household lighting and anything else that relies on electrical power. Eighteen CIKRs have been identified, and they include industries in the financial, information technology, agriculture, and water supply sectors, just to name a few.

Each of the identified sectors is assigned an agency responsible for developing and implementing a sector-specific plan (SSP). The SSP is developed using risk-managing techniques that examine the unique and critical functions of the sector, identifying sector vulnerabilities, and establishing a coordinated prevention and response plan involving government, business, and public organizations.

A provision of NIPP initiated by Michael Chertoff, former head of the Department of Homeland Security (DHS), has implications for CEOs because it calls on businesses to become partners in carrying out the SSPs. NIPP was introduced in 2002 and revised in 2006, yet little has been done to bring businesses into the partnership in meaningful ways.

Many people throughout the world fear that attacks against our critical infrastructure will increase in the future. Even though some efforts are under way to implement plans, there is no integrated national approach to protect America's critical assets.

Securing our national infrastructure depends on a keen understanding of the relationships among its CIKR's, how each element functions, their interrelationships, and how they affect each other. For example: even though individual businesses may have business continuity plans, there is no plan for how the entire sector will deal with a major event such as a flu pandemic.

SELF-ASSESSMENT

Supervisors, managers, and other persons charged with meeting specific security responsibilities tend to be nervous and run to the CSO when they learn that a peer has been called on the carpet for failing to prevent a security-related loss or when they are told a security audit is on the near horizon. "Tell me what I should do," is the usual plea. A good answer would be, "Make a self-assessment."

A self-assessment is typically a comparison between what is expected in the way of security and what is actually being done. The assessment is usually made of a department by its manager and supervisors. Formalized security expectations are matched against the security behaviors of the department. The assessment, with input from the CEO, might pose the following questions:

- What security processes and procedures are in place to meet the requirements of this expectation?
- What are the differences between what we have now and what we need to satisfy the expectation?
- Are people aware of their personal roles and responsibilities with respect to this expectation?
- Do employees comply with the security processes and procedures in place to meet this expectation?
- Are security standards clearly understood with respect to this expectation? Are standards being met?

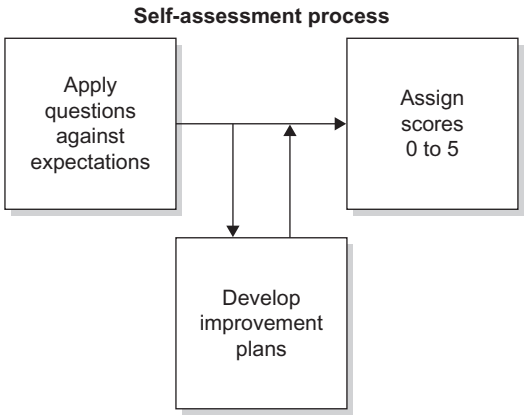


FIGURE 9.3
Self-assessment can be helpful in conducting an internal review and preparing for an external review.

- Where practice does not meet this expectation, are corrective actions being taken? What are they and are they succeeding?

The self-assessment model depicted in Fig. 9.3 is a very general model for identifying security weaknesses. However, it can be valuable in developing antiloss procedures and raising security awareness.

SELF-ASSESSMENT OF IT SECURITY

Self-assessment in the IT area can be assisted by several applications such as:

1. CobiT, a product of the Internal Guidance Institute. CobiT is a tool for ensuring good practices, measuring performance, and bridging the gaps between business risks, and technical issues.
2. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) OCTAVE is a suite of self-directed tools, techniques, and methods for strategic assessment and planning. In OCTAVE, small teams across business units and IT work together to address the IT security needs of the total organization. The OCTAVE approach can be tailored to the organization's unique risk environment, the knowledge and skill levels of the employees involved, and existing security standards.
3. *Security Risk Assessment Tool (SRA Tool)* The SRA Tool is a self-contained, operating system (OS) independent application that can be run on various environments including Windows OS's for desktop and laptop computers and Apple's iOS for iPad only.

4. The National Institute of Standards and Technology has issued a draft of a cybersecurity self-assessment tool. The Baldrige Cybersecurity Excellence Builder is a self-assessment tool to help organizations understand the effectiveness of their cybersecurity risk-management program.
5. The SEARCH IT Security Self-Assessment and SRA Tool is a companion resource to *The Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies*, which SEARCH developed for the Office of Community Oriented Policing Services, US Department of Justice.
6. The SysAdmin, Audit, Network, Security (SANS) Institute Information Security Management Audit Checklist is a comprehensive risk assessment checklist developed by the SANS and based upon the International Organization for Standardization 17799:2005 standards for an information security program.

SECURITY REVIEW

A security review is a loose comparison of security performance against formal, well-understood standards. Questions are asked and answers recorded, but not all of the answers are verified. The review points out areas of noncompliance and offers general suggestions for improvement.

A security review tends to focus on soft issues. For example, it may look at the organization's programs for overseas travel or employee security awareness but not look at hard issues such as safeguarding very critical assets or preventing and mitigating terrorist attacks. However, when a serious weakness is detected, a review can trigger a more penetrating analysis such as an audit or vulnerability assessment.

The security review is conducted at a frequency of about once per year. Each succeeding review examines what it examined previously plus weaknesses detected in a current review. The security review does not typically involve initial and exit interviews with the site's senior management.

SECURITY AUDIT

Where a security review is general, an audit is detailed and systematic, and applies analytical tools such as rating schemes with weighted values, matrices, and formulas. It is frequently conducted by more than one person. The auditor(s) are experienced professionals with in-depth knowledge of risk analysis. The length and detail of the checklist shown at Fig. 9.4 is appropriate when the assets under protection have a high value. An audit is a lesser

Checklist for a Security Audit

Is the facility security policy:
- In writing?
- Signed by the senior facility manager?
- Does it address the protection of people, property, and processes against loss or compromise?

Does the security policy provide guidance for preventing or mitigating the following?
- Larceny
- Burglary
- Loss or compromise of proprietary information
- Assault on employees and visitors
- Bomb threats
- Arson
- Civil disturbances
- Unethical business conduct
- Alcohol and drug abuse

Is the security policy:
- Communicated in writing to all employees?
- Conspicuously posted throughout the facility?
- Referred to during new employee orientation?
- Referred to at group meetings?
- Contained in a manual?
- Referred to in management and employee training programs?

Does senior management support the security policy:
- By periodic written communications?
- By regular security tours?
- By participating in security program audits?
- Are there written standards for management performance in the security program?

Are security program standards communicated to all levels of management?
- Are security instructions and procedures defined in a program manual?
- Are annual written security program objectives set for the organization?
- What percentage of managers has developed written security program objectives?
- To what degree are program objectives being achieved?

FIGURE 9.4

The length of this checklist should not be interpreted to mean that an audit is far more difficult to conduct than a review. An audit can be conducted in a relatively short period of time, such as 1 or 2 days, whereas a review demands coordinated work by two or more security professionals actively working for as long as a month.

Has a person been designated in writing to coordinate the security program?

- Does this person have direct access to senior management on security program matters?
- Are security responsibilities written into manager job descriptions?
- Is performance to security standards included in manager performance reviews?

Are local law enforcement, intelligence, security, and regulatory agencies contacted regularly for assistance in supporting the security program?

Are the people who are selected for sensitive or critical duties and positions screened for suitability and reliability? Does the screening and verification process include:

- Criminal record checks?
- Credit checks?
- Education?
- Employment?
- Driver's license and driving record?
- Professional certification and/or professional licensing?
- Personal identity documents?

What percentage of managers receives orientation and induction training to the security program?

- Is this orientation and induction training completed within 1 month of appointment to a management position?
- What percentage of managers has had a formal training course on fundamentals of security?
- Are written materials used in this formal security management training course?
- Is there a program that requires managers to attend formal security-update training at least every 3 years?
- What percentage of managers has had the update training?

What percentage of employees/contractors receives orientation/induction training to security program standards?

- Are written materials included in the orientation?
- Are security awareness signs and notices posted in appropriate places to reinforce knowledge of security standards?

What percentage of employees holding specific security duties has received formal training in how to perform their duties?

What percentage of contractors who have specific security duties has received formal training in how to perform their duties?

- Are training manuals used to aid and reinforce security training?
- Are records kept to verify security training and identify employees needing such training?

FIGURE 9.4
(Continued)

Has a survey been made to determine the need for security measures, systems, and devices? Did the survey determine the need for:

- Perimeter fencing or walls?
- Protection of doors, windows, and openings?
- Security alarm systems?
- Camera surveillance?
- Security lighting?
- Lock and key control?
- Security signs?
- Safes, vaults, and protected storage?
- Protection of vital utilities?
- Communications?
- Access control?
- Guard force?
- Computer protection?
- Information security?
- Emergency preparedness?

Which of the needs identified by the survey have been met?

When were the security needs last reviewed and updated?

Are methods taken to control entry and movement of people and vehicles as a security measure? Do these controls include the following categories of personnel?

- Visitors
- Vendors
- Service and delivery personnel

Do these controls include the following categories of vehicles?

- Employee
- Visitor
- Vendor
- Contractor
- Service and delivery

Is the duplication of keys to buildings, vehicles, and storage areas controlled?

Are procedures in effect to address the following?

- Marking of classified information
- Control of classified information

FIGURE 9.4
(Continued)

- Distribution of classified information
- Transmission of classified information
- Copying of classified information
- Storage of classified information
- Downgrading of classified information
- Destruction of classified information

Is a clear desk policy in effect?

Are all employees/contractors who have access to sensitive information required to sign a nondisclosure agreement?

Are speeches, news releases, presentations, technical papers, and other forms of open information reviewed for sensitivity and protection of trademarks before release?

Is the facility engaged in classified government work or involved in a classified contract?

Do written delegations of financial authority exist?

- Are delegations made to and signed at each level of authority?
- Are delegations current?
- Are delegations routinely followed?

Are adequate controls and written procedures in place to maintain individual accountability for employees with cash-handling responsibilities?

Are approving, purchasing, receiving, and paying functions separated?

Are procedures in place for the disposal of scrap waste and surplus materials?

Are "right to audit" clauses included in vendor and supplier contracts?

When was the last financial audit conducted?

How often are inventories, accountings, and records checks made to identify security losses?

Are security losses and incidents promptly investigated with the findings and actions reported?

Are loss event reports reviewed for action needed?

FIGURE 9.4
(Continued)

Does the security program require a complete investigation of criminal and malicious security losses and incidents that involve:

- Cash and negotiables?
- Irregularities in financial accounts?
- Equipment and materials shortages?
- Expendable supplies and inventory shrinkage?
- Production losses from disturbances?
- Product loss or theft?
- Product extortion or contamination?
- Computer theft?
- Other security losses?

Is there a central facility file of security incident investigation reports?

- Are investigative and incident reports kept in an active file for at least 2 years?
- Are the appropriate levels of facility management receiving copies of reports and investigative summaries for corrective action?
- Is the appropriate level of specialized security advisor support receiving copies of reports and investigative summaries for information and corrective action?

How often are inspections of facilities and operations made by line management to verify compliance with security standards?

- Are checklists used to guide the security inspections?
- Are the results of security inspections communicated in writing to senior management?
  - Is a copy of the inspection report given to the responsible affected supervisor for follow-up actions?
  - Is there a written follow-up procedure to ensure that appropriate remedial actions have been taken?
  - Is a copy of the inspection report, together with corrective actions, provided to the appropriate level of specialized security advisor support?
- Has an overall facility Emergency Plan Coordinator been appointed in writing?
- Are security requirements included in all emergency plans?
- Are emergency response plans reviewed at least annually?
  - Do these emergency plans address:
  - Terrorism?
  - Death or serious injury?
  - Kidnapping?
  - Extortion?
  - Bomb threats?
  - Product contamination?

FIGURE 9.4
(Continued)

Strikes?

Civil disorder?

Failure of alarm and control systems?

Natural catastrophe?

Catastrophic fire or explosion?

Hazardous material discharge or spill?

Are plans coordinated with local law enforcement, fire protection, private security contractors, and emergency response agencies?

How often are drills held to train employees in emergency actions and test their performance?

Does the organization receive security periodicals to update professional knowledge?

Are security articles or other written materials distributed to managers at least quarterly to update their security management knowledge?

Are there written guidelines on enforcement of security standards to aid supervisors and managers?

How often is an evaluation of key security program indicators made for major units to determine effectiveness of the programs in place?

Are the results of these program evaluations communicated to senior management?

Are security promotional materials in use at the facility?

Are security promotional materials conspicuously posted throughout the facility?

Does security promotion include:

Posters on bulletin boards?

Awards that recognize employees who demonstrate exemplary security behavior?

Presentations at employee meetings?

Notices on the company's email system?

Does the facility have written policies or directives requiring the conduct of security reviews at the concept and design stages of all new developments, construction, and modification projects?

How often are compliance checks of design engineering records made by an unbiased person, with results related management, to determine the percentage of compliance with the engineering policy or directive?

FIGURE 9.4
(Continued)

form of a review because it looks at the underlying conditions of security rather than visible conditions.

Unlike a review, an audit searches intensively for security weaknesses and gives details of corrective actions required. The major focus is on very critical assets such as biological agents studied at a research lab, radioactive material used in a hospital, or sensitive data in an information technology system.

The auditor(s) meet with and brief senior management before, during, and after the audit. The initial briefing covers the audit methodology, the people to be interviewed, and the site's major areas of interest. The midpoint briefing covers progress and tentative findings. The exit briefing covers actual findings and recommended corrective actions. An audit is conducted at a frequency of 1 to 3 years, or sooner when circumstances dictate. Such circumstances include the following:

- Operational changes at the site.
- Emergence of a new threat.
- A rise in threat level.
- Discovery of a serious security breach.

PROJECT REVIEW

The purpose of project review is to incorporate security features in the design of new construction projects and major renovations of existing facilities. A secondary purpose is to protect persons, equipment, and materials at the site during the project.

Project review is a team effort, with the CSO playing a central role. Other security professionals on the team can include consultants with know-how in selecting, installing, and integrating access control and intrusion detection systems, lighting, and security communications equipment. Team membership also will include specialists representing construction or renovation disciplines such as planning, designing, and engineering.

The review can begin before the decision that authorizes the project and at the end when the property is turned over to the user. It would not be unusual for the review period to last 2 years or more. However, not all members will be actively engaged in the project every day. The CSO, for example, needs to be directly involved when security issues are before the team and when an outside security consultant is at the site. Security at the project site is provided during the project. Every project has a unique set

of variables that impact security, and they tend to be external variables such as:

- Project location, size, and duration.
- Nature and complexity of the construction/renovation work.
- Environmental conditions.
- Constraints imposed by the public and local government.

The CSO's major responsibilities occur during the three Security Industry Association project phases (CSPM, 2014):

- Initiation
- Planning
- Execution

Project Initiation

In the initiation phase, the CSO puts on a thinking cap and gets down to serious business. Decisions made at this point can profoundly affect every security issue that follows. To make the best decisions possible, the CSO has to determine the following:

- The core business functions and processes that will take place at the facility.
- The critical assets that merit protection, and the extent of protection to be afforded.
- Actual and potential threats such as:
  - Terrorist acts.
  - Sabotage.
  - Criminal acts.
  - Compromise of sensitive information.
  - Internal theft.
  - Workplace violence.
  - Acts of nature.
- The preferences of senior management as to:
  - Contract versus proprietary guard services.
  - Armed versus unarmed guards.
  - Guards wearing uniforms versus guards wearing blazers and gray slacks.
  - Free-moving traffic versus restricted traffic entering and moving within the site.
- Site layout.
- Characteristics of the surrounding neighborhoods and community.

- The physical environment within and around the site.
- Weather conditions.

Two general sources are available to the CSO for making the cited determinations: site management and outside agencies that provide services to the facility. The outside agencies and the services they provide are sure to be:

- Law enforcement.
- Firefighting.
- Emergency medical treatment and public health.
- Emergency call centers.
- Contract security services.
- Contract property management.

In special emergencies, responders can include the US Coast Guard, National Guard, US Army ordinance disposal units, and the Bureau of Alcohol, Tobacco, and Firearms for bombing incidents.

The adequacy of the organization's security concept can be determined by collecting information through interviews and examining police call and arrest reports, traffic engineering and demographic studies, security guard incident reports, arson records and fire dispatch reports, emergency medical treatment reports, and hospital admissions related to crime-induced trauma. The mix of data can produce for the CSO a mental picture of human activities in and around the place of construction or renovation. A good feel for the data may allow recognition of security risks not immediately apparent. The collected information can answer pertinent questions.

- Are local response agencies capable of adequately responding to emergencies that are likely to arise during the project period and after the property is turned over to the user?
- Does the local jurisdiction impose any code restrictions that impact security (e.g., a code that prohibits certain types of exit door hardware)?
- Is there a capable and reliable private security force available for hire if needed?
- If the project is abroad, are there restrictions as to acquisition of security services and products?

In essence, the CSO ascertains what is needed, what is possible, and what is allowable. The broad outlines of a security system take shape, a shape that is sure to be modified in the design and specifications stage. Consider the following scenario.

CRITICAL THINKING EXERCISE

Barry Wilkes is the CSO for an insurance company planning to build a new office complex on the fringe of a major city. Wilkes is the security representative on the construction project team. While attending a luncheon meeting of the local chapter of the Building Owners and Managers Association, Wilkes learns that a shopping mall is planned to be built adjacent to his company's planned office complex.

The project review data he has so far collected indicates that each time a shopping mall had been constructed in or near city fringes the crime rate in the surrounding area rose suddenly. Companies near the malls had experienced a sudden upsurge in auto thefts, purse snatchings, vandalism, assault, and trespassing. The reason, Wilkes suspects, had to do with the mall attracting criminal opportunists.

What do you think about this risk; how to offset it proactively and manage it when the new office complex is in operation? What next steps should Wilkes take?

Planning Phase

Security Design Specifications

The CSO now begins to sketch in the details of the scheme formed tentatively in the Initiation Phase. In the matter of physical safeguards, the CSO establishes specifications. In the matter of fencing, for example, the specifications can address length and height, type and gauge of fencing fabric, pounds per square foot of resistance to brute force, size of poles and distances between them, type and alignment of barbed wire topping, and number, size, and type of gates. The specifications are supplemented with details as to cost for materials and labor, availability, and time required for installation. Specifications such as these are drawn up also for lighting, closed-circuit television, sensors, doors, and other physical safeguards.

Security design specifications are normally linked to the Threat and Risk Assessments earlier described. At the conclusion of the project, they are evaluated by the CSO to ensure they meet their intended effectiveness.

Specifications are also drafted for guards, such as age, education, certification in first aid/cardio pulmonary resuscitation (CPR)/defibrillation, physical stamina, proficiency with firearms, absence of felony convictions or general disregard for the law, and freedom from alcohol or drug abuse. The cost and availability of guard services are included in the specifications.

Execution Phase

Commissioning and Warranty Stage

The commissioning and warranty stage is reached when the constructed or renovated facility is ready to be turned over to the user. The CSO's main

responsibility in this stage is to ensure that physical safeguards are in place and that guard services are ready to commence. Because safeguards and guards complement each other, there needs to be guidance. The CSO provides the guidance in the form of training and written instructions. Important among the written instructions are incident plans and procedures that deal with contingencies such as fire, workplace violence, and terrorist acts.

Project review technically ends on the day the site is turned over to and accepted by site management. Not later than 6 months following the acceptance date, a comprehensive security audit or a vulnerability assessment should be conducted.

SECURITY INCIDENT CAUSATION MODEL

In the immediate aftermath of a serious security-related loss, the CSO can reliably expect anxious questions from people at the top. They will want to know what happened, why it happened, and who was responsible. Later, when the facts are in and the finger pointing finished, management will expect to see corrective actions.

The CSO, one of the principals charged with conceiving and carrying out corrective actions, will be called on to apply investigative and analytical skills. The investigative skill is applied first (e.g., the scene or venue of the loss is closely examined, evidence collected, and witnesses interviewed). The analytical skill is applied after all of the relevant facts have been assembled. From the analysis will come a guide for remedial action.

A security incident causation model (SICM) is a relatively unknown loss control procedure. More than that, it is a method of identifying potential loss situations before they happen. SICM channels the CSO into giving very careful consideration to every relevant circumstance in a potential or actual security-related loss, followed by a thoughtful analysis of the circumstances individually, in combinations, and totally. The analysis discloses the causal factors of a loss.

Incident

An incident is an undesired event that results in harm to people or loss to property or process, and it is usually the result of inattention or deliberate disregard of a workplace rule. The theft of an expensive piece of equipment is a violation of a security rule. Is the CSO at fault? No. The CSO may have written the rule and made it known throughout the organization, but the real fault lies with the manager responsible for protecting the equipment.

In the matter of a safety violation involving an injury, the manager in charge of the work activity should know why the violation occurred. Was it a failure to train, to supervise, or to provide personal protective gear? The employee who committed the safety violation is at fault, but does the manager share the fault?

It helps to think of SICM as an active volcano, as depicted in Fig. 9.5. Coming out of the crater is lava, which represents loss and destruction. Inside the upper part of the volcano was an incident that expelled the lava. In a magna chamber at a deeper level is a super-heated pool of bubbling lava just waiting to erupt. All that is needed is one more security weakness to trigger an incident and send the lava over the top. The triggering action represents hidden causes that may have gone unrecognized or viewed as not worth expending funds to correct. In the security arena, a hidden cause can be minor in nature such as a hole in a perimeter fence and a burned out security light, or it may be a major deficiency such as a failure to acquire an electronic intrusion detection system. Who is at fault for not correcting the deficiencies? Clearly, the fault is with middle and upper management. The CSO, if unaware of the deficiencies, has not been paying attention. If aware but not insistent on correcting them, the CSO is not doing the job. In either case, the CSO should find another career field. However, if the CSO is aware of the deficiencies and makes a case for correcting them but is ignored by upper management, the fault belongs to upper management alone. When the volcano explodes, will upper management accept responsibility for losses resulting from its failure to act? Not likely. The blame will be pushed down the chain of command. This is a very good reason why the CSO needs to be

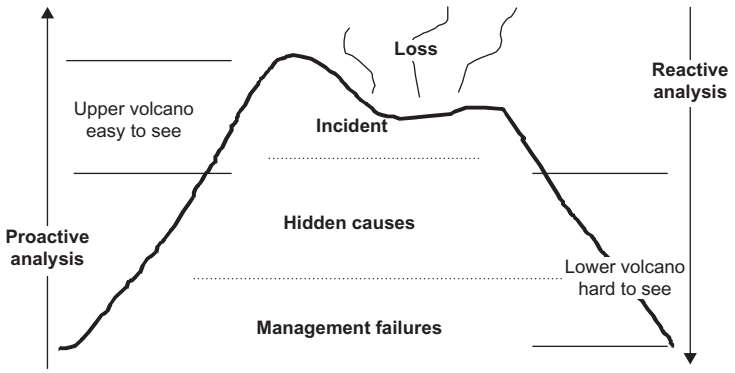


FIGURE 9.5

This illustration depicts loss (lava) flowing from a crater caused by an explosion (incident). The explosion is caused by hot gases and expansion of lava (hidden causes) that are not easily visible. The gases and lava are inside a magma chamber deep in the earth (management failures).

aware of the deficiencies, correct those that are within his or her authority to correct, and in all cases to report, in writing, the corrective actions taken and actions not taken or not allowed to be taken, (the implication being a failure of upper management to take immediate action).

Loss

The loss is the observable and therefore measurable impact on people, property, or process. It is the direct and indirect fallout of the security incident and can take many forms. A security incident involving violence will create time lost by employees who are injured or affected as the result of the misconduct. Time will be lost by coworkers who assist the injured and clean up the incident scene, and by supervisors who intervene to restore work activities, prepare reports, and testify at fact-finding proceedings. Then, there are losses of time resulting from upset, shock, diverted attention, and lowered morale of employees.

Increased operating costs are another form of loss. They result from medical claims and escalated medical insurance premiums; legal expenses associated with hearings and liability claims; penalties, fines, and civil court awards; recruiting, selecting, and training people to fill in for displaced employees; and acquiring interim operating equipment and supplies.

Property losses, which can be substantial, result from numerous violations, such as theft, misappropriation, malicious damage, and destruction. In addition, they often require expenditure of reserve supplies and equipment while dealing with the incident or compensating to overcome its immediate effects. Finally, there is the loss of profit, i.e., business income lost during downtime. Also are losses resulting from deterioration of employee and customer goodwill, adverse publicity, and missed business opportunities.

As stated earlier, loss is precipitated by an incident, which is often a combination of violations. A theft, for example, is a violation of law, of the employer's policy, and of a work rule. Addressing an incident in terms of unacceptable conduct helps direct thinking toward ways of influencing employees. This is more than just developing measures to managing conduct but of shifting employee attitudes toward behavior that will prevent incidents and minimize consequential loss when they occur.

Using the SICM model, incidents and losses are amenable to easy examination, but it is not so with hidden causes, which reside deep inside the volcano.

Hidden Causes

The hidden causes are the circumstances present in a situation at or immediately before the incident. In security parlance, a hidden cause is a nonsecure circumstance. It is very much like the crime prevention equation known as opportunity plus motive equals crime, except in this case, it is hidden cause plus incident equals loss. Essentially, a hidden cause is a deviation from a standard, a poor standard or lack of a standard. The term standard implies a minimum expectation, a basis for assessing performance against the expectation, and a means for deciding corrective action.

SICM STANDARDS

SICM standards have two dimensions: practices and conditions. Practices relate to job performance. Conditions are elements of the job environment such as physical setting and job tools.

Practices

When practices are substandard, they appear as human failures (e.g., failure to control access, lock things away, enforce security rules, make proper use of security resources, and act on the early warning signals of a loss incident). Human failures can result from lack of knowledge, skill, or motivation, and lack of physical mobility, stamina, or mental capability.

Conditions

Conditions pertain to the physical nature of the workplace and of the processes through which the work takes place. Physical aspects include building structure and layout, utilities, machinery, and equipment. Process aspects reflect how the work is carried out. To illustrate, a failure to control access to the company's stock of blank checks occurred when the stock clerk left the blank checks cabinet unattended because no one instructed him to the contrary (a substandard practice resulting from a deficiency in knowledge). The situation held a potential for loss due to the absence of a locking mechanism on the cabinet (a substandard condition resulting from poor physical construction) and because the accounting manager did not make access control of blank checks a mandatory step in the routine work processes of the department (a substandard practice resulting from the absence of a policy or directive). Many hidden causes are possible for each substandard practice and condition. Discovering the causes is essential to removing them.

SICM can be applied everywhere in an organization, including the security department. The substandard practices and conditions found in

security operations are poor and infrequent supervision, poor security program and procedures, poor selection of security applicants, poor initial and refresher training, poor assignment and utilization, poor team-building and interpersonal communications, lack of regularly conducted internal assessments, and excessive physical and psychological stresses.

With a little probing, hidden causes can be tracked down, but the reasons for them are not always apparent and not always fully understood. When discovered and made explicable, they tend to be controversial because they point fingers. Patience and persistent probing are needed to get at the root causes and expose them to rational examination. When brought to light, they often suggest the very changes that are needed but fault is rarely attributed to management.

MANAGEMENT FAILURES

The connection between causal factors and the failure of management is analogous to the connection between disease and medicine. The disease (think incident) produces symptoms (think early warning signals). If the disease is allowed to persist (think failure to act), the patient's health will deteriorate to the point of incapacitation to some degree (think loss). Had the patient engaged in healthy practices (think good management), the disease could have been avoided.

In SICM, a basic focal point is the practices of management. Errors of practice underlie deficiencies that lead to loss. Errors tend to occur in setting sound policies, work rules, and standards, but most of all, enforcing them.

It does not matter if management attention is directed at production, quality control, or accounting, nor does it matter where the responsible manager sits on the organizational totem pole. The simple fact is that every person in a managerial position has an obligation to protect the employer's assets.

Another simple fact is that in the rush of meeting other priorities, such as production goals, managers tend to push their assets-protecting obligation into the background, and even when not rushed, managers often have no idea how to go about meeting the obligation. Many are entirely dependent on the CSO, which in itself is a serious management failure. This is not to suggest ineptitude on the part of the CSO, only that the primary responsibility for the protection of assets belongs to managers and supervisors.

APPLYING THE SICM TECHNIQUE

SICM is a tool for fact finding, both reactively and proactively. If the facts to be found relate to a loss, the CSO starts with an examination of the incident and works downward. The amount of detail increases greatly as the inquiry probes deeper into the volcano. A single incident is likely to result from numerous substandard practices and conditions, and each practice or condition is sure to be rooted in a number of hidden causes.

Proactivity

A proactive use of SICM is to prevent an incident or reduce its negative impact. In this approach, the CSO starts at the bottom of the volcano and works upward. The idea is to identify the potential causes of an incident and take preventive steps before the incident happens. A logical start is to examine policies, rules, and standards that relate to the use and care of assets. One such policy is the security policy. Does such a policy exist? Is it in writing? Has it been communicated throughout the organization? Is it understood, followed, and enforced?

Programs

Next to be examined are the various programs for carrying out policies, effecting rules, and operating in accordance with standards. Several areas of interest come to mind: internal audit, safety, human resources, and the IT department. Program activities will vary, as will the work groups that create and operate them.

The security program is a legitimate and logical function to evaluate. Program activities worth examining include physical safeguards, security officer operations, protection of proprietary information, investigations, security awareness, and so forth. Each program component is or should be operated according to well-defined standards.

The CSO's Role

The CSO sets the organization's security standards, communicates them to managers, and provides guidance when managers demonstrate less than full understanding of their assets-protecting responsibilities. Finally, the CSO evaluates compliance.

The SICM technique can give a new perspective, one that prompts the CSO to ask the right questions and find answers buried below the surface. SICM does not replace good investigative practices and is not a substitute for

critical thinking, but it can be a tool for organizing the CSO's approach to risk management.

CONCLUSIONS

Risk management is neither rocket science nor voodoo witchcraft. It is a simple and straightforward process that systematically identifies security-related exposures that affect the organization's activities. It is not a function to be turned on, such as when a new project is announced, and then turned off when the project is running smoothly. Risk management is in the "on" mode at all times.

REVIEW QUESTIONS

1. What are some specific risks confronting security professionals?
2. In what ways is risk analysis helpful to a CSO?
3. What are the two categories of threat?
4. Name the seven steps of risk assessment.
5. What are the stages of a CSO's project review responsibilities?
6. Name and describe five opportunities for managing risk.
7. Contrast the Review and Audit Technique against the Project Review Technique.

References

CSPM, 2014. Security Project Manager Common Body of Knowledge Guidebook. Security Industries Association, Sllversprings.

Daniell, M.H., 2000. Next Generation Strategy for a Volatile Era. John Wiley and Sons, New York.

DePasquale, S., 1993. Risk analysis: development of a security program. In: Fay, J. (Ed.), The Security Management Encyclopedia. Butterworth-Heinemann, Boston, MA, pp. 635–639.

Roper, C.A., 1999. Risk Management for Security Professionals. Butterworth-Heinemann, Boston, MA.

Further Reading

Chertoff, M., 2009. National Infrastructure Protection Plan. Department of Homeland Security, Washington, DC.

CHAPTER 10

Managing Guard Operations

What You Will Learn

- The qualifications of a security officer candidate.
- Entry-level training topics and training methods.
- The relationship of a critical asset to a needs assessment.
- The typical duties of a security supervisor.
- How to determine the level of security staffing.
- The differences between proprietary security and contract security.
- What to look for when selecting a contract security company.
- The three pillars of a security system.

INTRODUCTION

Private policing arrived in North America with early English settlers. Private police, whose duties were principally to watch for crime during the hours of darkness, supplemented the town constables, and sheriffs. In today's workplace, Berg (1999) contends that security officers play a role that goes well beyond the role of their predecessors. They number more than close to three times the number of police officers and have become common sights in many sectors of society such as shopping malls, department stores, college campuses, office buildings, industrial plants, apartment complexes, airports, and residential-gated communities. Organizations and individuals of all types employ security officers to curb trespassing, theft, robbery, and assault.

Security officer services are primarily directed at controlling access, patrolling, escorting, inspecting for fire and safety hazards, and responding to emergencies. In some organizations, they direct traffic, receive supplies, ship goods, process visitors and guests, dispense general information, deliver mail, and escort company employees making bank deposits.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00010-4

SECURITY OFFICER SELECTION AND TRAINING

States vary according to entry-level requirements for selecting and training security officers. The requirements range from none to numerous. Study after study has concluded that the private security industry needs to operate from a single sheet of music in all states, yet nothing serious has been done about it.

Selection

States with entry-level requirements are fairly consistent in their hiring standards. Typically, they require the security officer applicant to:

- Be at least 18 years old for an unarmed security position and 21 years old for an armed security position, with provisions that the candidate be able to perform the duties required of the position.
- Be a citizen or immigrated citizen of the United States, a lawful resident, or an alien authorized to work in the United States.
- Possess a high school diploma or the General Education Development certificate, or an equivalent.
- Not have been convicted of or pleaded *nolo contendere* to a felony during a set period immediately preceding the date of employment.
- Not possess a history of disregarding the law generally.

Training

Training standards, where they exist at all, are inconsistent at best. There is no standard curriculum from state to state, nor is there a standard number of training hours, either for individual topics or the training course as a whole. Some states mandate security guard certification while others do not. New York, for instance, passed The Security Guard Act in 1992, which requires the training and registration of security guards, as well as state approval of all security training programs. In Alabama, security officers are not registered or licensed at all. In some states where training is mandated, the employer is allowed to defer training for a set period of time. Deferred training coupled with the high turnover rate in the private security services sector makes it possible for security officers to drift from one employer to another without ever being trained. Security officers employed by the military in war zones are an exception. To qualify for the work, they must undergo meaningful training, much of which is paramilitary in nature.

Topics suitable for entry-level training include the following:

- The role of a private security officer.
- Legal aspects of private security.

- Access control procedures.
- Emergency-response procedures.
- Life-safety procedures.
- Patrol operations.
- Intrusion detection and response.
- Workplace violence response procedures.
- Use of force.
- Note taking and report writing.
- Court testimony.
- Conduct and appearance.
- Interpersonal skills.
- First aid, cardiopulmonary resuscitation (CPR), and defibrillation.
- Ethics.

The American Society for Industrial Security has developed a set of training topics that are recommended to its members.

In addition to entry-level training, the client of a contract private security services company may require training appropriate for the client's business. For example, orientation to:

- The physical layout of the protected premises.
- The names, faces, and positions of senior management.
- The client's policies in respect to harassment, discrimination, diversity, and so on.
- Substance abuse.
- Telephone protocol.
- Demeanor and behavior.
- The key rules of a labor-management agreement if any.

Training can be administered in three ways: classroom, on-the-job, and online. Classroom training methods include lecture, demonstration, use of audiovisuals, and practical exercises. Professional trainers agree that retention of knowledge and acquisition of skills is greatly increased when practical exercises are used. Examples of practical exercises are how to administer first aid, CPR and the automatic external defibrillator, direct traffic, use self-defense, apply force, apply handcuffs, search persons and property, inspect parcels and packages, protect a crime scene, use communication equipment, and for armed guards, safety and nomenclature of the weapon to be assigned and extensive practice at a firing range.

On-the-job training (OJT) is an excellent method for teaching all of the above. The downsides are removing an experienced officer or supervisor from normal duties to conduct the OJT and monitor the officer's job performance.

Online training, a method of instruction relatively new to training security officers, is an excellent method for imparting knowledge. The advantages are as follows: training occurs wherever a PC or laptop is available, learning proceeds at the learner's pace, and done at anytime and anyplace, even at the officer's home if allowed. The method does not permit the trainee to move forward in study until all material has been covered, and the content of the training is uniform for everyone. The method is enhanced when the instruction is augmented with audiovisuals, progress questions presented throughout the course so that the student can assess his or her learning, accessibility to an instructor or course administrator by television, phone, e-mail, or in-person. The contract security services company is also able to free itself from maintaining a record of training because the software of the online learning system does it automatically. The downside of online training is the impossibility of conducting hands-on training methods. However, the cost of online training is significantly less than other instructional methods and the trainee can be placed on the job without a long delay. OJT would pick up the slack in tasks that are hands-on oriented.

A contract private security services company will find it difficult to rely exclusively on classroom training because there must be a scheduled class to begin with and students to fill it. Sporadic hiring is in the nature of the business, and to teach in a classroom when there are few people to be taught at one time can be costly and not helpful in quickly filling vacant jobs. To overcome the problem, some companies (despite rules against it) will simply brief the individual on the job's tasks, show a film, and test the individual on paper. If the individual fails the test, it is administered until passed. States that regulate the industry usually require the security services company to submit a statement to the regulatory agency affirming that the training has been completed. Little or nothing is done about the quality of the instruction. Finally, the regulatory agency rarely conducts inspections to verify that the security services company is meeting the mandated requirements.

NEEDS ASSESSMENT

Deciding the types of security officer services needed by an organization is best dictated by a needs assessment. A needs assessment will answer three important questions:

- What assets need to be protected?
- What knowledge and skills will security officers need to possess in order to provide effective protection of the assets requiring protection?
- What physical safeguards are needed to complement guard operations?

Assets

Before an assessment is made, the property under protection must be known. To decide whether three or thirty security officers are needed, there must first be an identification of the assets to be protected. Protection of a storage warehouse may require three officers, while the protection of a nuclear storage facility may require thirty officers.

In the general sense, assets include employees and everything owned or used by the business. Assets range from pencils to high-rise buildings and from mail clerk to chief executive officer. The needs assessment determines those assets that merit protection. Protection merit is based on:

- The importance of the asset to business operations.
- The dollar value of the asset.
- Replacement of the asset should it be stolen, damaged, or destroyed.

For the sake of clarity, we will use the term "critical asset" when referring to an asset that meets the above three criteria.

Some assets, such as office supplies, merit very little or no protection at all. Why? Because they are inexpensive and are easily replaced at low cost. The same is true of assets of a higher value such as company vehicles and merchandise in storage. The items may be worth more but the business will not be seriously damaged if they are stolen, and they can be replaced without much difficulty.

Critical assets are a different story. If removed from the operation of a business, a single critical asset could have a catastrophic effect, even kill the business. Because critical assets vary in criticality, they might be prioritized and receive protection according to priority. A low-critical asset, one that would have a serious effect if lost or damaged but would not cripple the business, would be low on the priority list. A high-critical asset would be at the top of the priority list and merit a high degree of protection.

The first task of the Chief Security Officer (CSO) is to form a priority list after a needs assessment has been concluded. The CEO's second task is to determine if the guard force, physical safeguards, and written instructions are adequate. The third task is to eliminate vulnerabilities exposed by the needs assessment. A vulnerability is a deficiency such as not having enough guards, poor or no training of guards, no perimeter fence and security lighting, and no written instructions for day-to-day operations or emergency response.

Take note that a security program has three components, which are sometimes called the three pillars of a security. To get the point, it may be helpful to analogize. Think of a cabinet maker (the security officer) who shapes

wood with a lathe (equipment) according to the design of the cabinetry (procedures). Another way of explanation is to think of the security officer using physical safeguards according to instructions.

The safeguards available to a security officer for protecting assets can address all or a combination of the following:

- Physical structures such as walls, fences, bollards, jersey barriers, and other devices that prevent unauthorized entry or channel traffic.
- Security lighting.
- Access control systems.
- Intrusion detection devices such as sensors and closed circuit television (CCTV) cameras and monitors.
- Security control center.
- Duress alarms.
- Gates.
- Safes, vaults, and locks.
- Communication equipment.
- Vehicles.
- Life-saving equipment.
- Fire suppressing and extinguishing devices.
- Protective gear.
- Weapons (if authorized).

Note the safeguards fall into two categories: those that are firmly affixed, such as fences and gates, and those that are portable such as life-saving equipment and cell phones. Both categories can be thought of as tools of the job.

Instructions that direct and guide the security officer include the following:

- Standard operating procedures.
- Post orders.
- Special orders.
- Temporary orders.
- Emergency plans.
- Emergency contact lists.
- Manuals for operating security equipment such as components of an access control system.
- Duty schedules.
- Verbal instructions.

The needs assessment evaluates all three pillars with special emphasis on the guard force. Why? The other two components have little value without security officers to monitor the safeguards, and in the event of an incident, no officers to respond. Fig. 10.1 is an example of a security officer

FIGURE 10.1
Operating safety monitoring equipment is a basic task of a security officer. *From Burns International Security Services.*

demonstrating competency in the operation of a hand-held electronic wand used to verify patrols are operating as prescribed. The figure highlights the need for security officers skilled in the operation of equipment provided to them.

LIFE-SAFETY PROGRAM

A critical asset is the workforce. Within this asset may be the chief executive officer or a group of senior managers, usually called the executive team. In addition to protection afforded, these individuals at the office may be an added level of protection such as a duress alarm, home intrusion alarm, security lighting at the home, and a security officer or security patrol in or around the residence. Because the threat has implications of violence, it is considered part of the company's life-safety program.

At the company's workplace is a different part of the life-safety program. It anticipates a full range of life-threatening emergencies such as fire, serious injury or illness, severe weather, bomb incidents, terrorism, and civil disorder. Because the guard force has roles to play in such emergencies, a supervisor of the guard force is often brought into the program. The security supervisor can be assigned to:

- Confer and liaise with local agencies such as fire, municipal police, and ambulance services; civil defense and emergency management services; and organizations that provide specialized services.

- Help prepare an overall Life-Safety Plan, as well as an emergency preparedness manual that delineates the specific responses of security officers.
- Designate life-safety responsibilities to individuals and designate backup officers to fill key positions.
- Train guards to look for and report fire and other hazardous conditions, operate the public address system, monitor the fire detection and suppression system, operate fire extinguishers and other emergency-response equipment, coordinate evacuation of the premises, and assist emergency-response personnel such as firefighters and police officers.
- Conduct periodic tests of emergency-response equipment such as fire-detection devices, fire extinguishers, public address system, air-handling system, order maintenance, and calibration when needed.
- Help educate employees as to how fire is detected and reported, building evacuation procedures, and the evacuation assembly areas. Also explain the tasks performed by floor wardens and security officers.
- Keep a name and phone number list of people involved in performing the procedures of the life-safety program. These can include floor wardens on each floor, maintenance staff, and security officers.
- Keep a daily attendance roster of people who perform essential life-safety duties, such as floor wardens and building maintenance workers, and be prepared in an emergency to designate security officers to fill in for life-safety responders who are absent from the workplace.
- Maintain in ready condition life-safety equipment such as bull horns, flashlights, first-aid kits, stretchers, and wheel chairs.

Staffing

When determining the number of officers required, the CSO looks at the staffing requirement for each post. If the post is to be manned by one security officer 24 h/day, 7 days/week, the number of actual performance hours per year will be 8736 (i.e., $24 \times 7 \times 52$). If the post operates with three 8-h shifts, the number of hours of actual performance by one guard per year will be 2912 ($8 \times 7 \times 52$). But the CSO does not want to overwork security officers or pay excessive overtime wages. He operates from an assumption that a security officer will be productive by working 8 h/day, 5 days/week, for a total of 2080 h ($8 \times 5 \times 52$). The difference between the required shift hours (2912) and the realizable shift hours (2080) will have to be made up by employing extra guards.

Other factors taking a security officer away from duties include vacation days, paid holidays, sick days, training, and time spent preparing for a day's tour of duty (e.g., checking out a weapon, standing inspection, receiving orders of the day, and traveling to the post). After running numbers on his pocket calculator, the CSO determines that an all-day post, although operated 24 h/day, will actually require 28 h of labor per day. He determines the post's staffing requirement by multiplying the required person-hours per day (28) with the days per year (365) divided by the realizable shift hours per year (2080). The result is 4.9 security officers for that post.

Skills

Security officer capabilities for each post are also identified. Every post demands a combination of cognition, psychomotor abilities, and attitude. Some posts require more of one than others. For example, a security console officer needs to know how to operate console equipment; a post that requires an officer to stand or walk has physical and stamina demands; and a post that brings an officer face-to-face with people requires tact and a positive attitude.

PROPRIETARY VERSUS CONTRACT SECURITY

The user of security officer services can choose to employ security officers directly or contract for services with an outside firm.

The Proprietary Option

In this option, guards are on the employer's payroll and are generally afforded the benefits and privileges of a regular employee. The arrangement will appeal to an organization that values loyalty, dislikes turnover, and feels a need to exercise close control over security officer operations. The CSO is held directly responsible for ensuring guard services contribute to the organization's overall assets-protecting mission. Also, the CSO works with the organization's human resources (HR) group. Recruiting, selecting, and hiring are handled in-house, with training provided or directed by the CSO. Going with a proprietary arrangement involves a hiring process unlike the hiring process of a contract security services company.

The Contract Option

The contract option will appeal to a management that does not want to commit its supervisory resources to the administration of security officer services. The usual procedure is to solicit bids from 10 or so contract security firms,

and it is here that the CSO does the homework. He or she looks for bidders with strength in the following three broad areas:

- Quality performance delivered consistently.
- Prompt responsiveness to concerns expressed by the customer.
- A competitive payroll rate.

Bid Solicitation

The bid solicitation will clearly define specifications and may specify also the pay rate of security officers. Although the contract firm may be free (within the limits of employment law and collective bargaining agreements) to offer compensation it believes reasonable and appropriate, the user of the contract service may want assurance that the officers' pay rate is high enough to attract and retain quality officers. A rule of thumb in the security industry says that an officer should receive about 65% of the rate paid to the contract firm. The other 35% represents fringe benefits, the contract firm's operating costs, and profit. So, for each $15.00/h of an entry-level guard's salary, the guard will actually receive about $9.75. Compensation must be high enough to account for this difference in order to attract and retain quality employees.

The solicitation will also describe the nature, place, and conditions of work; the personal qualities the officers must possess in order to perform the specifications; and penalties for failure to deliver the agreed services. Very specific details will be included as to how and when bids are to be submitted and judged. Fig. 10.2 is a security officer on patrol outside a protected facility, using a radio to keep in contact with the security control center.

Scope of Work

A solicitation will refer to the scope of work, a term roughly corresponding to a job description. The scope of work might state that the site to be protected requires a security officer to examine badges at an entry point such as an electronic gate at a nuclear power plant. Fig. 10.3 depicts a nuclear power plant.

The task of examining badges is broken down into specifics such as when and where the task is to be performed, manner of performance, and environmental conditions. Post orders and other written guidance would be suggested as to content.

FIGURE 10.2
Security officers patrolling the exterior of protected buildings must have a means of instantly communicating with the security control center. *From Burns International Security Services.*

In Fig. 10.4, you will find a sample procedure pertaining to duress alarms. An unauthorized entry through a controlled portal might require the security officer to sound a duress alarm, thus putting employees on notice that an authorized person is inside the protected facility.

Officer Standards

The solicitation might include details as to the knowledge, skill, and training required for acceptable officer performance. Note that Fig. 10.5 lists

FIGURE 10.3
A nuclear plant requires protection by security officers with impeccable personal histories, stamina, vigilance, and better-than-average ability to use firearms. *From iStockphotos.*

recommended standards for security officers. Attention would be given to those standards that most directly relate to the work to be performed. For example, they might call for previous experience, skill in operating certain equipment, and certification in CPR and first aid.

Bid Evaluation

Selecting a contractor begins by verifying the bidder's license and insurance certificates. A Dun & Bradstreet report can provide information on the history and ongoing operations of the bidder. Inquiries might include a check of civil court records and criminal histories of the bidder's owners and operators. The CSO should obtain written assurance that the bidder will agree to a hold-harmless clause, a stipulation that frees the organization of fault, or guilt stemming from improper performance of services. Other considerations include selecting a provider that can document:

- A lower than average turnover rate.
- A capability to quickly engage competent new hires.
- A hiring process that screens out undesirables.
- Skilled on-site supervision.

Responding to a Duress Alarm

Sounding the duress alarm	Duress alarms are in place at several key locations on Company premises, e.g., at perimeter and interior entrance points, the receptionist's desk on the executive floor. Also positioned at some locations would be CCTV cameras that automatically go into the record mode when the duress situation is in progress.
What to do when a duress alarm activates	Upon receipt of a duress alarm, the console operator at the security control center will look at the CCTV monitor to learn the nature of the emergency.
Non violent emergencies	If the emergency is of a nonviolent nature, such as an injury or sudden illness, the console operator will: • Use the base station radio to dispatch the roving patrol to the incident location and provide details as to the nature of the emergency. • Call 911 to ask for an ambulance, if one is needed.
Violent emergencies	If the emergency is of a violent nature, such as a shooting or a robbery in progress, the response will be to take no action that could cause an escalation of violence. In this case, the console operator immediately will take the following actions: • Call 911 and ask for police assistance. • Not dispatch the roving patrol. • Continue to watch the CCTV monitor and respond appropriately, e.g., relay further details to the police, such as descriptions of the offender, the offender's vehicle, direction of travel from the scene, or make a request for an ambulance if injuries occurred.
Needed reports	An activation of a duress alarm will in every case require an entry in the Daily Log and an Incident Report. A verbal report will also be made to the Security Leader.

FIGURE 10.4

This is an example of a specification as well as a procedure that would be a topic of OJT instruction and a written procedure kept in the security control center.

Recommended Hiring Standards for Security Officers

A security officer applicant must:

Be at least 18 years old if applying for an unarmed officer position, and be at least 21 years old if applying for an armed officer position.

Possess a valid driving license if driving is a part of the job.

Submit an application that includes full identification data, citizenship status, and a statement of conviction of crimes. Attach two sets of fingerprints and two passport-size photos.

Furnish information about prior employment during at least the last 7 years. Provide three personal references.

Pass a pre employment drug test.

Never have been convicted or pled guilty or *nolo contendere* to a felony.

Never have been convicted or pled guilty or *nolo contendere* to a misdemeanor involving moral turpitude, acts of dishonesty, or acts against government authority, including the use and/or possession of a controlled substance in the last 7 years.

Never have been convicted or pled guilty or *nolo contendere* to any crime involving the sale, delivery, or manufacture of a controlled substance.

Never have been declared by any court to be incompetent by reason of mental disease or defect.

Must have completed training in areas involving the law, security operations, firearms, administrative requirements, electronic technology, armored transport, and the use of force.

Must have completed training specific to the type of license applied for. Examples of licenses include:

Temporary Permit. Issued by the employer after the applicant has completed training and the license application has been submitted to the state licensing agency.

Class I: Security Officer/Unarmed Alarm Responder. Issued by the state licensing agency after the applicant has met the application criteria.

Class II: Armed Security Officer/Armed Alarm Responder.

Class III: Armored Car Security Officer. This license is issued by the state licensing agency after the applicant has met the application criteria and has successfully completed a state-approved firearms training course.

FIGURE 10.5
These standards are examples of specifications.

- A training program that provides new hires with entry-level knowledge, skill, and on-the-job tutorials. In Fig. 10.5, see a checklist that can be helpful in assessing the competency of security officers employed by the bidder.

Choosing a security services provider in an overseas area requires addressing the matter of human rights violations. The CSO should take care not to contract with companies whose past or current performance indicates a disregard for human rights. Excessive use of force and cruel or degrading treatment are examples.

Selection

Selection of a security services provider should be based first on quality of service. Price, although always important, should be secondary to quality.

At this point, assume a contractor has been selected. Now begins the CSO's next function: monitoring contractor performance and comparing performance against contract specifications. An important area of monitoring is guard supervision.

First, and most important, is the day-to-day supervision directly exercised on-site. The major duties of the contract supervisor's job include preparing the work schedule, briefing officers before going on post, maintaining and updating post orders, inspecting posts, maintaining documentation related to the work, and mentoring officers.

CRITICAL THINKING EXERCISE

Joe Palombo, on-site supervisor of the contract security officer services at a large shopping mall, knew he did not have enough security officers to adequately patrol the entire site, and he had made his concern known to his employer. Joe's employer, Iritus Security Services, had not responded. Joe was aware that Iritus had committed in its contract with the mall "to protect persons on mall property."

At the far end of the mall, away from the anchor stores visited by shoppers, was leased office space. The leaseholder was a county department of human services. A male claimant for assistance got into an argument with a female claims processor. The argument migrated into the hallway of the mall, at which point the claimant punched the processor in the face, breaking her jaw.

The claims processor sued the mall owner and Iritus, claiming negligence plus breach of the security services contract between the mall owner and Iritus. The trial court granted summary judgment to the mall owner but not to Iritus. The court said that the mall owner had met the obligation to provide security when it hired the services of a professional security company but the professional security company had failed to meet a fundamental duty described in the contract, specifically the duty of protecting persons throughout the entire mall. Iritus fired Joe 2 days later. Joe subsequently talked to an attorney about filing a wrongful termination suit.

Could Joe have approached the problem in a different way? Should he have gone to the mall management company to report the inadequacy of security services at all places in the mall?

ASSURANCE

The signing of a contract for security services is the starting point of a potentially tempestuous journey. Two travelers, the contractor and the customer, make the journey together. The contractor's function is to deliver services; the customer's function is to ensure that services are delivered according to contract specifications. The customer's agent for ensuring security officer performance is usually the CSO.

Looney and Whitley point out that assurance does not directly involve supervising contract security operations; nor does it involve meddling in the administrative affairs of the contractor such as questioning security officer performance ratings or intervening on behalf of a disciplined officer.

The interaction between client and contractor should be at the management level. For example, the CSO reports his concerns to the contractor's account manager, who decides the corrective actions and reports results back to the CSO. A positive interaction can prevent undesirable incidents.

To be effective at assurance, the CSO has to pay attention to what is happening. This imperative can be met by simply watching security officers at work and talking with people on the receiving end of security officer services. When security officer performance appears unsatisfactory or service receivers complain, the CSO acquires specifics and irons out problems with the contractor's account manager.

The purpose of assurance is not to carp in order to strengthen demands but to enlighten so that improvements can follow. The opportunity to enlighten is through frequent meetings, the ground rules of which require dialog in both directions. The CSO avoids an adversarial approach. Topics for discussion can include the contractor's strengths and weaknesses, problem-solving and quality-enhancing ideas, and solutions as opposed to iteration of problems. The CSO should also mention upcoming changes that might impact security officer operations. This can be an appropriate occasion for the contractor to make the customer aware of new technologies, added services, and an adjustment in compensation.

VALUE OF GUARD SERVICES

The value of security officer services is difficult to measure because prevention cannot be seen or measured. No one knows for certain the amount of loss that was avoided because a security officer was present as a psychological deterrent. However, in the retail field where loss prevention is paramount, the CSO can compare last year's theft losses against current losses. A positive finding indicates the security officer's effectiveness in reducing theft.

The marketing and customer relation aspects of service often overlap the operations function. A service delivered with excellence to the operations department may be arbitrarily described as poor if the relationship between the operations manager and security supervisor is fractious. Service value is likely to be undervalued by the operations manager because it was measured by the wrong yardstick.

Although security services are client centered, the client is not always present when the service is delivered. Excellent performance provided out of sight will go unrecognized, whereas minor lapses produce displeasure when seen.

The relationship between the customer and the contractor should be a partnership in which both sides strive for open communications. The CSO expresses what is wanted; the contractor listens carefully and follows up with action. If the contractor representative cannot deliver on what is wanted, he or she is obligated to say so. The CSO's expression of wants proceeds from a short list of questions, which are as follows:

- Is the contractor delivering services that correspond to the organization's overall goals and the security group's objectives?
- Does the contractor have and deploy resources that meet these goals and objectives?
- Does the security force have the right mix of officers and do their individual and collective talents match the work they are required to perform?
- Are security officers performing unnecessary tasks?
- Does the security force understand the workings of important physical security aids utilizing security aids such as access control and intrusion detection systems?
- Is the contractor meeting contract specifications?
- Are there any operating costs that can be reduced or eliminated?

Mutual Respect

Respect is an essential element for successful partnering. The CSO respects a contractor who asks if the services are on target, pays attention to the answers, tries honestly to deliver, and is not afraid to innovate. The CSO wants his partner to act like a winner, show a positive attitude, and be determined to do what it takes to satisfy.

The contractor's respect for the CSO is based on demonstrated competence. The CSO's image rises when he or she displays an understanding of the processes and technologies that drive the contractor's line of business. Competence is also reflected in the CSO's ability to work with people, to negotiate in good faith, and to give a little when merited. The contractor might be happy to reciprocate by awarding bonuses and other forms of recognition that reward superior security officer performance.

Agreement Issues

The contract between a client and a security services provider requires the provider to perform certain services according to specified standards. When a

service is not performed as specified, the CSO may at first seek to negotiate a satisfactory solution. A contract will often contain a "Failure-to-Perform" provision requiring provider to reimburse the customer for costs incurred as a result of the provider's failure to carry out the agreement. For example, the provider might be obligated to pay the customer when a security officer fails to show up for work, requiring payment of overtime. The Failure-to-Perform provision should not be used as a punishment tool. Another common gripe of the CSO is overbilling, which may require the provider to pay a monetary penalty.

Liability

The relationship between contractor and customer has to be robust but kept at arm's length. When the customer directly instructs security officers, a coemployer situation is said to exist. Coemployment opens a Pandora's box of legal woes because an unlawful act by a security officer can bring the customer into a lawsuit as a codefendant.

Even though a contract has assigned to the provider clearly stated responsibilities, courts have frequently held that the customer is fully or partly liable. Purpura (1993) reminds us that a legal principle called *respondeat superior* says that an employer can be held liable for injuries caused by an employee. An injured party, such as a shopper wrongly detained by a department store security officer, may sue the officer, the security guard company, and the department store. If found guilty of a civil charge alleging wrongful detention, the jury can order stiff, often unreasonable, punitive and compensatory awards.

The number and type of security officer violations go well beyond wrongful detention. Other offenses include false arrest, infliction of injuries, false reporting to the employer, theft, leaving post early, carrying weapons not authorized by the employer or prohibited by law, insubordination, and excessive use of physical force. Certainly, the most egregious violation is improper use of deadly force. Fig. 10.6 shows training in the use of firearms. Use of a firearm is an extremely important task that requires full understanding of when it is permissible to apply deadly force.

Fortunately, lawsuits are avoidable, mainly through effective training and close supervision. Security officers have to be taught the applicable laws in the jurisdiction where they work, the limitations on their enforcement powers, and the actions that may be taken against them for unlawful and improper acts.

FIGURE 10.6
Firearms training is given to security officers who carry firearms while on the job. *From iStockphotos.*

CONCLUSIONS

A facility's security system has three pillars: people, physical safeguards, and procedures. Without security officers, the other two pillars would topple. Employees cannot respond to a fire in progress or a bomb threat if there are no guards to inform them of the conditions and the actions to take. A CCTV system has no value if there is no one watching the monitors. Procedures are nothing more than words on paper when there is no one to bring them into action.

Although security officers are critical to the operation of the facility's security system, they are likely to commit more errors than the other two pillars. The probability that an intrusion sensor will fail is in the range of 1%. The failure of a lock is slightly higher. The failure of a security officer is much higher.

Managing security officer operations is not easy. Security responses cover many situations and are fraught with opportunities for human error. Security officer performance requires constant attention because a single failure can result in a major loss.

REVIEW QUESTIONS

1. List three standard requirements for an entry-level security officer.
2. List five topics that would be covered in an entry-level security training program.

3. Explain the difference between proprietary and contract security services.
4. What is a needs assessment?
5. State why knowledge of the nature of a critical asset is essential to the performance of a needs assessment.
6. Describe a life-safety program.
7. What is a Failure-to-Perform provision?

References

Berg, B.L., 1999. Policing in Modern Society. Butterworth-Heinemann, Boston, MA.

Purpura, P., 1993. Legal concerns in loss prevention. In: Fay, J. (Ed.), Encyclopedia of Security Management. Butterworth-Heinemann, Boston, MA, pp. 462–467.

Further Reading

Looney, V.S., Whitley, T.F., 1993. Contract security: Contracting for guard services. In: Fay, J. (Ed.), Encyclopedia of Security Management. Butterworth-Heinemann, Boston, MA, pp. 178–183.

CHAPTER 11

Managing Physical Security

What You Will Learn

- The two types of physical security.
- Factors that determine the selection of physical security safeguards.
- Concentric protection and its uses.
- The protective advantages of perimeter fences.
- The types of security lighting.
- The three main functions of sensors.
- The value and function of an intrusion-detection system.
- Lock and key systems.
- The two-person rule.

INTRODUCTION

Buildings are constructed to meet purposes: churches are places where people pray, schools are places where people learn, and palaces are symbols of power and status. All places for human assembly, regardless of purpose, are arranged with physical security in mind. Indeed, physical security can be the sole purpose of a facility such as a nuclear weapons storage site or a prison.

TYPES OF PROTECTED ASSETS

The term physical security refers to a logical set of tangible elements that protect selected assets. The tangible elements are integrated and mutually supporting. In an intrusion attempt, for example, a fence slows an intruder down, sensors send alarms, lighting makes the intruder visible, and closed circuit television (CCTV) cameras track the intruder's direction of travel.

A protected asset can be a site or something within a site. A site is often demarcated by a boundary, which can be a property line, a roadway, or

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00011-6

terrain features such as rivers and shorelines. A portion of the surrounding land, although not an actual part of the site, is sometimes included under the umbrella of protection.

When the protected asset is within the site, its location can be small, such as a cabinet or room, or large such as a wing of a building, the entire building, or a group of buildings. A group of buildings could be a college campus or an entertainment park. Some structures are assets that contain other assets within, such as planes carrying passengers, ships carrying cargo, or freight trains carrying chemicals.

SAFEGUARDS

There are two types of security safeguards: human and physical. One cannot be functional without the other. In the previous chapter, we discussed the human safeguard—security officers—and in this chapter, we'll look at physical safeguards. Physical safeguards vary widely and for various reasons. One of those reasons is the nature of the target. In security lingo, the target is the thing being protected against a threat. A target can be a physical object such as the Hope diamond; a nonphysical object such as the formula for Coca-Cola; human objects both individually (e.g., the President of the United States) and collectively (e.g., tourists visiting Egypt); or a large steel structure such as the Golden Gate Bridge. For purposes of clarity, we will refer to the target as a facility or a site. Both are catch-all terms that can mean anything from a grocery store to an entire city.

FACTORS IN SELECTING SAFEGUARDS

Now that we're on the same sheet of music, let's look at factors that influence the Chief Security Officer's (CSO's) choice of physical safeguards.

Environment

The area surrounding the facility will greatly influence the choice of safeguards. A fertilizer plant in Nebraska will require safeguards markedly different from those required for an office building in Manhattan or an ammunition plant in the desert of Arizona. For example, within the set of safeguards for the fertilizer plant may be nothing more than deadbolt locks on the doors and incandescent lights above them; the office building may opt for electronic locks and cameras at entrances and exits; and the ammunition plant may go with steel-reinforced doors with high-security padlocks and an electromechanical alarm.

Forces of Nature

Also at play in the selection of safeguards are the environment's climate and weather. Certain sensor devices cannot or do not work well in extreme temperatures. Others are vulnerable to floods, earthquakes, and sinkholes, and still others are susceptible to interfering effects of noise and vibrations from external sources such as aircraft flying overhead or heavy vehicles traveling on adjacent roadways. Then, there are those affected by smokestack releases and small animals.

Crime

Crime is a major influencing factor. The assessment of risk that precedes selection of safeguards will reveal the nature, intensity, and repetitiveness of criminal acts that have occurred in or near the facility at the present time and during the recent past. The apparent crime pattern will dictate the types of counteracting safeguards. Opportunists and nonprofessional criminals can be psychologically deterred when they believe a target is well protected. In this case, the safeguard is image. Safeguards against crime can have two purposes: prevention and postincident investigation. A convenience store, for example, will prevent or minimize loss by placing unneeded currency in a floor safe that cannot be opened except at a certain time and with the use of a second key infrequently available. The safe is a device for reducing loss. A video camera above the cashier's station is a device for aiding a postincident investigation.

Terrorism

Terrorism is a threat that defies standard safeguards. A group willing to sacrifice the lives of its members will overwhelm the average facility's protective shield. The CSO will want to know if there's a terrorist group having an interest in attacking the facility. If so, then he or she will want to know the reason behind it. Would the attack be made to intimidate or coerce, obtain publicity, make a political statement, destroy a critical asset? The CSO will make a judgment also about the probable method of attack. Would it be made with force or stealth? Would the attack involve firearms, an improvised explosive device, or even a bacterial agent?

Relative to the terrorist threat, the thinking process of a CSO at a government building will be much different than that of a CSO at a biological research lab. Each will have a different set of critical assets within, a different site configuration, a different external environment, and different human-dictated constraints within and outside of the site. The choice of safeguards will be

determined by the probable characteristics of the threat and the known characteristics of the site.

Site Characteristics

As stated, safeguards correspond both to the nature of the threat and the nature of the site. Fig. 11.1 shows the large number of safeguards to choose from. Selection of site safeguards is determined by the following:

- Size, layout, utilities, and compositional materials.
- Internal activities.
- Assets in or forming a part of the site.
- History of threat occurrences at the site.
- Security experience of the CSO.
- Philosophy of the site's ownership or management.
- Culture of the workforce.
- The surrounding community.
- Social and political constraints.

CONCENTRIC PROTECTION

A CSO in a high-security facility often abides by a concentric protection or defense-in-depth scheme; that is, overall protection will have several rings of security that in the abstract look like a shooting target. The diagram at Fig. 11.2 abstracts the theory of concentric protection. The outermost ring, which is at or on the far edge of the perimeter, might be a clear zone in which the approach of an intruder or intruder force can be seen by human and/or electronic means. The next ring might be a wall or fence, and then another wall or fence. Supplementing the walls or fences might be guard posts, patrols, detection sensors, CCTV cameras, and security lighting. The next ring might be sentry-protected and electronically controlled doors to a building or a complex of buildings. Within the building might be another ring of security consisting of access-controlled exclusion areas, and yet another ring within the exclusion areas might consist of safes, vaults, and similar containers, inside of which might be motion-detection devices. The theory operates on the simple premise that an attempted intrusion will have a lesser chance of success when multiple layers of protection stand in the way.

Perimeter

The usual starting point in assessing risk at a facility is the perimeter. Keeping in mind that the fundamental purposes of perimeter security are to

Physical Security Safeguards

	Security Control Center	Building Main Entrance	Secondary Personnel Entrances	Common Areas	Interior Doors	Ship and Receive	Perimeter
Electronic lock	X	X			X		
Access control	X	X	X		X	X	
CCTV monitors	X						
Security panel	X						
Integrated server	X						
Annunciator	X						
Lighting controls	X						
Fire panel	X						
HVAC controls	X						
Comm system	X						
Hi-Sec padlock		X	X		X	X	
CCTV cameras		X	X	X	X	X	X
Intercom		X	X			X	
Door closer		X	X		X	X	
Motion lighting		X	X			X	X
Reinforced doors		X	X		X	X	
X-ray equipment						X	
RFID/Bar code						X	
Barriers							X
Fence sensors							X
Electronic gates							X
Guard house							X
Boundary sensor			X		X	X	X
Motion sensor						X	X
Proximity sensor						X	X
Lighting		X	X			X	X

FIGURE 11.1

A single building can be protected with numerous safeguards.

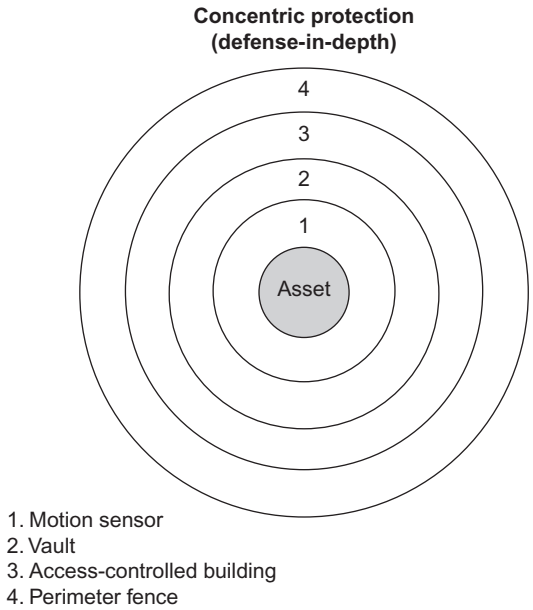


FIGURE 11.2
The protected asset is enclosed within several protective layers.

detect, deter, and delay unwanted intrusion, the CSO looks for an attainable balance between what is desirable and what is acceptable. To illustrate, the desire may be to maintain absolute integrity by erecting a formidable fence or wall on the property line supplemented with a patrol force, intrusion sensors, and a clear zone. However, when such measures happen to be forbidden by law, social mores, or terrain, the CSO will have to devise an accommodating protective scheme, yet one that is attainable and effective at an acceptable level.

Barriers

Barriers vary according to purpose:

- Control the movement of property, people, and vehicles.
- Segregate or compartmentalize.
- Provide a physical shield to objects, materials, and processes.

Within and around a protected site should be man-made structural barriers, for example, fences, walls, floors, roofs, bars, grilles, and bollards. Bollards are post-like crash-resistant devices placed forward of building

entrances. Decorative forms of the bollard are concrete flower planters. Around the property may be natural barriers such as mountains, ravines, rivers, lakes, and oceans. To the extent possible, the CSO should take advantage of natural barriers and complement them with man-devised barriers and sensors.

Barriers keep people in and out and can be used to channel pedestrian and vehicle traffic. Both natural and man-made barriers can require movement along roadways and pathways that are set a distance away from the locations of critical assets. They can also make movement visible.

Jersey barriers placed in tight curves at the approach to a gate are effective in slowing the speed of vehicles, a tactic that gives gate guards a greater amount of reaction time should a driver attempt to "run the gate" or crash into it.

Three security advantages can be obtained through the intelligent use of barriers. First is psychological deterrence. A potential intruder is dissuaded when access appears problematic. Second is the actual difficulty in getting through physical barriers. Third is the benefits of reducing the cost of security staffing by substituting barriers for people.

Chain-link is used almost exclusively for perimeter fencing. The US Army's Physical Security Manual requires the height of the fence to be 7 ft high, have a galvanized mesh of 9-ga thickness, and mesh openings not larger than 2 in. The selvage at the bottom and top of the mesh is twisted and barbed. The mesh is taut and sturdily attached to rigid metal posts set in concrete. The depth of the concrete settings will vary according to soil conditions (e.g., deeper settings will be required in sand and shifting or loose soil).

The integrity of the fence line can be jeopardized by crawl-through openings at the bottom. These openings are usually the result of natural erosions, as well as man-made culverts and ditches. Compensation can be obtained by blocking the openings with additional chain-link or steel mesh and grillwork.

Protection is added when the fence has three strands of barbed wire or razor tape strung equidistantly between supporting arms attached to the top of fence posts. The top guard faces outward and upward, adding at least 1 ft to the overall height of the fence. The photo at Fig. 11.3 displays a top guard arrangement.

An alternative to a chain-link fence is a masonry wall. It, too, will have a height of 7 ft, a top guard or shards of glass cemented to the top surface, and blocking material at ground-line openings.

FIGURE 11.3
A top guard adds protection against climbing over a fence. *iStockphotos.*

Environmental design may be used in any number of crime prevention strategies. To cite a few:

- In external areas, boundaries may be displayed as impassable physical structures or as symbolic barriers such as hedges and shrubbery.
- The dividing point between public space and restricted space can be made clear with the use of trees and heavy foliage.
- Office buildings on the fringe of a restricted area can have windows that allow employees to spot strangers moving toward the area.

SECURITY LIGHTING

According to Roper (1997), security lighting should be used in conjunction with other protective measures such as fixed guard posts, foot patrols, fences and other barriers, and alarm systems. The protective capability of lighting is diminished in the absence of observation by a security officer force. A preventive or reactive response cannot be launched without first having someone in place to confirm an intruder's approach or penetration attempt. A modicum of protection is afforded by the psychological deterrence of lighting, but the greater value by far is lighting supplemented by human intervention.

Lighting can be helpful also when security officers examine entry badges, inspect entering and departing vehicles at gates, and control access at stationary posts.

Protective lighting is often categorized by type or purpose:

- Flood lighting is continuous illumination of a protected area during the hours of darkness by means of overlapping cones of light from overhead lamps (e.g., pole- and roof-mounted lamps).
- Glare lighting is lighting directed outward from the protected area so that the intruder is made highly visible and is not allowed to easily see what lies ahead. Glare lighting also adds protection to security officers behind the light source.
- Controlled lighting is illumination that does not impede nearby operations such as traffic moving on a roadway, aircraft landing at an airport, and ships traveling in navigable waters.
- Moveable lighting consists of manually operated portable lamps. They often supplement or temporarily replace other forms of lighting.
- Emergency lighting consists of standby lamps that come into operation when a primary lighting source goes out of operation due to power failure or emergency condition. The power source of emergency lighting is usually a backup generator or an arrangement of heavy-duty batteries. Lamps mounted in a stairwell that automatically light up during a fire fall into the emergency lighting category.

A variety of lamps are commonly used for security purposes:

- The incandescent lamp operates the same way as the light-bulb type of lamp used in homes. It immediately goes on when electric current is applied to a filament. Incandescent lamps are manufactured in a wide variety of wattages and sizes and meet the requirements of many security needs.
- The fluorescent lamp, also common in the home, has an elongated tubular shape and is typically ceiling mounted. It is efficient and economical but casts illumination over a relatively short distance.
- The gaseous discharge lamp goes on when electric current is applied to a luminous gas. Mercury (blue–white color) and sodium (golden-yellow color) lamps operate on the gaseous discharge principle. These lamps have a relatively long life and produce a high degree of light, but arrive at full illumination slowly.
- The quartz lamp produces a bright white light that when directed into the eyes (e.g., the eyes of the intruder) is intensely glaring. This lamp reaches full illumination almost as quickly as the incandescent lamp and is often utilized in outdoor and portable applications where brightness facilitates detailed work such as that performed at the scene of a vehicle crash.

Lighting specifications as to purpose, location of use, efficacy, efficiency, light distribution, coverage, illumination distance, and foot candles are obtainable

from manufacturers, publications, and industry associations such as the Illumination Engineering Society of North America.

SENSORS

Sensors perform three functions: (1) detect intruders, (2) open a portal, and (3) turn another device on or off. For example, sensors that react to motion, sound, and body heat are used to detect intruders; a sensor that reacts to the presentation of a card key opens a door; and a sensor that reacts to changes in light conditions will turn security lights on or off.

Sensor Reactions

Sensors operate using many different principles. Types of sensor configurations are shown in Fig. 11.4. Intrusion can be detected through:

- Breaking of a circuit.
- Interruption of a light beam.
- Movement.
- Sound.
- Vibration.
- Change in an energy field.

Sensors variously detect penetration of a boundary, unexplained presence within a zone, and unexplained presence in close proximity to a zone or a protected object. Intrusion detection sensors are calibrated to activate when a monitored norm is altered outside a predetermined level. The activated sensor causes an alarm to be sounded or a signal to be sent to a monitoring station such as the security control center of a protected facility.

Sensor Groups

Detection sensors, both exterior and interior, are essential components in any serious protective scheme. When properly installed, calibrated, and serviced, sensors are accurate and reliable, not to mention economical compared with the cost of labor. Sensors that operate out of doors are said to be exterior sensors. Sensors that operate within a structure are called interior sensors. Some sensors can be exterior and interior.

The sensor group selected will be influenced by the physical nature of the environment in which it will operate. For the outdoor environment, the factors to be considered include topography, soil composition, weather, and radio or electrical interference. For the indoor environment, the choice

Sensor configurations

Sensor type	EXIN		PAAC		VOLI		LSTF		COVICV		
Vibration	X		X			X		X		X	
Vibration		X	X			X					X
Taut wire	X		X			X		X		X	
Magnetic field	X		X		X			X	X		
Electric field	X			X	X			X		X	
Fiber-optic cable	X		X			X		X	X		
Seismic	X		X			X		X	X		
Pressure	X		X			X		X	X		
Pressure		X	X			X			X		
Ported coaxial	X			X	X			X	X		
Active infrared	X			X		X	X			X	
Active infrared		X		X		X	X			X	
Active infrared		X		X	X		X			X	
Passive infrared	X		X		X		X			X	
Passive infrared		X	X		X		X			X	
Microwave	X			X	X		X			X	
Microwave		X		X	X		X			X	
Video motion	X		X		X		X				X
Video motion		X	X		X		X		X		
Magnetic switch		X	X			X					X
Capacitance	X		X		X			X	X		
Capacitance		X	X		X				X		
Sonic		X		X	X					X	
Ultrasonic		X		X	X					X	

EX, exterior; *PA*, passive; *VO*, volumetric;
IN, interior; *AC*, active; *LI*, line;
CO, covert; *VI*, visible; *CV*, covert or visible

FIGURE 11.4
This chart depicts configurations by type of sensor.

can be affected by building structure, tremors, and sound resulting from the facility's operational activities. Sensors are also selected on the presumed capabilities and intentions of potential intruders, and the capabilities of the security force to respond to and effectively negate intrusion attempts.

Distinct Characteristics of Sensors

Sensors are grouped according to distinct characteristics:

- Exterior
- Interior
- Passive
- Active
- Volumetric
- Line detection
- Line-of-sight
- Terrain-following
- Covert
- Visible
- Covert and visible

Exterior sensors: These devices are typically installed in open areas, such as in a clear zone; atop, upon, or inside a fence or wall; and under the ground. They can be manufactured to withstand extreme temperatures and operate in severe weather conditions. However, by comparison with interior sensors they have a reduced probability of detecting intrusion and an increased false-alarm rate. This results mainly from uncontrollable factors such as standing water, blowing debris, and stray animals. When uncontrollable factors are present, two or more sensors, each operating on a separate principle of detection, can be set up to cover the same area or asset.

Interior sensors: Unlike their exterior counterparts, these sensors are unaffected by weather and terrain features and are less affected by uncontrollable factors. In addition to detecting intrusion, interior sensors can be used to detect fire, contaminated air, and in-progress attempts at sabotage or theft of critical assets.

These sensors detect intrusion into or within a building or complex of buildings and are largely (although not exclusively) unsuitable for outdoor applications. They fulfill their functions by detecting the following:

- Approach and/or penetration of an intruder.
- Movement of an intruder within a protected area.
- Touching or movement of a protected object.

Interior sensors are not immune to false alarms but given the relatively benign environments in which they operate, they are reliable to a higher degree than exterior sensors. When an exterior sensor is defeated, the culprit is almost always an outsider trying to get in. When an interior sensor is defeated, the culprit can be an inside employee or an intruder.

Passive sensors: This sensor group does not emit energy. It reacts to energy emitted by the intruder or to a change in a field of energy caused by the intruder. The phenomena reacted to can include heat (e.g., body heat of the intruder), vibration (e.g., opening of a door), sound (e.g., breaking glass), and capacitance (touching an object or being in close proximity to it). The passive infrared sensor, a commonly used sensor, detects thermal energy (body heat), and therefore falls into this group.

Active sensors: These sensors send energy into a defined area, which may be a zone through which an intruder must pass to reach the protected asset. The energy, usually radio frequency (RF) energy, is disturbed when it encounters something that should not be in the zone. The disturbed energy is returned to the sensor device. This requires a transmitter for sending energy and a receiver for receiving returned energy. As opposed to a passive sensor, which emits no energy, the energy of an active sensor is able to detect an adversary outside the protected zone.

Volumetric sensors: This sensor group detects movement in a given volume of space (i.e., a zone room). The zone is filled with an energy form such as magnetic, electric, or RF energy. When the "normal" pattern is altered to a degree indicative of movement within the zone, the sensor activates. An advantage of the volumetric sensor is that it detects movement anywhere within a zone, whereas boundary sensors can only inform the monitoring station that a penetration occurred on the edge of the zone.

Line-detection sensors: These sensors react to movement. They can be placed on fences, gates, doors, and windows to detect vibration; on objects to detect touching; and on buried cables to detect movement of soil caused by above-ground passage.

Line-of-sight sensors: These sensor devices have a transmitter and receiver. A continuous signal, such as a photoelectric beam, moves between the two. When the signal is interrupted, the sensor reacts.

Terrain-following sensors: This sensor group might better be called the nonline-of-sight group because it can be used just about anywhere the line-of-sight sensor can't be used. Also, "terrain-following" is a little misleading because in addition to the sensor being functional on irregular ground surfaces, it is functional on fences and walls that are curved or angular. On irregular

ground surfaces, the sensor is typically a buried cable that variously reacts to changes in electric or magnetic fields radiating upward, and to pressure at ground level caused by the weight of a passing person or vehicle. On fences and walls, the terrain-following sensor reacts to magnetic and electric field changes, vibration, and tension.

Covert sensors: As the name suggests, sensors in this category are concealed from the view of an intruder. A rationale for use of covert sensors is apprehension of the intruder.

Visible sensors: These are visible to an intruder. A rationale for use of visible sensors is deterrence.

Visible sensors: These sensors can be used both ways.

Sensor Types

As explained, each of the sensor groups has a distinct characteristic, e.g., exterior or interior. Sensors are also categorized by what they detect: vibration, motion, sound, interruption of an electric field, a magnetic field, or a photoelectric beam, and weight. These are types of sensors, and a sensor type will fall into any or all of the sensor groups. For example, a magnetic field sensor (a type) can be used in the exterior environment (group). The chart titled "Sensor Configurations" depicts the relationships.

The more common types of sensors are described below.

- *Vibration:* This type of sensor is attuned to vibrations caused by pulling on or cutting through a fence, breaking glass, and sawing or smashing through a wall. A transducer in the sensor detects low-frequency energy associated with brute force intrusion. In the exterior environment, the sensor is often mounted on a fence fabric (metal mesh or chain-link) or on the top mount of a fence (barbed wire or razor tape). In the interior environment, the vibration sensor can be installed on or inside walls or on glass surfaces.
- *Taut wire:* In this application, a strain-sensitive cable is mounted on a fence horizontally. When the cable is stretched, such as by climbing or shaking the fence, the taut wire is stretched beyond a tolerance level, causing an electric circuit to be broken and a signal sent to the monitoring station. A variation is a conduit containing a line that transmits and receives electrical energy. Cutting, shorting, or removing the conduit will alter the flow of electrical energy passing along the line.
- *Magnetic field:* A magnetic field sensor reacts to the movement of metal in a magnetic field set up by wires buried in the ground. They are useful in detecting weapons and/or vehicles moving into a guarded area.

- *Electric field:* This device creates an electrostatic field through an array of wire conductors and an electrical ground. Change or distortion of the field results when an intruder enters the zone.
- *Fiber-optic cable:* It helps to think of this device as a "pipeline of light." The pipeline is a cable that encases a light-carrying fiber strand. The cable can have any number of curves without affecting the light; however, once the cable has been installed, any bending beyond a preset tolerance will trigger an alarm. Fiber-optic cables are often arranged in a mesh pattern placed slightly below the surface of the ground. A person or vehicle passing over the ground causes the mesh to bend.
- *Seismic:* This sensor consists of geophones placed under the soil. Vibration of the soil, such as that caused by a walking person, creates high-frequency energy which in turn activates the sensor.
- *Pressure:* In the exterior environment, this sensor consists of a hose containing a pressurized liquid. Like the seismic sensor, it is placed under the soil. A person walking on the soil changes the pressure. In the interior environment, the sensor can be a pressurized mat placed under a carpet or flexible flooring.
- *Ported coaxial cable:* This sensor detects movement of humans and metallic material. Inside the cable is wiring that radiates a signal. The cable's sheathing has holes (i.e., ports) that permit the signal to "leak out." The cable is buried. When the signal comes into contact with a person or metal object, the sensor activates.
- *Active infrared:* This sensor can be used outdoors and indoors. Think of it as an electronic trip wire: a transmitter sends an infrared beam to a receiver, and activation occurs when the beam is interrupted. In the outdoor environment, the active infrared sensor can be free-standing, i.e., it can be moved from place to place. Indoors, the transmitter and receiver are typically wall-mounted, with the beam passing across entrances (doors and windows) and intruder pathways (hallways and staircases). Another form of the active infrared sensor broadcasts a curtain-like pattern of infrared energy extending to the boundaries of the protected area. The energy pattern is reflected back to a receiver. The reflected energy pattern is analyzed, and if found to be in an altered state, then it causes an alarm.
- *Passive infrared:* The passive infrared sensor does not transmit at all. It is sensitive to thermal energy received from the intruder. Typically, the sensor covers several contiguous zones. Activation occurs when an intruder crosses two adjacent zone boundaries or twice crosses the same boundary within a specified time. Like the active infrared type, it can be used indoors and outdoors.

- *Microwave:* This motion-detecting device transmits a microwave signal along a perfectly straight line that can extend as far as 1500 ft. A zone is created on both sides of the line. Movement within the zone sets off an alarm. A microwave sensor can be supplemented with a passive infrared sensor. An alarm is sent when both sensors react to a change in their different energy fields. These sensors are often installed along a perimeter fence or wall and arranged to detect an approach to the zone, an actual intrusion, or both. In high-security situations where there is an advantage to viewing and recording intruder movement, the microwave alone or the microwave in tandem with passive infrared can be supplemented with CCTV cameras. Microwave sensors can be used indoors as well.
- *Video motion:* This sensor is called a video motion detector (VMD), and it can be used outdoors and indoors. A CCTV camera views a scene of interest. Movement within the field of view sends an alarm signal. Outdoors, VMDs are usually mounted on towers, light poles, and walls. Indoors, they are mounted on walls and ceilings, with the usual scenes of interest being doors, hallways, and rooms.
- *Magnetic switch:* This simple device activates when the magnetic field between two contact points is broken. For example, one contact is mounted on a window with a corresponding contact on the windowsill. When the window slides open, the contact is broken and an alarm signal is sent.
- *Capacitance:* The capacitance sensor is similar to the electric field sensor. Three closely spaced wires produce an electric field around an object. The capacitance of the electrostatic field is changed when an intruder approaches or touches the object. In the outdoor environment, the object can be a handle on a gate or delivery door; in the indoor environment, it can be a door knob, lock, combination dial, or the protected asset.
- *Sonic:* This sensor operates on the principle of sound detection. It is typically mounted on a stable interior surface that serves as a barrier. It reacts to sound waves such as those produced by forced entry. When noise is unpredictable (sonic boom, thunder, engine backfire), it can be supplemented with another sensor operating on a different detection principle.
- *Ultrasonic:* This motion-detection device reacts to high frequencies associated with intrusion attempts. The sounds of metal striking metal, an acetylene torch in operation, and the shattering of concrete or brick are in the high-frequency range. It is usually wall- or ceiling-mounted and supplemented with another sensor form such as the passive infrared sensor.

Detection Reliability

Infallible is not a term associated with sensors, or for that matter any other detection device. The reliability of detection hinges on the following:

- *Amount and pattern of energy emitted by the intruder*. The more definitive the pattern, the greater the reliability of the sensor.
- *Size of the intruder*. The larger the intruder, the greater the reliability.
- *Distance between the sensor and the intruder*. Reliability rises as distance shortens.
- *Speed at which the intruder is moving*. Very slow and stealthy movement decreases reliability.
- *Direction of intruder movement*. Lateral movement is more easily detected than straight-on movement.
- *Characteristics of the energy waves of the intruder and of the environment in which the sensor operates*. The greater the contrast between the energy waves of the intruder and the environment of the zone, the greater the reliability of detection.

INTRUSION DETECTION SYSTEMS

An intrusion detection system (IDS) is an arrangement of one or more sensors, one or more sound alarms (enunciators), alarm processor, alarm monitoring station, circuitry to send and receive signals, a person or persons to monitor and operate the system, and security officers to respond to suspected intrusions. Signals within the IDS move from one device to another along wires or wirelessly.

Assessment

When the IDS senses an intrusion and sends a signal, the operator of the system "reads" an alarm panel and determines the location of the intrusion. The officer assesses the nature of the intrusion, the assessment is given to one or more security officers, and the security officers go to the scene to investigate.

The IDS control panel is almost always located in a security control center or on a console monitored by an officer performing other duties such as checking passes. IDS sensors can be standalone, such as free-standing devices that search for movement ahead and sensors buried in the ground. Most sensors are attached to physical structures such as fences, doors, windows, and locked containers.

Three Characteristics

The CSO charged with selecting intrusion-detection sensors would do well to examine the following:

- Reliability, which takes into account their sensitivity, the nature of the environment, and the assumed behavior of the intruder.
- Frequency of alarms resulting not from intrusion but from faulty equipment, poor installation, maintenance, calibration, and a host of uncontrollable factors such as loss of power, earth tremors, high wind, heavy snow, flooding, and the movement of animals.
- Ability of the sensors to detect attempts to thwart or circumvent detection. Resistance to defeat can be increased by overlapping sensors in contiguous coverage areas, installing more than one sensor per coverage area, and building into a single-device multiple sensors that operate on different principles.

The objective of the CSO is to establish an IDS that has high reliability, a low false-alarm rate, and high resistance to defeat. After selecting sensors, the CSO selects an alarm processor, a monitoring capability, and a communication mode that connects the components. Fortunately, a wide variety of alarm processors are commercially available in off-the-shelf packages that include computer hardware, software, operating procedures, and training for system operators. The software for most of these systems allows the purchaser to choose options that correspond to specific needs.

Monitoring and Communication

The monitoring function can be performed at a security console operated by the purchaser's own security group or at a central alarm station operated by a vendor. A common feature is both an audible and visible alarm enunciation. The audible signal is usually a buzzer, horn, or other distinctive sound. The visual signal is usually a flashing light and alarm data displayed on a screen such as a CCTV monitor or the screen of a desktop computer. The alarm data can consist of text, icons, maps, floor layouts, and other formats that tell the operator what is happening and where. A highly sophisticated system can also provide a real-time CCTV view of the penetrated area and the path of the intruder. Instructions in text and/or sound prompt the operator to initiate appropriate response actions.

The communication protocols of the system will vary according to purpose and agreeable interfaces. In some cases it will be advantageous, if not necessary, to place a preprocessor between the computer and the rest of the

system. The purpose of the preprocessor is to eliminate signal delay by reducing tasks that would otherwise be handled by the computer.

Tamper Detection

Nearly all alarm systems have a tamper detection feature (called line supervision) that indicates if a line has been cut or bypassed. An intruder who knows a system has line supervision may attempt undetected entry by entirely cutting off the system's power supply. A system is vulnerable to this form of attack when it lacks an immediately operating automatic restart capability. For this reason, it is critical that an alarm system have an uninterrupted power supply and alternative power sources.

LOCK AND KEY SYSTEMS

By any reckoning, the lock is the most widely used physical security device, yet it is hardly foolproof. All locks are vulnerable to physical force, and against a determined and knowledgeable intruder, the best a lock can be expected to achieve is delay. The duration of delay is largely a matter of the locking principle and the resistance of the lock to force. Locks are also vulnerable, although to a lesser degree, to nonforce techniques. A key-operated lock can be picked and impressions made secretly of keys. A combination lock can be defeated by manipulation of the spindle or compromise of the lock's numeric or symbolic code.

Types of Locks

Locks operate on various principles and are manufactured in a variety of sizes, shapes, and defeat-resisting abilities. Locks commonly used in business, industries, and the military are usually of three general types: key, combination, and electronic. Fig. 11.5 is a high-security electronic lock.

Key lock: This multipurpose lock opens on the insertion and turning of a key. In a lock that secures a door, the turning action of the key causes the bolt to retract from the strike (a recess in the door frame); in a padlock, the turning action allows the shackle to be lifted free. Many forms of key locks have an interchangeable core (the component that receives the key) that can be removed and replaced by a core that operates with a different key. Variations of the key lock have names that correspond to their internal movements. For example, the warded lock has ward cuts in the key that correspond to wards (obstructions) in the keyway or lock; the wafer or disk tumbler lock has spring-tensed wafers that retract when the correct key is inserted; the pin

FIGURE 11.5
In this electronic lock an internal battery moves the cylinder. The key contains embedded data about the key holder, authorization level, and the times and days of permitted access. *Videx Corporation.*

tumbler lock opens when pins are moved by a key having cuts in the key blade that line up with the pins; the lever lock has spring-tensed levers that properly align upon insertion of the correct key; and the deadbolt lock has a bolt that retracts when the correct key is turned.

Combination lock: This lock is incorporated in padlocks, safes, vaults, and doors. The operator turns the spindle in a specified order of right and left directions to reference points on a dial. Tumblers inside the lock release the locking mechanism. Three is the usual number of tumblers, although four or five tumblers are a feature of so-called high-security locks.

Electronic lock: In this category are digital locks that open when the correct code is entered by pushing buttons, and electromechanical locks that open when an electronic signal is received. The received signals arrive at the lock after the user's identification and right to entry are verified. Verification can be made by an assessment of the distinguishing features of the user such as signature dynamics, fingerprints, and the retina. In some devices, a handheld key contains in electronic format the user's identification and access privileges plus battery power to operate the cylinder.

Key Control

The key-operated lock used in the typical office building will open for anyone who possesses the correct key. This simple fact explains why key control is so vitally necessary when protection is an objective of building management.

A variety of physical techniques are available for protecting keys not yet issued. These include strategies such as keeping keys locked inside a wall-mounted box, filing cabinet, floor safe, and so on. The degree of physical protection, of course, can vary widely with the choices of protection determined by building management.

A popular high-security approach is to store keys in a locked and permanently affixed cabinet in continuous view of security personnel or other trusted employees. A less secure approach is to store them in a penetration-resistant container that is not continuously under observation. The container's penetration resistance in this case must be greater than that of any locked door in the protected premises. A two-dollar padlock on a key cabinet makes no sense at all when the keys in the cabinet open doors giving access to assets worth thousands.

Procedural Control

The physical side of key control is relatively simple and problem free, at least in comparison to the procedural side. Why? Because procedures involve people and people are human. In Fig. 11.6, there is a person checking a lock on a cargo truck. People make errors of judgment, something a lock can never do. The human procedure that requires demonstration of a right and need to pass beyond or open a locked door is likely to be met with: "What do you mean I can't have a key? I supervise that office." Breakdowns in procedures occur not because keys can't be physically protected but because the human element of the key control system can't function properly.

A usual reason for key control being difficult is the notion that status in the organization confers a right to possess keys. But does the CEO really need a key to every door in the building? Does the Chief Financial Officer (CFO) really need a key to the power plant?

Another unacceptable reason is the proposition that long and faithful service should be rewarded, such as giving a multiple-entry key to an employee who everyone likes and trusts. Close behind is the idea that convenience should count for something. It is convenient, for example, for the boss' secretary to possess a master key so that when an employee in her department wants to get into a locked area, she can open the door without having to call a

FIGURE 11.6
Checking locks on trucks is standard procedure. *Burns International Security Services.*

security officer. Pretty soon she is handing the key to anyone who asks for it. After a while the key gets lost and all locks opened by that key have been compromised.

The least supportable rationale for issuing a key is to silence a complainer. Putting grease on the squeaky wheel is often the reason for circumventing good practice. "He just kept bugging me until finally I issued him a key."

What is at issue here? Nothing less than the compromise of an entire system. The compromise operates like a disease eating away portions of a living body. A nibble here, a nibble there. Closet keys lost, desk keys stolen, office keys misplaced, floor keys duplicated. Then comes the big problem. Too many submasters issued, the master lost, the grand master unaccounted for. The system is soon dead. No choice but to start over.

Compromise

One of the fastest ways to compromise a key system is to disclose the cut code numbers established by the lock manufacturer. These numbers, which are often cut into the thumb grip, identify all keys in a system of keys. They serve as a convenience to the purchaser in placing later orders with the manufacturer. The code number on a key also tells a locksmith that duplication is permitted or forbidden. The custodian of a key system should never issue

a marked key, but if issuance becomes absolutely necessary, the code number should be ground off.

Unauthorized duplication is made more difficult when the keyway of the locks in the system will accept a single key blank, one that is available only to the registered owner of the system. Still, this is not a foolproof precaution because the number of ways to configure the guide cuts in a blank is finite. A determined person with locksmith skill and knowledge can eventually come up with a key blank that will work.

One more point on key blanks is worth mentioning. When duplication of keys is done in-house, the key blanks should be protectively stored apart from the key-grinding equipment. A signature receipt form is the usual administrative device for key accounting. The form can also be used to impress upon the recipient the concern of management by including, for example, an acknowledgment that personal responsibilities will be met. These might include protecting the key, not loaning it, not duplicating it, and turning it in when asked to do so.

Periodic Inventory of Keys

Keys that are in daily use for gaining access to particularly sensitive areas, such as keys held by security officers, cleaning staff, and building maintenance employees, require a protective approach that emphasizes periodic inventory. The frequency of the inventory can vary. For example, security officers likely turn in their keys at the end of each shift. Signed receipts, log books, or other records reflect the transfer of keys from officers going off work to those coming in.

For cleaning staff, the frequency of the inventory might be once per day, once per week, or not at all if the cleaning routine calls for security officers to unlock doors to the areas to be cleaned. For building engineers, keys might be counted periodically, depending on the sensitivity of the areas they service and how the engineers are supervised.

Two-Person Rule

When the protected area is so sensitive that unaccompanied entry cannot be permitted, key access can be controlled using a two-person rule. Access to bank vaults often requires the two-person rule, as shown at Fig. 11.7. One version of the rule is to place the key in a penetration-resistant container maintained by a key custodian (who may or may not be a security officer). The key custodian issues the key only at the simultaneous request of two predesignated persons. A variation is to have two separate locks, with the keys

FIGURE 11.7
The two-person rule is almost always used when the asset is of high value. *Burns International Security Services.*

held by the key custodian. In this way, both of the predesignated persons must sign for their keys and must be present with their keys at the entry point before either of them can get in.

Dual Systems

In some situations, it may be preferable to operate two systems of key control: one nonsensitive and one sensitive. Locks to the nonsensitive areas would be of one brand or one model, and locks to the sensitive areas would be of a different brand or model. Two advantages are present in such an arrangement. First is cost. There is no point in purchasing high-security locking hardware for all doors when only some doors require high-security protection. Cost also weighs heavily when a compromise in the security system requires replacing or recombinating lock cores. The second advantage is eliminating the possibility that a lock core previously used in a low-security area (where keys are less controlled) would be placed in a high-security area. The difference in brand or model would alert the key custodian to prevent interchanges.

Finally, many fine software programs are being brought to market for companies wanting to improve the management of their key control systems. These programs variously provide graphics that depict the hierarchy of keys in the system; identification of the persons to whom keys have been issued, when, by whom, and on what authority; tracking and crossreferencing keys; and computer-generated forms for requesting, assigning, turning in, and destroying keys.

CRITICAL THINKING EXERCISE

Herbert Marlowe, CSO of a major chemicals manufacturer, was called to the CEO's office. There with the CEO was the Chief Operations Officer (COO) and the Chief Financial Officer (CFO). The CEO handed Marlowe a diagram of a facility and said, We have just purchased this property. It has been empty for two years but is in good shape. We plan to manufacture acrylonitrile, which you may know is highly toxic in a gaseous form. The raw material will arrive by trucks and a train, and leave with finished product. The CEO reached out and used a finger to point out the locations of the truck delivery and departure areas and a railroad spur. He said, "The raw material is neutral, but I want it protected to the same degree the finished product is protected." He dropped his hand from the diagram and with a stern countenance, added, "I want you to come back to me in five working days with a security plan for this facility."

Marlowe answered, "Yes, Sir," and walked to the door. A voice behind him said, "One second, please. Make sure the plan does not impede operations." The instruction came from the COO. Marlowe turned again to leave but was stopped by the CFO who said, "And make sure the plan is cost effective."

During the return to his office, Marlowe was stopped by the company's Public Information Officer (PIO). The PIO said he had learned of the planned purchase and of the product to be manufactured. He told Marlowe, "Whatever you do, don't let the word get out. It will scare the heck out of the community, especially people living nearby."

Back at Marlowe's office he studied the diagram. The building or plant that would manufacture the product was a stand-alone structure. Behind it was the spur. Both were encircled by a chain-link fence. A pedestrian gate operated by a turnstile with an access control reader gave entry to the area around the plant. An administrative building and a parking lot were nearby, but outside the plant area. The entire property, consisting of 500 acres, was surrounded by a chain-link fence. On the exterior side of one section of the fence were trees and heavy foliage. The property had a single entrance point with a guard shack large enough for one security officer. The property sat back 200 yards from the highway. Vehicles entering and leaving the property traveled on a gravel road between the highway and the entrance gate.

You are to assume you are Herbert Marlowe. From what you have learned to this point develop a plan that will take into consideration the three pillars of a security program. Do not ignore the possible use of safeguards such as lighting, sensors, and guard posts; determine the number of guards you believe will be needed and the training appropriate for them; and identify the types of plans and other written guidance. Be sure to consider the instructions of the CEO, COO, and CFO, and the advice given by the PIO.

CONCLUSIONS

A facility's physical security posture is but one part of a larger functional program that typically includes security officer services, fire detection and suppression, access control, investigations, personnel screening, employee education, risk assessment, inspections, and audits.

The buzz term of this decade may turn out to be "integrated systems." The idea that economy and efficiency can be achieved by combining two or more independent systems is especially appealing to cost-conscious purchasers. The more-bang-for-the-buck philosophy has naturally led to the development of integrated office lighting/air conditioning systems with security systems featuring two-way communications between linked functions. Although called integrated, many of these systems retain aspects of functional independence, especially in regard to fire detection integrated with security. In Fig. 11.8, there is a checklist for assessing physical security features.

The concept of integrated systems points toward a much fuller merging of functions than has been seen to date. However, there are impediments. Of concern to fire experts are the integrity and reliability of the fire detection and alarm components. Absolute assurance, they say, cannot be compromised. Failure of a nonfire component affecting a fire component cannot be allowed. Experts worry, for example, that a security officer who has access to the integrated system will mistakenly change the system's fire-related program or operate the equipment in a manner that could override fire detection and annunciation. The facility's full program of security can be likened to an automobile engine. The parts are interdependent and function synchronously, with the CSO serving as driver and mechanic.

REVIEW QUESTIONS

1. Name the two types of physical security.
2. List four factors to consider in selecting security safeguards.
3. Describe the concept of concentric protection.
4. Name the advantages of perimeter fencing.
5. Name the types of security lighting and their purposes.
6. What are the three main functions of sensors?
7. How are sensors grouped?
8. List four of the most common sensor types.
9. What is the two-person rule?

Checklist for Assessing Physical Security

Yes	No	Environmental Factors	Yes	No	Countermeasures
____	____	Prohibitive seismic activity?	____	____	Control approach to the facility?
____	____	Poor surface and subsurface stability?	____	____	Fencing and other perimeter barriers?
____	____	Soil contamination?	____	____	Protective and/or glare lighting?
____	____	Severe weather potential?	____	____	Anticoncealment landscaping?
____	____	Prohibitive topography?	____	____	Gates?
____	____	Flooding potential?	____	____	Turnstiles?
____	____	Poor air quality?	____	____	Mantrap zones and cubicles?
____	____	Extreme temperature?	____	____	Guard towers and gatehouses?
____	____	Fire hazards?	____	____	Intrusion detection sensors?
____	____	Inadequate utility feeds?	____	____	Signage?
____	____	Inadequate emergency services?	____	____	CCTV?
____	____	High crime rate?	____	____	Electronic access control?
		Threats	____	____	Badges?
____	____	Crime in the facility?	____	____	Duress alarms?
____	____	Crime in the neighborhood?	____	____	Shielding against eavesdropping?
____	____	Traffic accident potential?	____	____	Blast and/or bullet resistant shielding?
____	____	Terrorist target?	____	____	Fire-rated walls/ceilings?
____	____	Kidnapping potential?	____	____	Penetration-resistant walls/ceilings?
____	____	Workplace violence potential?	____	____	Bar grates?
____	____	Bomb threats?	____	____	Vaults, safes, and secure containers?
____	____	Employee theft?	____	____	Mechanical and cipher locks?
____	____	Electronic eavesdropping?	____	____	Antipass back readers?
____	____	Sabotage?	____	____	Uninterruptible power systems?
____	____	Vandalism?	____	____	PC-assisted security control center?
____	____	Natural disaster potential?	____	____	Video archiving equipment?
____	____	Manmade disaster potential?	____	____	Alternate security control center?

FIGURE 11.8
A checklist can be helpful when evaluating the adequacy of physical security.

References

Roper, C.A., 1997. Physical Security and the Inspection Process. Butterworth Heinemann, Boston, MA.

Further Reading

Purpura, P.S., 2007. Physical security: lighting. In: Fay, J. (Ed.), Encyclopedia of Security Management, second ed. Butterworth Heinemann, Boston, MA.

CHAPTER 12

Managing Access Control

What You Will Learn

- The rationale for access control.
- Types of identification cards.
- Uses made of card keys.
- Methods of materials control.
- The concept of layered protection.
- Biometric identification.
- The pros and cons of closed circuit television (CCTV).
- The basic components of an intrusion detection system (IDS).
- Minimum expectations of an IDS.

INTRODUCTION

The business rationale for access control stems from the belief that the workplace must be safe for everyone and secure for property and process. In practice, the belief is carried out by eliminating harm to people, such as by controlling entry to a hazardous work zone or denying entry to persons posing a threat. The rationale extends to protecting property and preventing hostile acts that disrupt business operations.

A facility that requires even a minor level of protection exercises access controls. Indeed, a strong argument can be made that a facility without access controls is an unprotected facility. An access control system regulates movement into, within, and from a protected facility. The controls are placed on people, forms of transportation, and materials. The people typically affected are employees, visitors, customers, contractors, vendors, repair and salespersons, and deliverers. Transport forms include automobiles, trucks, motorcycles and bicycles, trains, buses, watercraft, and aircraft. Materials that are under control when entering can include raw materials, supplies, and equipment. Inside the protected area, controls can be placed on authorized movement and removal of cash, valuables, and sensitive documents. At exits to a

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00012-8

protected area, controls can be applied to finished products, scrap, and refuse, as well as hand-carried property.

EMPLOYEE BADGES AND VISITOR PASSES

A basic and time-honored access control tool is the employee identification card or badge. A workplace with few employees and low security needs may choose to rely on personal recognition as an alternative to the identification badge, but a workplace with more than a few employees will find the identification badge essential.

The control of visitors works differently. Visitor passes issued at an entry control point substitute for identification cards. Visitor passes are typically constructed of paper and may have a feature that causes self-destruction after 1 or 2 days. The pass is dated and issued for a set period, usually day; applied for at a reception or security desk adjacent to the entry point; and requires the visitor to present a form of photo identification such as a driver's license. A condition of issuance may be approval by an employee. In some situations, only certain employees are allowed to approve visitor access, and the day and time of visit must be prearranged. In medium- to high-security situations, the visitor is escorted while inside the facility.

In a safety-sensitive workplace, a visitor may have to undergo a briefing, view a film, sign a release, and put on protective apparel such as a hard hat, safety glasses, and steel-toed boots. A record of the visit is wise.

TYPES OF IDENTIFICATION CARDS

Control of access at a protected facility is very likely assisted by a card identification system designed to verify each entering person's authority to enter. As one can expect, the efficiency and effectiveness of the system is affected by the reliability of the card identification equipment, speed of operation, number of entry points, size of the workforce, operating hours, and above all else, human cooperation. A well-designed and skillfully managed identification system achieves the basic goal without impeding the work flow.

Many different types of identification cards are available. The type of card purchased by the company will correspond to system hardware. A few types carry just the owner's name, affiliation, and signature, whereas most incorporate a head-and-shoulders photograph laminated to the card, a tamper-detecting feature, and a post office box number for mailing found cards back to the issuing organization.

Nearly, all access cards are of the same general size and shape, and in overall appearance look somewhat like a credit card. The common types are Hollerith, magnetic stripe, barium ferrite, bar code, Wiegand, proximity, and smart card.

- Hollerith: This very early form of access card has small holes that can be read by a light source or contact brushes. Today's use of Hollerith cards is pretty much limited to hotel security. The guest slides the card into a slot above the door handle. The lock disengages when a reading of the card matches a guest's registration at the lobby desk. This very simple technology is not suitable for high-level security.
- Magnetic stripe: This type of card has a data-encoded stripe on one face. When the card is swiped through a reader, the stripe passes over a magnetic head not unlike that of a tape player. The code on the stripe is compared with access criteria that earlier were entered into the system. Access criteria reflect the cardholder's identity, the areas the cardholder is authorized to enter, and time frames for entry. Compared with other card types, the magnetic stripe costs less and can hold a large amount of data. However, the magnetic stripe can wear out or become damaged over time, and the vinyl plastic construction of the card can lead to chipping and breaking.
- Barium ferrite: This type of card is sometimes called a magnetic spot card or magnetic sandwich card. It is cut from three-layer plastic stock. The middle layer, or core, is barium ferrite that has been magnetized with a pattern of dots arranged in a readable pattern. The pattern is a code fixed by the magnetic polarity of the spots. The barium ferrite card is slightly more expensive than the magnetic stripe card. It is also subject to problems resulting from wear and tear and is vulnerable to deciphering.
- Bar code: This card bears on one side (usually the front) a series of lines forming a code readable by an optical scanner. The pattern of lines (i.e., the bar code) looks very much like the pattern of lines found on the outside of supermarket items. Because a bar code is easy to duplicate, it is not suitable for good security practice. This card, however, can be used for tracking inventory; for example, a late-shift security guard with a hand-held reader can determine the locations of desktop assets. A processor at the security control center conducts an analysis and prints out findings such as when an asset has been moved, the asset's current location, and assets that are missing.
- Wiegand: This card is also called an embedded-wire card. The technology is based on the Wiegand effect, a phenomenon observed when specially prepared ferromagnetic wires suddenly reverse themselves on exposure to an external magnetic field. Wires inside the

card are formed in a permanently tensioned helic twist. The order and spacing of the wires establish a unique code for each card. The magnetic reversals in the wires are converted into distinct, consistent electrical pulses that are read and processed. The card's thickness and composition of stock make it resistant to pocket damage. It is, however, susceptible to malfunction arising from wear after many passes through reader slots.

- Proximity: The proximity card has an embedded microcircuit that emits frequencies detectable by a reader. The reader reacts to the frequencies when the card is placed in close proximity (2 to 4 in.). Sturdy composition makes the card resistant to tampering and the interfering effects of weather and shock. Two other features of the card make it attractive. The emitted frequencies can be made sufficiently powerful for the reader to be concealed behind a thin wall or mounted inconspicuously (possibly for aesthetic reasons), and the card can work through clothing or a handbag.
- Smart card: Regarded as the card of the future, the smart card contains its own processor, making it capable of running its own internal programs. The very large amount of data that can be contained in a smart card allows it to serve purposes that go beyond access control. For example, the cardholder's medical history can be stored for quick retrieval in a medical emergency and cashless purchases recorded. Fig. 12.1 shows one use of access control cards. The downside to the smart card is cost. However, it offers several advantages: the card is durable and tamper resistant, counterfeiting and duplication are difficult, encryption presents an obstacle to compromising the code, the

FIGURE 12.1

Access control cards of many types can be used at many different types of readers. *iStockphotos.*

card can be programmed to expire on a certain date, and smart card technology is suitable for many applications.

- Radio Frequency Identification (RFID) card: The RFID card does not need to make contact with a reader. Inside the card is a tiny RFID tag that communicates with the reader from a distance. The card can give to the user speedy and convenient access. The technology is widespread, especially in the retail sector where it is used for keeping track of inventories.

TRAFFIC CONTROL

Control of vehicles can start and end at a property line distant from or in close proximity to the operating portion of the facility. If the property line is immediately adjacent to a crowded public roadway, the Chief Security Officer (CSO) may want traffic to be directed. Local police officers can be hired to perform traffic-directing duties or can be performed by specially trained security officers approved for the work by local law enforcement authority. This option has three advantages: safety is enhanced, vehicle flow is smoothed and moves fairly rapidly, and the drivers of entering vehicles are reminded that access control is taken seriously.

During the hours of high-traffic movement, it may be advisable to open more entry gates. If manning more gates is not practical, the alternative may be gate arms that lift when a proximity card is passed near a card reader. If the entry is to a parking lot or garage, the gate arms can be locked into the open position to allow faster movement.

Traffic control can be simple, yet problematic. Signage, marked lanes, and a visible security force should be sufficient to regulate vehicle movement, yet some individuals insist on driving and parking in areas where they are not permitted to be.

The growing number of vehicle bomb incidents calls for the use of traffic-slowing devices, such as jersey barriers, crash protectors, such as bollards, and placement of parking areas outside the blast zone.

MATERIALS CONTROL

Materials requiring control, such as shown in Fig. 12.2, include supplies and raw goods that enter a warehouse. Any section of a facility can be a criminal's target. The targets could be items worked on or produced such as manufactured goods, tools of work, and materials leaving the facility such as finished products, returned items, and scrap.

FIGURE 12.2
The receiving area of a warehouse is often the special target of thieves. *Burns International Security Services.*

Inspection, Entering, and Moving Internally

Truck-delivered mail and courier-delivered packages, containers hand carried by employees and visitors, and small shipments received outside a facility's supply channel can be made subject to routine inspection. Care must be made to inspect, not search. An inspection is an administrative control known to and agreed by persons subject to inspection. A search is a law enforcement action ordered by a court and performed by police officers.

Only specially trained individuals should perform inspections. Examples are security officers inspecting baggage at an airport and mailroom employees looking for the indicators of mail bombs. Metal detectors, X-ray viewing equipment, explosives detectors, bomb barrels and bomb-resistant rooms, and sniffer dogs facilitate the work.

The use of inspections is a policy matter decided at senior management level, with input from the CSO. Typically, a policy will prohibit introduction to the facility of explosives, firearms and ammunition, knives, poisons, drinking alcohol, stolen property, offensively pornographic items, illegal drugs, and drug-administering paraphernalia.

Movement control can also apply to e-mail messages and electronically transmitted information such as classified documents, business plans and strategy, and trade secrets. Inspection of this type, in addition to being an issue of policy and the personal sensitivities of employees, is often restricted to what the computer hardware and software permit.

Accounting for Property

A reasonable business necessity is prevention of loss and prevention of unauthorized use of organizational assets. The necessity can be satisfied with a system for controlling the movement of property from the facility through pedestrian portals such as property in the possession of employees and visitors who leave by the front door, and a system for tracking the migration of physical assets within the facility.

A property removal system can require the remover to obtain a removal pass signed by an authorizing supervisor. The pass is attached to or enclosed with the property to be removed. At the exit point, the pass is shown to a security officer. The pass can be taken by the officer and be held on file for reconciliation purposes.

An assets-tracking system keeps track of items such as desktop equipment and valuable tools. The items are tagged, labeled, imprinted, or encoded in some way. To illustrate, a bar-code sticker is affixed to an item. The sticker identifies the type of item, its location, and identity of the person responsible for its custody. During the midnight shift, a security officer moves throughout the facility passing an electronic wand across bar code stickers. A microprocessor or computer in the security control center reads each sticker and matches it against a database. If the match is not perfect, such as the item being in the wrong location, an exception is noted by the computer. At the end of the midnight shift a report is printed. All noted exceptions are highlighted. Copies of the printout are placed in the company's mail room for delivery to supervisors responsible for custody of the items. Items that were not tracked can be assumed missing or stolen.

Inspection of Materials Leaving

Some facilities, for public safety reasons, simply demand inspection of departing vehicles. Examples are nuclear energy plants, weapons storage buildings, and precious metal processing factories. Certain necessary prerequisites apply: ensuring that the inspection program conforms to the Constitution, laws, contracts, and agreements with bargaining units; ensuring that people affected by the inspection program are informed in advance; and ensuring that the security officers or others who perform the inspections have been trained.

ACCESS CONTROL BARRIERS

In a very basic sense, an access control system has a barrier of some type standing between the person desiring entry and the place to be entered.

According to San Luis (1994), when the place to be entered is an open area, warehouse or building, office area or conference room, the barrier can be physical in nature such as a door or gate, or the barrier can be a human such as a security officer permitting entry based on personal recognition or checking passes.

When the area to be accessed is other than a pedestrian or vehicle entry point and the portal small, the barrier may be a padlock on a container, the combination to a vault or safe, or a deterrent device such as a conspicuously placed capacitance sensor that will activate a siren if a small object is touched.

In short, there can be no access control system without a barrier. Figs. 12.3 and 12.4 depict a form of access control.

FIGURE 12.3
Access control is exercised at shipping and receiving docks. *Burns International Security Services.*

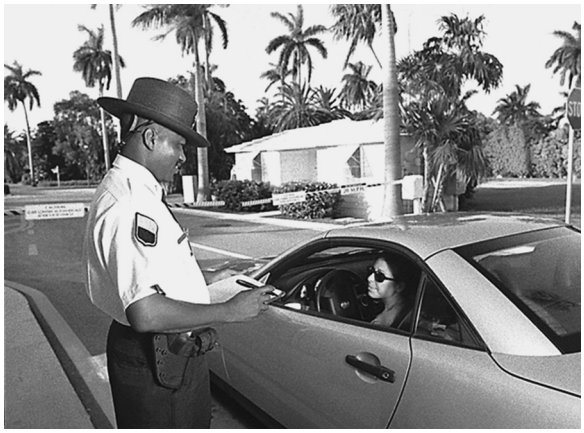


FIGURE 12.4
Access control at a vehicle entry point. *Burns International Security Services.*

Layered Protection

Access controls are often layered to decrease the chance that an intrusion will succeed. A layered system could, for example, start with a requirement that an employee present a card key to a reader at a perimeter gate, similar to the situation shown in Fig. 12.4. The employee drives to the main gate where a security officer recognizes the decal at the top center of the windshield and waves the employee through. The employee uses a different key card to enter the company's covered garage. The employee enters the company's office building by punching in an alphanumeric code on a reader next to the entrance door. The employee stops at a security desk and shows his or her company identification card to a security officer. The employee enters an elevator activated by insertion of a mechanical key or card key. The elevator stops and the employee steps into the floor's lobby. The employee is recognized by a secretary on the other side of a glass door. The secretary presses a button that releases the electronic lock on the door. The employee enters and walks to his or her office and opens it with a mechanical key. Inside the office, the employee manipulates a combination dial on a safe and removes a laptop PC. The employee takes the PC to his or her desk, sits down, and pushes the start button on the PC. When the screen lights up, the employee enters a log-on password and a network password. The employee has now reached the protected asset: very sensitive information residing on the hard drive of the PC. The employee had to move past 10 layers to gain access to the protected asset.

Layered protection and concentric protection are not quite the same. Layered protection is designed to carefully facilitate entry of authorized persons; concentric protection is designed to deny and detect entry by unauthorized persons. When used for detecting intrusion solely, each layer can be designed so that an intruder's movement toward the target becomes increasingly difficult.

Uniformity and Diversity

An electronic access control system is uniform because it conforms to rules and logic and treats transactions the same way every time. For example, a certain door always opens when a valid card key is presented and never opens when presented with an invalid card key.

However, diversity is a norm. The system is driven by software and internal devices that will be diverse in purpose and operating principle. Doors, locks, lights, and sensors perform unique functions, but each will be different from the others because each has its own purpose and operating principle.

Access control systems are diverse from place to place. The CSO at Facility A may decide that entry control is best done with biometric technology, whereas the CSO at Facility B may decide that entry control can be done with card key technology. At Facility A, the biometric choice may be fingerprints as opposed to retinal pattern, and at Facility B the card key choice may be proximity as opposed to magnetic stripe. Security needs and CSO preferences vary widely, making diversity a common theme.

Even within a single technology, there are variations in components, logic, options, and price. All access control systems, regardless of technologies, have one thing in common: they are dependent on humans. A fatal mistake of the CSO can be the neglection of the human side while overemphasizing the technology side. This sometimes happens when the CSO sees an opportunity to reduce costs by replacing security manpower with electronic devices.

BIOMETRICS

Garcia (2004) states that an individual's identification can be verified on the basis of a unique personal characteristic. Much like the card key, the person desiring to pass through a portal is required to present a form of identification, but in this case, identification is biometric in nature. Presently, the biometric identification systems are principally finger and hand geometry, fingerprints alone, retinal pattern, voice, face, and handwriting.

- Finger and hand geometry: This method examines the shape of the fingers and hands, length of fingers, distances between fingers, and thickness of the hand. The usual procedure requires the individual to first present a card key for scanning or entering a code on a keypad or cipher lock. After the card or code has been verified, the individual places his or her hand on a reflective platen. Placement can be palm-down, palm-up, and palm facing one side (to measure thickness). One, all, or a combination of all placements can be used. A camera integrated with the platen takes photos that are compared against photos in a database.
- Fingerprints: The most popular form of biometric identification is fingerprint evaluation. Fig. 12.5 is an example of a fingerprint identification device. The individual places a finger, usually the index finger of a preselected hand, on a platen that is sized to accommodate a single finger. The act of the individual is similar to pressing a button and holding it motionless for a predetermined number of seconds. The platen is integrated with a prism and camera. The photo taken of the print is compared against photos in a database. A couple of problems

FIGURE 12.5
The fingerprint identification device is small and easy to use. *iStockphotos.*

are associated with this device: dryness of the skin that was not present when the database photo was taken, oil and sweat, and a recent laceration or disfigurement of the finger.

- Retinal pattern: An individual's retinal pattern consists of blood vessels that are unique in the same way fingerprints are unique. The center of the eye is scanned with a very low-intensity light that produces light-emitting diodes (LEDs). With the enterer's eye socket pressed against the device, a target is visible. The individual focuses on a target while the scan is made. The scan is compared with a scan in the access control database.
- Voice: Verification of identity is made through the measurement of wave form, pitch, amplitude and resonant frequencies of the voice. This form of identification offers low security, but it is easy to use and widely accepted by persons seeking entry through the portal.
- Face: This system is essentially a camera that photographs the face of the individual and compares it against a photo on file. Comparison between the portal photo and the database photo is keyed to distinguishing characteristics of the face and head. The system is low-tech and fraught with problems: distance between head and portal camera, head rotation and angle, cosmetics, hair dye, new hair style, and the presence or absence of eye glasses.
- Handwriting: In this system, the individual uses a certain pen to write his or her signature on a certain tablet. The distinguishing characteristics are displacement, velocity, and shape. Statistical evaluation of the characteristics judges whether the portal signature is reasonably unique and similar to the signature on file.

CLOSED CIRCUIT TELEVISION

A security officer sitting in front of a monitor can be at many places simultaneously. Decisions can be made quickly to allow authorized persons to enter controlled areas far from the nearest security officer. According to Kruegle, access control is only one of many tasks that can be harnessed to closed circuit television (CCTV). These include deterrence, detection, validation, apprehension, and investigation.

Deterrence occurs when conspicuously mounted cameras persuade a criminal opportunist to try elsewhere. Detection occurs when a security officer sees on a CCTV monitor an intrusion in progress. Validation occurs when CCTV confirms an event reported by an intrusion detection sensor. Apprehension occurs when security officers take into custody an intruder spotted on CCTV. The investigation objective is met when a CCTV tape identifies the person involved in the act of interest.

Business owners acquire CCTV systems for any or all of the capabilities just mentioned. A hotel proprietor, for example, can use CCTV to evaluate persons walking through the hotel lobby late at night, and look for suspicious persons in hallways, auto thieves in the hotel parking garage, and persons attempting to force open ground floor windows or side entrances. Fig. 12.6 shows CCTV monitors in a security control center at a high-security facility, and a console operator in a security control center. CCTV cameras mounted at an area of concern transmit images to the CCTV monitors at the security control center. When suspicious activity appears on a CCTV monitor, the console operator dispatches an officer to investigate. In addition, a CCTV system can be a valuable tool for identifying the person(s) involved and serve as evidence at a trial.

FIGURE 12.6

A console operator in a security control center is a main player in an access control system. *iStockphotos.*

CCTV has quality control and training applications. A security supervisor can use CCTV to evaluate visitor processing and replay tapes that teach officers how to process visitors more effectively. In addition, CCTV can be used to watch the activities of employees performing sensitive duties such as counting money, and in less serious activities, watching cashiers.

Comfort Level

Even where CCTV is not justified by earlier incidents, business owners favor the method because it gives them a level of comfort. An owner of a public building, such as an office tower, wants assurance that people entering through unlocked doors at street level are under observation. Protection of the public, employees, and property is both a duty and a business necessity.

Pros and Cons

On the positive side of the CCTV ledger are the following advantages:

- Many locations can be watched simultaneously from one central location.
- The approach of intruders and attempts to intrude can be detected early.
- Costs can be lowered by replacing expensive manpower with a less expensive CCTV system.
- Human performance errors can be detected such as when a CCTV system is monitoring normal work activities such as guards on patrol.
- Deterrence.
- Create a visual record of an incident to aid a postincident investigation.

On the negative side, a CCTV system:

- Can be expensive to purchase.
- Can be complex and difficult to operate.
- Can require considerable preinstallation time.
- Can suffer from bugs and glitches.
- Requires periodic maintenance and calibration throughout the life of the system.
- Can become dysfunctional in extreme conditions such as tropical heat, arctic cold, wind and sand storms, flooding, earth tremors, and direct sunlight on the lens.

System Features

A simple system can be a video camera cabled to a monitor. A complex system can have many bells and whistles: multiple digital cameras that pan and tilt, zoom in and out, display many views simultaneously, send digitized images to a computer; and compress images to facilitate long-term storage. Systems that lie above the simple and below the complex are usually adequate for most security purposes.

Using white and infrared light, cameras can capture clear, high-resolution images under poor lighting conditions. Cameras can operate remotely, react to movement in the field of view, track objects, and scan randomly. They are typically mounted in weather-resistant housings and send signals via fiber-optic cable.

Monitoring and recording equipment vary in the manner images are captured, displayed, and stored. Real-time and time-lapse recorders are very popular. Some recorders automatically display and record images on receipt of a signal from an intrusion detection sensor. To save space on tape or a hard drive, the image can be broken up so short time intervals are not recorded and therefore reduce the length of the tape or size of the digital memory. Hundreds of hours of images can be stored on a single medium.

An uninterrupted power supply is essential. In addition to providing backup power, it overcomes interference caused by electrical spikes and surges, and its instant restoration of power neutralizes an intruder's attempt to avoid detection by shutting down a sensor's electric circuit.

Also essential in choosing an electronic access control system is quality, both in equipment and installation. A bargain can turn out to be false economy when equipment malfunctions require frequent repair, recalibration, or retrofitting.

Managing a Purchase

Before purchasing a CCTV system, the CSO would do well to be absolutely clear as to what is needed and what is not. A state-of-the-art system can be sufficiently enthralling to draw the CSO's focus from consideration of the protected facility's requirements. Requirements, of course, are identified by characterizing the nature of the threat and determining what is needed to counter the threat. These steps are followed by cost/benefit analysis.

A common approach is to compare the costs of acquisition and operation against dollars saved by reducing the need for security manpower and preventing losses that would result absent the system.

Operating the System

Before a system can be operated, the operators need to be trained. The purchase agreement should include provision of training by the manufacturer or supplier. The job description of a system operator, which is prepared by the CSO, can serve as a training reference. A follow-on step is to prepare written procedures supplemented with literature of the manufacturer.

System Performance

Ensuring system performance is a CSO responsibility. Carrying out the responsibility requires attention to detail and exactitude, with the focus on performance of equipment and operators. Performance errors tend to be moderate to great in the period immediately following system start-up, with few errors occurring over the remaining life of the system. As each error is detected, corrections are made to equipment, tasks of the operators, written procedures, and training content. An important yet often unconsidered correction is to make the system operator's job challenging and as interesting as possible.

Maintenance

Keeping the system up and running at an optimum level calls for technical support delivered quickly. The relatively complex and rapidly evolving nature of CCTV requires a level of technical knowledge not often found in a security group. Knowledge includes an understanding of the facility's security needs and the CSO's concept of protection.

As is the case with most major purchases, the CSO evaluates offers. Guidance that can help the CSO make a decision appears in Fig. 12.7. Generally, the manufacturers of top-shelf systems provide high-quality technical advice and service. The leading manufacturers of CCTV systems advertise in security products catalogs.

CCTV System Guidance

Pre-Acquisition

Conduct a risk analysis to determine the facility's security needs. Examine the site during both day and night conditions, take photos and make video tapes, prepare notes and a layout sketch, and evaluate environmental factors that may impact the operation of a CCTV system. Also evaluate possible interference of nearby facilities such as roadways, airports, and industrial plants.

Identify CCTV applications that correspond to the identified security needs. Develop a scheme for tying the CCTV applications into a single system.

Determine how the CCTV system will interface with other security systems such as intrusion detection and access control.

Draft a technical design and conduct a cost-benefit analysis.

Acquisition

Select a supplier (on a bid basis, if appropriate).

Require the supplier to test the system and/or system components prior to their delivery to the site.

Prepare a schedule for receiving, installing, testing, and accepting the system.

Ensure installation under supervision of the supplier's in-house expert.

Ensure calibration by the supplier. Calibration factors include lens angles, resolution, fields of view, panning, programming, and interfaces with sensors and adjunctive systems.

Develop written procedures to guide every person involved in system operations.

Train system operators.

Test the system.

Correct problems before accepting the system.

Post-Acquisition

Conduct periodic maintenance, calibration, and troubleshooting.

Conduct refresher training and training of new system operators.

Evaluate the installed and functioning system vis-à-vis what had been planned and expected.

Look for cost-effective revisions and add-ons.

Update written procedures.

FIGURE 12.7
Acquiring a CCTV system follows a step-by-step process.

CRITICAL THINKING EXERCISE

Harriett Bowers, CSO of JBR Warehousing and Distribution, is concerned with the growing number of equipment breakdowns and general effectiveness of an obsolete CCTV system used to observe night-time activities at a complex of warehouses located on the fringe of the company's property. These particular warehouses are used to receive, temporarily store, and ship high-value items, such as television sets and stereo equipment. Bowers had previously recommended to management to store the high-value items away from the perimeter fence line but management did not agree because the size and interior layout of the warehouses were ideal for stacking and

moving crates. At the time of her recommendation, the CCTV system worked perfectly, security lighting was more than adequate, and the night-time security patrols, which rattled doors and patrolled in a random fashion, were effective in reducing the number of break-ins and attempted break-ins by thieves who scaled or cut through the perimeter fence. Much of what the patrol deterred in the way of attempted break-ins was based on images that appeared on CCTV monitors at the security control center.

When Bowers' recommendation to replace the aging CCTV system came before the executive team, she received permission to replace the CCTV system with a leading-edge system but the night-time patrol, which consisted of two security offers, would have to go. Management's rationale was that a superior CCTV system would easily provide intrusion detection without the services of the night-time patrol. Bowers objected but the CFO was adamant in expressing the executive team's decision.

The new CCTV system was installed and worked perfectly. She terminated the night-time patrol which required nine officers. Almost immediately the number of break-ins increased, causing loss greater than before installation of the new CCTV system. The cost of the increased losses pretty much matched the savings acquired by the reduction of labor costs.

What is the basic problem? What security concept was abandoned? Make recommendations that will justify Bowers returning to the executive team. Should she approach the team with a concept that costs a little more than before the new CCTV was installed but stabilizes losses at an acceptable level? What would approach might that be? Instead of dollars, use estimated percentages you believe are adequate.

INTRUSION DETECTION

An extremely critical function in controlling access is detection of intruders. In a very real sense, intrusion detection is at the core of the access control rationale. Without it, the integrity of a facility is in question.

An intruder detection system (IDS), as discussed in the chapter on physical security, is an arrangement of electronic devices for detecting the entry or attempted entry of an intruder and sending an alarm. An IDS can involve substitution of electronic surveillance for human surveillance.

An effective, long-life IDS is professionally designed, planned, installed, and serviced regularly. Without these minimum standards, an IDS may be vulnerable to circumvention, malfunctioning, and false alarms.

IDS Components

The basic components of an intrusion detection system are as follows:

- Sensors and their locations.
- Circuitry or communications infrastructure that connect sensors to a control unit and the control unit to an alarm display panel.

- A control unit that monitors the sensors, receives signals from them, and transmits an alarm signal.
- An alarm display panel with visual and/or sound enunciators that alert monitoring personnel to an intrusion.

Sensor Selection

Sensor selection is determined by the intrusion threat, the operating environment (e.g., indoors, outdoors, subsea, hostile climate), and power source constraints. Types of sensors to be considered are as follows:

- Volumetric and spatial sensors that detect movement within a confined area, such as a room, and are referred to in terms of their scientific principles. These are, for example, ultrasonic (sound waves), microwave (interruption of a linear signal), and passive infrared (detection of body heat).
- Beam sensors that operate on infrared and microwave principles.
- Contact sensors that activate when an electric circuit is broken by the separation of magnets such as those commonly attached to doors and windows.
- Vibration sensors attached to rigid structures. These are, for example, the inertia switch that reacts to physical vibration, the geophone that reacts to sound vibration, and the crystal vibration switch that reacts when a piezoelectric crystal is compressed by physical vibration.
- Closed-circuit sensors that activate when an electrical circuit is broken; for example, by the cutting of a charged wire inside a wall or on the mesh of a window screen.
- Sensors that activate when weight is applied to a surface such as a pressurized mat concealed under a rug.
- Video motion detectors that activate when movement is picked up by the lens of a video camera.

Minimum Expectations

The CSO should expect an intrusion detection system to

- Operate despite potentially interfering environmental phenomena such as extreme weather and climate, tremors, topographical obstructions, and loud noises.
- Resist and detect tampering.
- Be fail safe (i.e., continue to operate when the primary power source fails).
- Report tampering and equipment malfunctions.
- Be linked to a monitoring station.

- Have a designated response capability.
- Be designed and planned by an IDS-certified engineer.
- Be monitored by a security officer.

THREAT INDIVIDUALS

The nature of a threat confronting a protected facility can be viewed from two perspectives. The first is tradition, or what has happened in the past. Preventive action steps are shaped by what has been learned from experience. What is the chance the threat incident will happen again? When, where, and how?

The second perspective looks at the type of threat. Is it nature-related or human-related? In the context of access control, the nature-related threat does not apply. However, it can be useful to compare the two. Logic says that there would not be a nature-related threat to even think about unless it had occurred in the past. Imagine that a hurricane occurred in the past. Good judgment predicts that a hurricane will occur again, will most likely occur during a certain part of the year, and will come from a certain direction. At a certain velocity, it will damage property to a certain extent. In short, a nature-related threat has a baseline that permits prediction and preparation. By comparison, a human-related threat has a partial, murky baseline at best.

Experience and judgment is sufficient to conclude that threats posed by humans exist. Possible targets can be identified, the method of criminal action can be surmised, and the potential magnitude of loss can be computed. Shaky judgments can be made about the capabilities and resolve of the adversaries. The best that can be done is to label adversaries according to who they are, what they have done in the past, what they want, how they will act, and most importantly, learn if the company is on the adversaries' agenda.

Right off the bat it can be said that human-related threats exist within and outside the organization. For example, a disaffected employee is an internal threat, a criminal opportunist is an external threat, and a terrorist is both.

The greatest concern, although not always the greatest exposure, is with internal threats. There is a tendency not to consider the possibility that someone within the tent has evil intentions. The natural thinking process gives trust to those who are close and distrust those who are not.

The Insider

The inside threat is typically manifested in theft, disruption of operations, destruction and damage of property, and harm to people. An accountant

embezzles, a wise-guy hacker erases important files, a disgruntled employee tosses a monkey wrench into machinery, and a terrorist sympathizer sets off a bomb in the lobby.

A combination of physical and procedural safeguards can be valuable in thwarting the inside threat. Access controls, at least those that regulate movement of people entering the facility, will not impede the insider. Barriers and sensors at critical points around critical assets can be effective. The trusted insider, however, can be expected to have access to lock combinations and keys, have a good working knowledge of security equipment and procedures, and enjoy freedom from suspicion.

The Opportunist

This individual, typically an outsider, looks for chinks in the protective shield. He or she knows or thinks that behind the shield are valuables worth taking or prey worth sexually assaulting. If it appears that the shield cannot be penetrated, the opportunist moves on to more promising territory. If it appears that the shield is vulnerable, the opportunist follows a path of least resistance. If detected or challenged, the opportunist flees and does not return. If penetration appears possible, the opportunist selects a primary and secondary route of escape and begins looking for exposed valuables and/or victims. Fortunately, the opportunist is just that—a person skilled in looking for an opportunity but less skilled in acting on it.

The best tools for reducing crimes of opportunity are deterrents such as fences, lights, signs on the perimeter, and guards at vehicle gates and pedestrian doors. A less recognized but important deterrent is maintenance. When the facility is shabby, the opportunist tends to connect poor maintenance with uncaring occupants. The thought process is, "Here is a place where I can get inside, move about freely, and get away without getting caught."

Of all deterrents, the human presence is most effective. It is best shown by conspicuous guards who are alert, well-groomed, and trained to challenge strangers.

The Professional

A third type of external threat is the skilled professional. He or she has a particular target in mind, possesses technical knowledge of security devices and how to defeat them, has security-defeating tools and other resources, and operates from a plan. The professional is likely to be assisted by an accomplice who works inside the protected facility.

The professional is often patient and willing to abort when he or she confronts an unanticipated risk. When trickery does not succeed in getting past a security guard, the professional makes an attempt to use stealth. If confronted, the professional has a believable cover story and false identification. The professional is thwarted by physical safeguards, sensors in particular, well-trained security officers, and employees suspicious of unrecognized faces.

The Ideologue

The ideologue frequently operates alone but is almost always supported morally or materially by a group rooted in a cause: religion, nationalism, human rights, animal rights, environmental protection, and other causes. The ideologue cleaves to the group's beliefs and agenda, accepts the group's set of targets, and follows its standard attack scenario.

As a general rule, material greed is not a motivator for the ideologue. However, the ideological group does have a history of resorting to robbery, extortion by threat, and kidnaping to acquire operating revenue for the group. Individual and group tactics range from terrorist acts, such as bombings and assassination, to purely symbolic acts such as splashing blood on fur coats, or burning a flag in a public place. The ideologue may or may not be skilled, is likely to be intelligent, very likely to be strongly committed and dedicated, willing to take chances, and willing to suffer the consequences of being caught.

Because ideologues make no bones about their enemies and lodge their protests every way they can, the CSO to some degree is able to anticipate the acts and be prepared to deal with them. The appropriate countermeasures are similar to those that apply to the professional.

The Avenger

This type of individual can be inside or outside the protected facility. Of the two, the inside avenger represents the greater risk. However, when the outside avenger had been an insider at one time the risk is highest. This individual has knowledge of how to get inside, and if successful in doing so, the chances are great that an adverse act will follow.

The number of incidents involving violence by an employee or former employee against coworkers and supervisors has increased dramatically in recent years. The number of injuries and deaths at work has also increased. When robbery-related shootings are factored in, workplace violence is the leading cause of on-the-job deaths.

Workplace homicides are often the result of an unstable employee being laid off or terminated. The worker returns with a gun and kills the supervisor and others who get in the way. When layoffs and terminations rise, violence also rises.

An employee who releases frustration through acts of violence is likely to have a history of violence and is likely to demonstrate frustration through temper tantrums, threat making, and bursts of anger. It is too late at this time to apply the best countermeasure: preemployment screening. It is not too late, however, to teach supervisors how to spot the indicators of frustration and how to intervene.

Terminated employees have a right to be decently treated during the termination process. At the same time, however, the organization has a right to take protective steps. One of these is to quickly collect keys, company items and materials, data files, and if the employee owes money to the company, draft an agreement for repayment. Also important are steps to immediately remove computer access and reentry privileges. More discussion on these issues can be found in Chapter 20, Workplace Violence.

The Terrorist

By definition, terrorists are persons who use force or violence against others to intimidate or coerce, often for religious or political reasons. In the context of access control, terrorists can be seen to possess some of the characteristics of opportunists, professionals, ideologues, and avengers. But the resemblances are obscured by the magnitude of human casualties and destruction inflicted by terrorists. By and large, terrorists have demonstrated the know-how, capability, and resolve to carry out their acts. For these reasons, they are at the top of the intruder list and are the first priority for protection.

A terrorist attack through intrusion is likely to be made by numerous terrorists acting simultaneously and employing a combination of trickery, stealth, and direct assault. The resistance capability can be overwhelmed, even at high-security facilities.

A terrorist acting alone can be as destructive as a group of terrorists acting in unison. We have seen that the driver of a van carrying explosives can destroy an entire embassy and kill nearly all people in it, whereas a band of terrorists assaulting an embassy can succeed in destroying little in the way of structure and killing relatively small numbers of people. The epitome of a terrorist acting alone was the Timothy McVeigh bombing.

The capacity of a security system to neutralize or resist the single terrorist or band of terrorists can be enhanced when the CSO is plugged into an intelligence-sharing group. One of the oldest is the State Department's Overseas Advisory Council. CSOs send information to and draw from a body of processed data received from US embassies and consulates worldwide. CSOs of major corporations in a single industry have always shared information concerning common adversaries. In the petroleum industry, for example, CSOs of Exxon, Shell, and British Petroleum meet regularly to swap information about criminal and terrorist activities occurring in their separate domains. Similar groups are forming in sectors of the critical national infrastructure. The Environmental Protection Agency serves as a repository and clearinghouse for security-related information pertaining to water and waste water plants. The Department of Transportation does the same for the aviation, rail, trucking, city transit, maritime, and pipeline industries.

CONCLUSIONS

The security domain operates using numerous practices, such as concentric and layered protection, redundancy, crime prevention through environmental design, and psychological deterrence. All concepts share a common purpose: keep the adversary away from the target. The nature of the target is somewhat beside the point. It can be a person, such as a celebrity; an object, such as a nuclear bomb; information, such as a trade secret; a structure, such as the White House; a city, such as New York City; or Wall Street. Although terrorist attack techniques tend to vary, they have one thing in common: the need for access to the target.

REVIEW QUESTIONS

1. Why do businesses employ access control systems?
2. List three types of identification cards.
3. Describe the differences between a magnetic stripe card key and a proximity card key.
4. Which type of identification method would be best for hotel room access? Access to a business office? To a nuclear facility?
5. Give an example of layered protection.
6. What is biometrics?
7. Name at least two problems associated with the fingerprint method of biometric identification.

8. Name at least two advantages and at least two disadvantages associated with the use of a closed circuit television (CCTV) in an intrusion detection system (IDS).
9. Name the basic components of an intrusion detection system (IDS).

References

Garcia, M.L., 2004. Entry control. In: Fennelly, L.J. (Ed.), Effective Physical Security, third ed. Butterworth Heinemann, Boston, MA.

San Luis, E., Tyska, L.A., Fennelly, L.J., 1994. Office and Office Building Security. second ed. Butterworth Heinemann, Boston, MA.

Further Reading

Kruegle, H.A., 2007. CCTV: the many roles of CCTV in Security. The Encyclopedia of Security Management. Butterworth-Heinemann, Boston, MA, pp. 276–277.

CHAPTER 13

Managing Investigations

What You Will Learn

- The case management functions of a Chief Security Officer (CSO).
- The difference between constructive and reconstructive investigations.
- The definition of bribery.
- The purposes of a survey and how they relate to standards.
- Three actions that management can take to curb employee theft.
- The dynamics of an undercover operation.
- Polygraph theory.
- The difference between industrial espionage and electronic spying.
- The purpose and mechanics of a deposition.
- Outside sources available to the corporate investigator.

INTRODUCTION

The investigative function is part and parcel of the organization's efforts to protect its property. The Chief Security Officer (CSO), among other duties, manages investigations. The CSO will have one or a few investigators on staff or will have a formal agreement with an outside investigative agency. The main functions of investigators are to conduct formal investigations when the organization is a party of interest; determine where loss exposures exist; and devise controls for eliminating them. Many of the loss exposure facts are acquired outside of formal investigations. An analogous expression is "look under the rocks." In this sense, investigators test the efficacy of loss prevention controls and report their findings to the CSO, and the CSO modifies the controls.

The relationship between a formal investigation and a loss prevention inquiry is this: when a loss prevention control breaks down and a loss occurs, a formal investigation is opened. Three objectives come into play at this point. First, find out what caused the loss; second, find out who profited by the loss; and third, replace or retrofit the control to prevent reoccurrence.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00013-X

CASE MANAGEMENT

Investigation cases are managed by the CSO and the task involves several responsibilities.

Infrastructure

The CSO must create an underlying foundation or basic framework for supporting the investigation function. This is more than just acquiring office space, furniture, and supplies. It means:

- Defining the mission of the investigations department.
- Writing a policy, rules, and procedures that set parameters and provide performance guidance.
- Establishing a "chain of command" within the investigations department.
- Granting authority and delegating responsibilities.
- Acquiring physical resources such as vehicles, cameras, video recorders, weapons (if appropriate to the department's mission) and confidential funds for meeting "off-the-book" expenses such as payments to informers. When the company's business requires protection of sensitive information, resources might include antieavesdropping equipment or specialists on retainer to provide antieavesdropping services.
- Acquiring human resources, specifically investigators with skills that align with the department's mission.
- Providing opportunities for investigators to improve their skills and acquire new skills.
- Linking the department with other company departments such as the auditing department for identifying fraud and the legal department for obtaining legal guidance.
- Linking the department with external organizations such as law enforcement departments and prosecuting agencies.

Internal Operations

The CSO holds responsibility for establishing certain functions and ensuring they are performed effectively, legally, and within the department's budget.

Assigning Cases

The CSO might assign cases on a rotation basis, on the basis of expertise, on the discovery of an offense by a particular investigator, or on who is available at the time the investigation is first initiated.

Monitoring Investigation Activities

Daily progress or activity reports are filed to keep the CSO informed of activities and progress. Generally, these reports are for internal use.

Writing Reports

The report writing function might require submission of a formal report immediately after an investigation is opened; a progress report prepared according to a schedule or to important developments; a final report that includes facts, describes evidence and its relevance, identifies persons involved, makes conclusions, and recommends corrective actions; and a supplemental report that reports postcase facts such as the firing of the offending employee, receipt of restitution, and court adjudication. Reports of investigation are distributed on a need-to-know basis. The recipients are generally the persons responsible for taking action such as the manager of a department employing the offender or affected by the violation, in-house legal counsel to advise on the sufficiency of evidence, and a public prosecutor to determine if court action is to proceed.

Coding Cases

The CSO should establish a method for assigning a numeric or alphanumeric code to each case. The coding system would allow systematic filing of case reports and quick retrieval of them when needed.

Tracking Costs

The cost of investigations, totally and individually, should be recorded. When an investigation requires expenditures that go beyond what has already been allocated in the security department's overall budget, the CSO will need to seek approval of the expenditures. It is usual for a budget to have a category for extraordinary expenditures; it is also usual for such expenditures to receive approval in advance without dictating a dollar amount.

PRIVATE INVESTIGATION

A corporate security department may have one or a few investigators on staff or no investigators at all. The gap is filled with private investigators.

Nearly every state requires persons performing investigative functions to hold a private investigator license. Licenses are issued by a state regulatory board.

The definition of "investigative functions" can vary from state to state, and the requirements to become licensed vary from state to state. The procedures

incidental to license application usually include presenting evidence of having met certain educational requirements, evidence of having completed entry-level training, an application, and fingerprint cards for background checking.

Generally, the requirements of licensure include being above a certain age, possessing a high school or GRE diploma, and being a citizen or a person in the country legally. In some states, the applicant must not have been convicted of a felony or acts of a violent nature. Persons with mental health problems can be excluded. Many states require entry-level persons to complete a training course of a certain length that contains topics designated by a state regulatory board.

A few states will not allow a license applicant to perform investigative duties until a background check has been completed and passed; the usual procedure in most states is to allow the individual to work as a private investigator (under the supervision of a licensed investigator employed by a licensed agency) until the report of background investigation is received.

The private investigation field has many niches and specialties, for example, cases involving child abuse, divorce, employee theft, criminal defense investigation, workers' compensation fraud, insurance fraud, bank fraud, forensic auditing, eavesdropping detection, recovery of computer data, undercover operations, surveillance, loss prevention, executive protection, preemployment screening, assets tracking, skip tracing, missing persons, the service of warrants, and background investigation.

INVESTIGATION TYPES

Constructive and Reconstructive Investigations

Sennewald and Tsukayama say there are two categories of investigation: constructive and reconstructive. Constructive investigations are covert in nature. The investigation is in process while the suspected activity is taking place or is anticipated. An example might be an investigation into a complaint that a member of middle management solicits sexual favors from female subordinates in exchange for a favor such as a promotion or increase in pay. The purpose of the constructive investigation is to determine if objectionable activity is taking place.

Reconstructive investigations are necessary when an event has taken place and the investigator must recreate what happened after the fact. This type of investigation is usually carried out in the open.

Preventive or Preemptive Investigations

A prime example in this category is the prevention of espionage and eavesdropping. According to Muuss and Rabern (2006), economic or industrial espionage is the illegal practice of one company attempting to learn its competitors' secrets. The operative term is "attempting." The objective of a preventive investigation is to defeat the attempt.

Industrial espionage is typically carried out through a variety of tactics, some illegal and all unethical. In the purely illegal type are larceny, burglary, bribery, extortion, and blackmail. Unethical forms of espionage include employing moles, searching trash, sympathizing with disgruntled employees, and tricking researchers to reveal sensitive information in speeches or scientific papers or during a false job interview.

Eavesdropping is espionage committed with the use of concealed devices such as telephone bugs, hidden microphones, and other electronic instruments that capture conversations.

Murray makes the point that electronic spying is a serious economic and privacy concern in corporations and government agencies. Best practices suggest antieavesdropping inspections at a frequency of two to six times per year.

Due Diligence Investigations

The term due diligence refers to the care a reasonable party takes before entering into an agreement with another party. The inquiry serves to confirm all material facts regarding the agreement under consideration. In a big picture context, due diligence is a process for examining the financial underpinnings of a corporation in a pending investment, merger, or acquisition, with the goal of understanding risks associated with the deal.

For example, in a sell or purchase deal, both parties will want to check out the other party's bona fides. The seller wants assurance that the buyer has the financial ability to meet the sales price, and the buyer wants assurance that the seller's property is worth the price. Due diligence is essentially a way of preventing unnecessary harm to either party.

Issues examined in due diligence are complex. They can involve corporate capitalization, cash flow, loans outstanding, accounts receivable and payable, inventory on hand, ownership of intellectual property, material agreements, public filings, and so on. Of particular interest in due diligence investigations are answers to a few simple questions:

- Have any of the corporate officers been indicted or convicted of crime?
- Does the company have a litigation history?
- Is there a lawsuit pending or on the horizon?

- Is the company claiming assets that do not exist?
- Does the company have a hidden agenda?

The party undergoing the investigation is asked to fill out forms, provide copies of relevant documents, and give consent to being investigated. In due diligence, many documents are requested, for example:

- A management organization chart and biographical information of corporate officers.
- Copies of pleadings or correspondence for pending or prior lawsuits.
- Summaries of disputes with suppliers, competitors, or customers.
- Correspondence regarding threatened or pending litigation, assessment, or claims.
- Decrees, orders, or judgments of courts or governmental agencies.
- Reports made to regulatory groups such as occupational safety and health administration (OSHA) and environmental protection agency (EPA).
- Summaries of labor disputes.
- Correspondence, memoranda, or notes concerning pending or threatened labor stoppage.
- Consulting agreements, loan agreements, and documents relating to outside transactions involving corporate officers, directors, key employees, and related parties.
- Compensation schedules of corporate officers, directors, and key employees showing salary, bonuses, and noncash compensation (e.g., use of cars and property).
- Summaries of management incentive or bonus plans.
- Confidentiality agreements.

The investigative techniques used in a due diligence inquiry consist mainly of checking records, verifying references, and interviewing knowledgeable persons.

Surveys

A survey is a type of investigation that seeks to prevent loss by identifying weaknesses in a loss prevention scheme. Generally, surveys are conducted of the physical features of facilities as opposed to internal. For a survey to be effective, the business must have standards against which the survey can be compared. Broder (2000) defines a standard as a level of acceptability against which things measured can be prepared. For example, very little meaning can be derived from a survey observation that 12 security lights surround the facility when there is no standard that says 12 security lights are required. The investigator conducting the survey may conclude that 15

are required, and all things being equal, a standard to that effect would be created.

It is the CSO, with input from investigators, who creates the standards. Standards can apply to the following:

- Fencing and its characteristics such as height, topping, and depth into the ground, and the gauge, size of opening, and distance between supporting poles on a chain link fence.
- Security lights by type (such as halogen, incandescent, fluorescent, metal halide, high- and low-pressure sodium, and infrared), height, cone of illumination, foot-candle, portability, reliability, back-up, glare, and self-starting.
- Doors, windows, walls, ceilings, roofs, wiring systems, and maintenance.
- Power sources.
- Water and sewage.
- Intrusion detection system including sensors and CCTV.
- Access control system, both human-operated and electronic.
- Locking devices and key control.
- Cabinets, safes, and vaults.

A primary focal point of a survey is the guard force. The investigator will examine the number of security officers, training received, turnover, supervision, and adherence to specifications of the contract.

Administrative Inquiries

An administrative inquiry is a fact-finding investigation. The inquiry may be to obtain facts important to the business, for example, determining the number of employee identification cards issued by type, the number of access control readers and where they are located, the number and frequency of particular violations, the names and addresses of certain persons, and other facts. This type of inquiry is generally not complicated, ordered from above, and assigned to a particular investigator. The report is typically in a memo format written and delivered to the requester by the CSO.

Internal Theft Investigations

One of the most frequently investigated incidents in the business environment is employee theft. Hemphill (1976) reports that ending, or at least controlling, theft by employees begins with management. Three imperatives apply:

- Decide that internal theft is unacceptable.
- Do something about it.
- Involve employees in bringing it to an end.

It is generally accepted by security professionals that a workforce is three groups in one, as far as honesty is concerned. The first group, about 25%, is consistently honest no matter what. Another 25% are outright thieves consciously looking for ways to steal. The honesty of the remaining 50% is up to management. This half of the workforce can fall on either side, depending on opportunity. If opportunity exists, the temptation exists. Given sufficient temptation and the example of successful thieving by coworkers, many employees in the 50% category will steal also. The types and causes of employee theft are listed in Fig. 13.1.

On the surface, it might appear that a business failed because it could not compete in a highly competitive and evolving marketplace. But below the surface, where the investigative focus should be, there is likely to be evidence that the company's demise resulted from employee dishonesty in one form or another.

For it to be said accurately that employee dishonesty is deviant behavior, there must first be rules and controls to deviate from. San Luis et al. (1994) say the lack of clearly understood rules is a management failure that can lead to a downward spiral of ever-increasing dishonesty, the corollaries of which are loss of productivity and customer dissatisfaction.

Causes of Employee Theft

Some employers choose to do nothing in the face of internal theft. They don't want to upset their workers

Some employers are simply unaware of theft or make no effort to be aware

Some employers keep an eye on internal theft and take preventive action only after losses reach a predefined level

Some employers choose to keep dishonest employees on the payroll in order to give them an income that will permit restitution

Some employers and their employees believe that stealing is in the natural order of things and should therefore be allowed

Many employees have never been told not to steal or that stealing has consequences, such as being fired

Low-pay employees tend to feel justified in stealing

High-pay employees steal, but because they are fewer in number than low-pay employees, the overall impact of their stealing is usually less

New employees are more likely to steal than long-time employees

The opportunity to steal is more often present than the motive to steal. Some employees steal, not because they need or want something, but because they have a chance to steal

Many honest employees see other employees steal but do not report it, often for stupid reasons

FIGURE 13.1

It would appear that a great deal of employee theft can be averted by educating employees.

According to Tyska and Fennelly (1998), the cost of crime (excluding computer crime) to American business is in excess of $40 billion per year. Perhaps the biggest problem is that most corporate managers do not know or do not want to know if they have a loss prevention problem. Some managers prefer to keep things as they are and to regard any suggestion of needed security as criticism.

Although internal theft does not account for all crime inflicted on business, its pervasiveness and heavy impact on the bottom line strongly indicate the need for a security program to prevent internal theft, and where prevention fails, determine why. The follow-on steps of a successful investigation are pursuit of restitution, termination of offenders, and vigorous criminal prosecution when appropriate.

The signals of theft by employees are not all that subtle and are fairly easy to spot. The main reason they are not spotted is that supervisors and coworkers don't think to look for them, and when spotted, they are attributed to other causes. The signals include the following:

- Gambling.
- Borrowing.
- Living above apparent income level.
- Writing bad checks.
- Indebtedness.
- Drug and alcohol abuse.

Things stolen by employees range widely and include the following:

- Cash such as receipts in a cash register.
- Merchandise such as items sold directly to consumers.
- Materials in production, storage, or transit.
- Desktop equipment such as PCs, fax machines, printers, and scanners.
- Furniture.
- Supplies.
- Sensitive information.

In addition to theft is the misuse of company assets. Violations range from copying personal documents on the office copier to using the mainframe computer to operate a side business.

Fraud Investigations

Fraud is not entirely an internal offense. It can involve collusion with outsiders or outsiders operating alone. The ordinary ritual is for crimes to be reported after they have occurred. The investigator goes to the place of the crime, interviews the victim and witnesses, and tries to figure out what

happened. This is not always the case with crimes involving fraud. Very often, the crime is discovered while in progress, often after it has existed for an extended period of time. Because the place of the crime is usually the place where the offender is working, the investigator must collect evidence and interview witnesses cautiously. The investigator does not want to give the offender an opportunity to destroy pertinent records before they can be seized. Neither does the CSO want the fraudulent activity to continue unabated.

Fraud is not necessarily crime committed by employees who wear white collars. The criminal can just as well be a shipping dock employee as a senior executive. In fact, the term white-collar has nothing to do with apparel and everything to do with the nature of the crime. The common elements are nonviolence, deceit, corruption, and breach of trust. The crime has no boundaries; victims can include individuals, businesses, schools, churches, and governmental units.

Business fraud operates out of view and is difficult to detect. At first, the victim is not aware of the loss, which usually takes the form of repetitive, incremental thefts. When discovery is made, it may be too late to recover even a small portion of the loss or to take strong action against the thief. Fig. 13.2 lists characteristics of fraud.

The mixed-bag nature of fraud techniques rules out the application of a universal test for determining the existence of a fraud in progress. The best a business can do is make sure loss control standards are operating properly and investigate when they appear to be not working.

Business fraud is complicated by a strange willingness of the courts and public to forgive fraudsters, and an inability of police detectives to deal with

Characteristics of Fraud

It is often discovered by accident or reported anonymously

It is difficult at first to figure out

It has been going on for some time

It is likely to span several investigative/prosecutorial jurisdictions

It usually violates more than one law

It is the act of a respected and intelligent individual

It often involves record destruction, such as when the criminal learns that an investigation has been opened

FIGURE 13.2

This list of characteristics is also a list of actions that signal a potential fraud in progress.

complex business-related crimes, a fact that places fraud investigations on the shoulders of corporate investigators. The police rationale is that they protect the public generally and that business losses are private matters and therefore not within the purview of law enforcement.

Medical Fraud

Employers who provide health benefits are often cheated through double billing, overbilling, and billing for services not performed. Bills are sent to the employee, the employer, and the health insurance carrier for the same medical service or product, thus tripling payments received. The crime can also be committed by billing for services provided by another physician or hospital. This is done by gaining access to the other provider's records and billing for the other provider's as-yet-unbilled services. Also included in medical fraud is ping-ponging, a practice in which the employee-patient is given unnecessary services at the same time needed services are performed. Fig. 13.3 is a pictorial representation of the first stage of medical fraud in which an initial record is made of treatment procedures that were not actually provided or not needed at all.

Bid Rigging

In this scheme, a contract awarded through competitive bidding is corrupted by connivance among the bidders. For example, the bidders collectively decide who will be the low bidder. For the next contract, a different contractor is chosen to deliver the low bid. To ensure substantial profit, the low bid and all the other bids are greatly inflated. Bid rigging can be difficult to prove

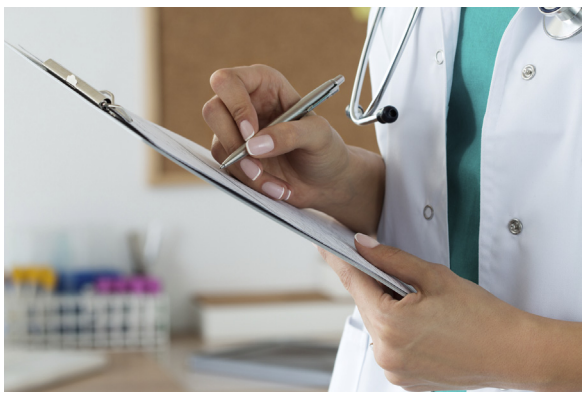


FIGURE 13.3

Subordinates unaware of fraud in progress can be tasked by the treatment provider to record services not performed or unnecessary to the treatment. *From iStockphotos.*

when the bidders operate from a tacit understanding, as opposed to a planned conspiracy.

False Billing

In a false billing scheme, a criminal sends to a company an authentic-looking invoice for products or services never ordered or received. The criminal hopes the company will process and pay the invoice without scrutiny. Some criminals, using lists of business addresses obtained from open sources (such as The Yellow Pages), will mail invoices with the hope that poor accounting procedures will result in payments. In other cases, the criminal will telephone companies and use enticing or high-pressure tactics to obtain orders for exorbitantly priced products. These sales persons falsely represent that the business has already ordered the product, either currently or in the past.

Workers' Compensation

A workers' compensation claim is likely to land on the investigator's desk when the circumstances of a workplace accident or injury point to the possibility of fraud. A claim can be judged suspicious when the alleged injury was not witnessed, the injury was not reported immediately, and treatment was not administered by a physician approved in the company's health benefits plan. Another indication is a difference between the employee's description of injuries and the report of medical treatment. Fig. 13.4 lists the indicators of workers' compensation fraud.

Indicators of Workers' Compensation Fraud

Be skeptical when these facts are present in a workers' compensation claim

- The injury was sustained in 1 week and reported the following week
- The accident occurred very close in time to a strike, a layoff, or a job termination
- The accident was not witnessed
- The claimant has a history of filing workers' compensation claims
- The claimant's initial description of the injury does not agree with the medical report
- The claimant is often not at home when called
- The claimant refuses a diagnostic examination to confirm the injury
- The claimant has hired a lawyer to pursue the claim
- The claimant's physician has a history of being involved in suspect claims
- The claimant switched to another physician after receiving a release from work

FIGURE 13.4

Investigation of fraudulent worker's compensation claims is usually assigned to the security group.

The plot thickens when the employee retains an attorney within days after the alleged injury.

When a questionable claim is indeed false, the claimant fears two outcomes: not obtaining the fruits of the fraud and getting caught in the attempt. To avoid those outcomes, the claimant may do everything to thwart the inquiry, such as not agreeing to be interviewed and accusing the investigator of harassment.

Care must be taken by the investigator to operate strictly within the law and ethical standards. For example, taking photographs of the claimant through a window of his or her home may seem like a good idea at the time, but it's an invitation to be charged for trespassing and invasion of privacy.

An example of a privacy violation was a case decided by the Georgia Court of Appeals. The plaintiff testified that the defendant (a private detective) cut a hole in her hedge, peered into a window, followed her when she left home, and behaved in visible ways that caused her neighbors to talk about her. The court found the surveillance unreasonable and awarded considerable damages to the woman.

Surveillance operations carry other types of risks. Stalking laws, which are relatively new, can place the investigator in legal hot water. As a general rule of thumb, an investigator gets into trouble in this area when the person being watched is placed in reasonable fear of bodily injury or is caused substantial emotional distress.

Criminal violations associated with surveillance involve wire taps, video and audio recordings in places private to the individual such as bedrooms and restrooms, and intercepted voice mail and e-mail. An example is a finding by a federal court jury that the American Broadcasting Company committed fraud and trespass against Food Lion in an undercover investigation of Food Lion's alleged doctoring and bleaching of spoiled meat and fish. An ABC employee hid a camera in a head wig and taped a microphone to her chest. A jury held that ABC had gone too far in gathering the evidence.

Bribery

Bribery occurs when an employee working in a responsible position accepts a payment of some type in exchange for special consideration. In the business environment, bribery is most often related to contracted services. It occurs when a corrupt employee working in a responsible position accepts a payment of some type in exchange for special consideration. Fig. 13.5 depicts the payment of cash, which is one of the methods of payment in a bribery scheme. Payment can be made in advance or at a later time. For example, an invoice sent by one conspirator to another is approved though the cost of

FIGURE 13.5
In this photo, cash is the bribery payment. *From iStockphotos.*

the product or service is inflated. When the first conspirator receives payment, a "kickback" is given to the person that approved payment. Other forms of illegal payments include discounts on personal purchases, gifts, use of a leased automobile, home improvement, and vacations. The special consideration given to the person making the payment can include awarding a contract improperly, overlooking deficiencies in the performance of the contract, certifying payment for unsatisfactory work or work not performed, and purchasing materials at inflated prices.

CRITICAL THINKING EXERCISE

Ralph Bonneville is the company investigator for Candler Enterprises. The CEO, Ellis Candler, wishes to expand operations by entering into a joint venture. Two companies have indicated a desire to be the joint partner: Adamson Consulting and Outerbridge Solutions. Candler instructs Bonneville to conduct due diligence inquiries on both companies. In the course of the inquiries, Bonneville is greeted by Steve Shepherd, a VP at Adamson. It turns out that Bonneville and Shepherd had served in the Army together in Afghanistan. Shepherd invites Bonneville to go with him to a night baseball game at Fenway Park. They meet at the stadium, and Shepherd takes Bonneville to a sky box leased by Adamson Consulting. Drinks and food are served by a caterer, and Shepherd gives Bonneville an autographed baseball bat as a memento of the occasion. The matter of the due diligence inquiry does not arise. The following morning, Candler receives a telephone call from the owner of Outerbridge Solutions who suggests that favoritism is being given to Adamson Consulting because during a baseball game the previous night Shepherd had been seen treating Bonneville as "royalty."

Candler calls Bonneville to his office and asks for an explanation. Bonneville tells Candler he was simply having fun with an old Army buddy, and it had never occurred to him the incident would be seen as favoritism.

Candler concludes Bonneville exercised poor judgment. He assigns the due diligence inquiries to another investigator and gives Bonneville a letter of reprimand.

What are your thoughts on the matter?

Compliance Investigations

A compliance investigation is launched when an organization (typically a large corporation) learns that its officers or other senior managers have engaged in misconduct that may expose the organization to criminal or civil liability or administrative sanction. An order by a CEO that resulted in the dumping of toxic chemicals in violation of an environmental protection law is an example of misconduct that would lead the organization's chairman or board of directors to order an investigation.

Bologna and Shaw (1997) are on record as saying the overall goal of the investigation is to gather information for the purpose of reducing punishment of responsible individuals or fines imposed on the company. The objectives determine the true facts of the violation, immediately discontinue the violation, compensate those damaged, and make the regulatory agency aware of the situation.

Computer Crime

Prosecuting a crime committed with the use of a computer may not be possible when there is no law covering the crime. However, it may be possible to prosecute on other grounds such as theft of service, criminal mischief, or eavesdropping. The Computer Fraud and Abuse Act (CFAA) was enacted by Congress in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030) makes unlawful and provides punishment for certain uses of computer technology to commit fraud and abuse proprietary rights. The CFAA defines computer crime as an act punishable by law when an automatic electronic device that performs mathematical or logical operations is used to commit crime, or damage, destruct, compromise, manipulate, or otherwise interfere with information owned by another party. The Act has been updated a number of times—in 1989, 1994, 1996, in 2001 by the USA PATRIOT Act, 2002, and in 2008 by the Identity Theft

Enforcement and Restitution Act. Further amendments are under consideration as the information technology threats continue to evolve.

The tools of crime committed with the use of a computer include infecting a targeted computer system with viruses and the like, stealing passwords, breaking codes, and circumventing firewalls.

Juniper research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015. But the actual price tag may be higher because some organizations fail to report losses because they do not want it publicly known they failed to protect themselves against computer crime. Reyes et al. (2007) recommend protective steps that can be taken by business organizations.

- Establish policies and work rules governing appropriate and inappropriate use of computers.
- Develop and enforce strict password rules.
- Establish procedures for auditing user accounts, computer accounts, and servers.
- Prohibit employees from holding in their personal possession sensitive information, including intellectual property.
- Discipline employees that allow unauthorized access to their computer.
- Regulate changes to phone numbers, fax numbers, e-mail addresses, and entry to the Internet and intranets.
- Report violations and suspicious activities that relate to the use of computers.
- Contact the FBI when fraud is confirmed or suspected.

Computer-assisted fraud can be made to work in just about any way a computer can be made to work. Ingenuity of the criminal plays a large part in making the amount of the theft substantial and the fraud undetectable, at least in the short run.

Computers can be used to secretly read proprietary data, such as learn the details of a business plan or a trade secret formula; change data to alter entitlements; obtain personal identification data for making purchases on credit cards issued to others; destroy or manipulate data; transfer funds to accounts accessible to the criminals; and order movement or delivery of goods. Computers can also construct a framework for perpetrating a fraud at a future time or wiping out the evidence of past and current fraud.

Undercover Investigations

The use of an undercover operative in a private investigation should be a consideration when criminal activity is affecting a business but the details are unknown and proof is needed to bring it to an end. An option for the business is to engage an investigative agency skilled in undercover operations. The agency is obligated to provide an operative that is experienced and free of prior crime. The work to be performed by the agency should be clearly set out in an agreement. It sometimes happens that the client gets cold feet or wants the operation to be altered in some way. Ferraro (2000) believes the client should never be allowed to call the shots. The client can provide useful information but should not be allowed to tell the investigative agency what to do, save shutting down the operation.

The first step is to bring the operative into the business in an apparently routine way such as hiring him or her to fill a vacant position, even if it means creating a vacant position. It will help if the operative has the skill and know-how to perform the tasks of the job or the job can be made so simple that skill and know-how are not necessary, such as a janitorial job. The position should be such that the operative is placed in a physical location where the activity can be observed. If the location proves to be the wrong location for observation, a routine transfer to a better location should be made.

The second step in the operative's game plan is determine the nature of the activity, i.e., the what, where, how, and who. In other words, find out what is being stolen or compromised, where the activity is occurring, how the activity is being carried out, and the identities of the persons involved. A controller, an experienced investigator, should be the operative's only point of contact with the agency.

The third step for the operative is to establish a relationship with the persons involved such as befriending a member of the criminal group or posing as a thief interested in becoming a member of the group. A cover story is essential and should be capable of validation in case the criminal group wants to check out the operative's cover story. A point needs to be made on this matter: if the operative is in danger, such as his or her cover being blown, the operative must be removed, and done so in a manner that does not confirm suspicions of the criminal group. An example would be transferring the operative to a new, remote location; firing the operative for a reason of manpower reduction; or firing the operative for a violation not actually committed. The objective is to protect the operative first and investigate the criminal activity second. After a reasonable period of time, a second operative can be inserted.

A fourth step is to avoid entrapment if the police are informed of the operation or are involved in anyway. Entrapment relates to the police, and if there is any indication the police have participated, even in a minor way, prosecution may not be possible. Also, there is the risk that at trial, the criminal group will attempt to show that the operative helped plan the activity and participated in it, and the activity would not have occurred if it were not for the operative. This can be shown if the operative participates in the activity and shares in the profits generated by the activity. If taking a portion of the stolen items or a share in the profits becomes absolutely essential in order to be "legitimatized" by the group, the operative should not personally benefit in any way and keep the stolen items and the share in a secure hiding place or turn them over to the controller.

A fifth step is to have a controller constantly receive information from the operative and direct him or her to take certain actions or avoid certain actions. The communication between the operative and the controller should be daily. The method of communication can be by telephone and recorded, provided use of the telephone does not draw suspicion. An alternative is to communicate by tape or CD that is left at a secure "drop" location. Communicating in writing (including e-mail) is a no-no.

Of great importance is the identification of places where stolen goods might be hidden before being removed from the business' facility. When the operation comes to a conclusion, the hidden stolen goods can be seized and held as evidence. Typically, the police arrive at the scene with a warrant. Property is seized and arrests made, including arrest of the operative. The idea is to conceal the operative's true identity. The standard police procedure is to separate the arrested persons while they are in confinement. This practice can facilitate a safe release of the operative. Depending on the judgment of the prosecuting attorney, the operative may or may not be called as a witness.

When the operative is able to use a camera with zero chance of being caught, the preponderance of evidence is increased. Obviously, the camera should have a time and date generator.

The operative should not keep notes. Everything goes to the controller on a daily basis. If the daily report is not made, the controller should be concerned that the operative is in trouble.

Interest Group Investigations

Interest groups use the Internet to acquire members, contributions, and public support of their causes such as protecting the ecology, establishing animal rights, and outlawing abortion. Some groups, certainly not all, will engage in

illegal acts that can range from intimidating to bombing. Companies that harvest lumber, use animals for research, or emit carbon are natural targets.

Other interest groups are much more radical. They are motivated by hatred of the government, hatred of another race, and extreme belief in a religion. Advocacy of a group's issue tends to create an opposing advocacy that can lead to violence.

Some interest groups will install "footprint software" on their websites that identifies visitors who may be persuaded to join or contribute funds or are perceived to be the opposition. When a visitor to the site remains on it for a long period of time or downloads certain information, a suspicion can be created that "the enemy" is plotting to take action. "Footprint software" allows the website owner to track back through the system and learn such details as the visitor's phone number. After that, it's a simple matter of using the phone number to learn the visitor's name or company and address. From there, all manner of details can be acquired. If purchases are made on the Internet, such as advocacy group publications, the purchaser opens a path of discovery to credit card information.

The paranoia that infests some advocacy groups opens a real possibility that even an innocent pause by a corporation on an interest group's website will be seen as an act of war, if not proof that "big daddy" is spying on little people whose only objective is to make the world a better place to live in. A corporation worried about retaliation, yet prudent enough to want to check out the opposition via the Internet, will insist that its investigators cover the electronic footprints.

How is that done? One way is to set up a drop box for billings and providing cover identification for the address. The idea is to provide a phone number or credit card not associated with the corporation or the investigators. A drop box that quickly comes to mind would be one in the name of a college student (real or false) using a post office box number. A credit card with a modest line of credit, such as $500, adds an element of credibility.

PHYSICAL EVIDENCE

Evidence is anything that tends to prove or disprove a fact. Within that general definition, physical evidence is any material substance or object, regardless of size or shape. Generally, there are three categories of physical evidence. Movable evidence is an item that can be transported or moved, such as a tool or glass fragment. Fixed or immovable evidence is an item that cannot easily be removed, such as a tree or utility pole. Fragile

evidence is an item that is easily lost, destroyed, contaminated, or subject to degradation. Examples include hairs, fibers, snow, ice, dust, and perishable food.

The success or failure of an investigation can depend on the investigator's ability to recognize physical evidence, derive understanding from it, and protect it. The process of evaluation begins with a preliminary collection of facts, preparation of an initial report, and concludes when the case is adjudicated. Evaluation is usually carried out in concert with forensic laboratory technicians, prosecuting attorney, private investigators, experts in certain fields, and persons whose knowledge contributes to a better understanding of physical materials and their relationship to the case at hand.

Evidence Collection

Identification Markings

Evidence must be marked for identification as soon as it is discovered. Identification markings help the investigator identify the evidence at a later date. Markings are normally made by placing initials, time, and date on the container such as a plastic, sealable bag containing hairs and fibers. The container is then marked for identification.

Evidence Tag

Identification markings on the container are supplemented by attachment of an evidence tag that is filled out at the time the evidence is acquired. Entries on the tag are made in ink, and the tag accompanies the evidence from the moment it is acquired until it is relinquished. An evidence tag is an administrative convenience for locating evidence while it is in custody: it is not a substitute for marking evidence.

Chain of Custody

When an item of evidence is received, it is recorded on a document called a chain-of-custody document. Because all persons who handle an item are considered links in the custody chain, the number of persons who handle the item should be kept to a minimum. An investigator in possession of evidence is personally liable for its care and safekeeping.

FORENSICS

Physical evidence collected by a corporate investigator can take on added probative value when it is examined at a forensic laboratory. The kinds of

physical objects amenable to forensic examination are numerous, as is the number of analytical tests for evaluating the objects.

Among all forms of evidence, physical evidence ranks highest in importance to the successful conclusion of an investigation. It is often something that a suspect leaves at a crime scene or takes from the scene or that may be otherwise connected to the crime. Forensic evidence aids in the solution of a case because it can establish the criminal's modus operandi, identify suspects, prove or disprove an alibi, connect or eliminate suspects, and provide investigative leads. Testimony of the forensics examiner is required for the evidence to be admissible.

Probative Value

Probative means to test for the purpose of proving. The word is also expressed as "substantiating" or establishing by proof of competent evidence. The word value is the advantage derived from the test, thus the term probative value. When an investigator collects materials that have a potential for becoming evidence and submits them to a forensic laboratory, he or she is attempting to establish probative value.

A crime lab examiner is an investigator. He or she applies a skill or knowledge to the analysis of physical evidence. Through the application of scientific principles and equipment, the examiner attempts to glean from the physical evidence every bit of probative value possible.

In a very meaningful sense, the investigator and the crime lab examiner are partners in a search for truth. The examiner's ability to make a thorough examination and present a conclusive judgment depends in no small part upon the investigator's ability to identify, collect, and preserve physical evidence in a manner that facilitates a full scientific examination.

A third party is involved in determining probative value. That party is the legal system. Laws and rules permit or prohibit the admissibility of evidence, and trial courts are required to rule within the framework of laws and rules. A good example is the Exclusionary Rule. Evidence collected illegally, such as by a violation of the search and seizure rules expressed in the Fourth Amendment of the US Constitution, can be excluded from presentation in court, thus canceling the probative value of the evidence.

Qualitative and Quantitative Analysis

A forensic lab makes determinations as to the properties and composition of samples of materials submitted. Two general types of analyses are

conducted: qualitative analysis, which establishes what the sample is, and quantitative analysis, which measures how much.

A sample of a single compound may be analyzed to establish its elemental composition or molecular structure and also its weight or volume. For example, a submitted sample might be a liquid, the properties of which are unknown to the investigator but are believed to be a poison. A specialist skilled in that area of forensic examination would analyze the sample according to its morphological appearance and its molecular structure and arrive at a conclusion as to what the sample really is. The examiner would also determine the quantity of the substance. So in this example, the examination was both qualitative and quantitative.

Mixed Samples

A sample consisting of more than one element is called a mixed sample. A mixed sample is usually analyzed by separating, detecting, and identifying its components by methods that depend on differences in their properties. Such differences can include volatility, mobility in an electric or gravitational field, and distribution between liquids that do not mix.

Markings

A sample that is an object, such as a crowbar or bullet, is not examined in respect to what it is made of but how it was used. In the case of a crowbar, the examiner's objective is to determine if the size and markings on the crowbar match markings on a jimmied door. In the case of a bullet, the examiner's task is to match the bullet with a particular firearm. In both of these examples, the examination is a visible examination using instrumentation that permits the examiner to see the distinguishing characteristics of the sample and match them against another sample such as the wood on the jimmied door or the lands and grooves in the barrel of the firearm.

DNA Samples

DNA technology is believed to be the most significant forensic breakthrough in the history of investigations. It can implicate the guilty and clear the innocent. The technology can resolve questions of identity. For example, a DNA profile can be made from the remains of an unidentified deceased and be retained for comparison with the DNA profiles of the parents or other blood relatives. DNA can also be useful as an aid in the identification of missing children.

A complete copy of an individual's DNA is found in every nucleated cell in the body. Body surfaces that are normally wet (e.g., surfaces inside the mouth, nose, eyes, and urogenital tract) are lined with epithelial cells that continuously slough off. These cells are easily transferred to objects with which they come into contact and as a result can be a good source of material for DNA testing. These sources can include envelopes, stamps, cigarette butts, and chewing gum. Materials very suitable for DNA testing are blood and semen stains, hairs, bone, and teeth.

Arson Debris Samples

If there is residue at the site of a suspected arson, such as wood that appears to have been soaked with an accelerant, such as gasoline, a sample of that residue is collected by the investigator. At a separate location where accelerant residue is not detected, the investigator takes another sample. This second sample is called a reference sample. The sample containing the suspected accelerant is compared against the reference sample. Many such samples are collected to assist the lab technician make a definitive conclusion.

Blood Samples

The same approach applies to blood. Assume that blood is found on a bed sheet. The origin of this blood cannot be determined without a reference sample. In this case, a reference sample would be taken from the blood of a suspect. Both are compared to determine if they match. DNA testing is the gold standard for this type of examination.

Assume in the above case that a suspect has not been identified. The lab can prepare a DNA profile of the unknown sample and then compare its profile against profiles in an existing database. This type of comparison is computer assisted.

In many of the serious cases, such as homicide, the DNA profile is prepared and placed on file to be used if a suspect is later identified.

Deceased Persons Samples

With recently deceased persons, biological samples are obtained incidental to autopsy. Such samples can be blood, teeth, bones, and tissue. If a blood sample can't be collected, such as would be the case of a badly decomposed or burned person, a tooth can be collected, preferably an unrestored molar. This should be collected only after the teeth have been charted for identification purposes. If teeth are not available, then a segment of rib bone or a

segment of the femur can be collected. This segment should be at least one to two inches in length.

Tissue Samples

Tissue, including partial or complete organs, is collected by a pathologist during an autopsy. These samples are valuable in determining the cause or manner of death, as opposed to identification of the deceased.

Fingerprint Samples

Each finger and thumb is unique to an individual, and no two prints have ever been found to be the same from two different people. Also, palm and footprints are also unique to each individual. A person's fingerprints do not change. Barring scar-causing injury, fingerprints, palm prints, and foot prints remain the same from birth until well after death.

There are approximately 75 to 200 characteristics on a finger or thumb. The forensic analyst uses a variety of techniques such as carbon powder dusting, super-glue and ninhydrin spray techniques, amido-black print visualization, and argon laser analysis to identify and match prints.

Fingerprints of unidentified persons may be compared with the fingerprints of known persons or to fingerprints on file. The Federal Bureau of Investigation maintains a fingerprint file on more than 90 million people, which is in addition to fingerprint files maintained by most state law enforcement agencies.

The analysis of fingerprints in a forensic lab is dual purpose: first, to develop the prints to a condition that allows them to be seen and second, to match the prints with another person such as a suspect, a missing person, or a victim.

The Automated Fingerprint Identification System (AFIS) is a computerized system that stores the fingerprint characteristics of millions individuals. AFIS makes systematic computer searches of unknown fingerprints by optically scanning a print and comparing it with those on file. Prior to AFIS, fingerprint searches had to be done manually, making it an impractical, time-consuming process to compare an unknown print to the millions of known prints on file.

A latent print is an impression left on a surface that has come into contact with friction ridge skin (fingers and palms of the hand and toes and soles of the feet).

The latent print is usually "hidden" or not visible to the human eye. Therefore, latent prints have to be processed by some means to render them visible. A latent print is composed mainly of sweat and any foreign material that may be on the finger, palm, or foot at the time the print is deposited on a surface.

A known print is a print acquired from a person who is known such as the victim of an offense or a suspect in custody. The print is obtained by placing the person's fingers on a platen that illuminates and copies the print in much the same way a document is scanned on a computer.

Drug Samples

A drug examination is typically an examination of illegal drugs such as marihuana, cocaine, methamphetamine, amphetamine, heroin, prescription drugs, and designer drugs. There are many technologies for examining drug samples. These include gas chromatography/mass spectrometry, Fourier transform infrared spectrophotometry, ultraviolet visible spectrophotometry, and bench chemistry techniques.

Ballistics Examinations

Ballistics examinations are different than firearms examinations. In ballistics, the examination is of the projectile, while a firearm examination focuses on the weapon used to fire a projectile. This ballistics examination draws upon the science of propulsion, flight, and impact of projectiles. The science of ballistics can be divided into several types: internal, external, terminal, and wound.

- Internal ballistics deals with the propulsion of projectiles, such as within the barrel of a gun. A gun converts chemical energy of a propellant into kinetic energy of a projectile.
- External ballistics deals with projectile flight. The trajectory, or path, of a projectile is subject to the forces of gravity, drag, and lift.
- Terminal ballistics deals with the impact of projectiles on a target.
- Wound ballistics deals with the mechanisms and medical implications of trauma caused by bullets and explosively driven fragments such as shrapnel.

Firearms Examinations

The firearms examiner studies expended cartridge cases and bullets to determine if they can be linked to a specific firearm. This examination also allows a determination to be made of the type of weapon used. Other examinations

can include function and accuracy tests, trigger pull measurement, and measurement of muzzle-to-target distance.

A firearms section will also participate in the National Integrated Ballistics Information Network (NIBIN), a computer-assisted program that can link a firearm to different cases in different jurisdictions.

The examiner relies on two types of characteristics when performing comparisons: class and individual characteristics.

- Class characteristics are common to a group of firearms. They comprise caliber, number of lands and grooves, direction of their twist, and their widths.
- Individual characteristics are the markings that actually allow an examiner to say that a projectile or cartridge case relates to a specific firearm to the exclusion of all other firearms.

Shotgun Examinations

Several examinations can be performed on evidence involving a shotgun. The hull of the shotgun shell can be matched against the shotgun that fired it, and the pellets and wadding can be compared to the expended hull to determine if they are consistent with the gauge, shot size, and manufacturer of the hull submitted.

The firearms examiner will routinely examine an unfired shotshell to determine if it was loaded into and extracted from a weapon based on the presence or absence of extractor marks.

The distance at which a shotgun was fired can be determined by test firing the suspect weapon at various distances, using the same type of ammunition involved in the case.

Gunshot Residue Examinations

Gunshot residue is material deposited on any part of the body, most particularly the hands, face, and clothing of the shooter, as a result of the discharge of a firearm. The residue can include particles from the primer, the gunpowder, the projectile, and the cartridge case. Particles from the primer and gunpowder are most forensically significant.

Current technology does not allow gunshot residue to be linked with a particular firearm or ammunition. This is because nearly all ammunition, regardless of type of manufacture, contains the same basic materials.

The presence of gunshot residue on the hands of an individual indicates that the person recently discharged a firearm, handled a firearm or an object with gunshot residue on its surface, or was in close proximity to a firearm when it was discharged.

In a suspected suicide by gunshot, the presence of residue on the victim's hands has little probative value. In those cases where the investigator suspects someone else may have been involved, the analysis of samples from other individuals present at the scene may prove helpful.

Tool Mark Examinations

The methodology of tool mark examinations parallels that of firearms examinations: the examiner looks for class characteristics and individual characteristics. By examining impressions on various materials, such as wood, metal, and plastics, the examiner is able to identify the class of tool that made the impression, for example, a pry bar or screwdriver.

Also by observing unique variations in the impressions, such as those made by a chipped edge on a screwdriver, the examiner is able to match a particular screwdriver with a particular impression to the exclusion of all other screwdrivers.

The tool mark examiner also examines objects that have had their serial numbers altered or removed and objects that have been fractured.

Questioned Documents Examinations

A document examiner studies written and/or machine-generated documents to determine authorship and authenticity. The documents typically examined include checks, wills, birth and death certificates, business agreements, forms and correspondence, suicide and threat letters, ransom notes, tickets, coupons, and voting ballots.

In addition to establishing authorship and authenticity, the examiner can connect a typed document with a particular typewriter, printer, or copier; connect a torn document with a missing part; connect a stamped impression on a document with the item that formed the impression; and restore obliterated data.

Standards and Exemplars

When authorship is the issue, the examiner must have, along with the questioned document (called the exemplar), a number of handwriting or hand printing samples (called standards or known standards). The examiner's objective is to determine if the person who wrote the exemplar is the same person who wrote the standards.

The original of the exemplar is much preferred by the examiner. Copies can conceal some of the fine details of pen writing and can also disguise simulation and tracing of a signature and the use of cutting and pasting.

When a questioned document is examined for fingerprints in addition to examination of authorship or authenticity, the document should be placed inside a clear plastic wrapper, accompanied with a written request to have the document also processed for latent prints.

Requested Standards

A standard is known when it was obtained when the taking of it was directly witnessed. Such standards are called requested standards. The paper and writing instrument must correspond to the paper and writing instrument of the questioned document. The number of requested standards that should be obtained is typically between 15 and 20 depending on length and may variously contain cursive writing, printing, and Arabic numerals.

Collected Standards

A standard is called a collected standard when it appears on a document that was collected. The nature of a collected standard must be such that it definitively establishes authorship. For example, signatures in a loan application file might serve as collected standards.

Forged Writings

There are three types of forged writings:

- Traced forgery: In this type, the writer traces over a signature or other writing. Because the writer does not write in his or her natural hand, it is not possible to identify the writer, but it is possible to determine if the writing was produced by tracing.
- Simulated forgery: This is the copying of a signature or other writing by "drawing" it. If the writing contains enough normal characteristics of the writer's true hand, it may be possible to identify the writer. In any case, a determination can be made that the writing itself was produced by simulation.
- Freehand forgery: This writing is made in the natural hand of the writer. No attempt is made at tracing or simulating. In freehand forgery, the identity of the writer may be determined.

In all three types, the document examiner will need to have "true" writing in order to make comparisons.

Torn Paper Examinations

Forged checks and official documents with erasures are common in fraud cases. Torn documents collected during an investigation appear less frequently, and perhaps because of infrequency, investigators make mistakes in submitting torn documents to an examiner. A common mistake is to attempt reconstruction by taping pieces together. The document examiner, no matter how skilled, cannot perfectly disassemble a reconstruction. The result may be a lost opportunity to conclusively determine that torn part A matches perfectly with torn part B. This extra handling at the lab can also damage the document's surface and the writing on it.

Another mistake is to send the document to the lab in an envelope heavily sealed with tape. Tape used in excess makes it difficult for the examiner to open the envelope to remove the torn document without damaging it. Moistened tape, such as brown paper tape drawn through water, can cause moisture to migrate into the envelope, make contact with the torn document, and cause blurring of ink and disappearance of indented impressions.

In addition, a document examiner can make conclusions based on study of:

- Altered or obliterated writing.
- Impressions created by a typewriter.
- Photocopied material.
- Machine-printed material.
- Paper (torn edges, water mark, impressions, charring).
- Documents the true age of which is in question.
- Inks and writing instruments.

It is possible to determine if a particular pen is the source of ink comprising the writing on a questioned document. Ink examinations have only two possible results: (1) significant differences existing between the inks indicate they are different or (2) no significant difference was found between the two inks by the examination techniques applied. Not finding a difference does not prove that two or more inks are the same.

There is no known technique that can prove two ink samples are identical. While it may be able to say that two inks are different, it can't be said they are the same.

Ink pens are mass-produced products with class characteristics, but virtually no individual characteristics. The only exception to this might be an unlikely situation involving someone creating a very small quantity of ink with a unique formula for one-time use.

A few ink manufacturers have added trace elements to ink formulas to signify the date that the formula was introduced. These "tags" make it possible to

determine the earliest possible date that an ink existed for use in making a questioned writing. Ink examinations are categorized as destructive and nondestructive. Destructive exams involve removing ink samples from documents or pens and analyzing their physical components. Nondestructive exams involve visual and instrumental assessments of the appearance and spectral response characteristics of inks.

Other Types of Examinations

A forensic lab with a full range of expertise and instrumentation can perform all the examinations just mentioned. In addition, examinations can be made of paint, glass, fibers, hair, and metals.

POLYGRAPH TESTING

The Employee Polygraph Protection Act (EPPA) of 1988 permits the testing of employees only for the investigation of crimes in which the employer has an interest. An employer may test an employee who falls under a cloud of reasonable suspicion. Reasonable suspicion can be shown when the employee was at the place of the crime at or near the time of the crime, had opportunity (such as access to property that was stolen), and is implicated by a credible witness. A showing of reasonable suspicion is also present if an employee lied when questioned about the crime. Fig. 13.6 depicts finger attachments used to measure galvanic skin resistance.

Written Consent Required

Testing can be done only with the written consent of the suspect. Prior to obtaining the consent, the employer and/or the polygraph examiner must disclose to the suspect the specific offense under investigation, time and place of the offense, and why the employee is a suspect. If reasonable suspicion is supported by a witness, the name of the witness can be withheld from the suspect.

Polygraph Theory

Lie detection is based on the assumption that when an individual experiences apprehension, fear, or emotional excitement, his or her respiration rate, blood pressure, and galvanic skin resistance sharply increase. A polygraph instrument records the changes as the individual is questioned by a trained examiner. The examiner interprets the recordings and renders an opinion as to the truthfulness of the person examined.

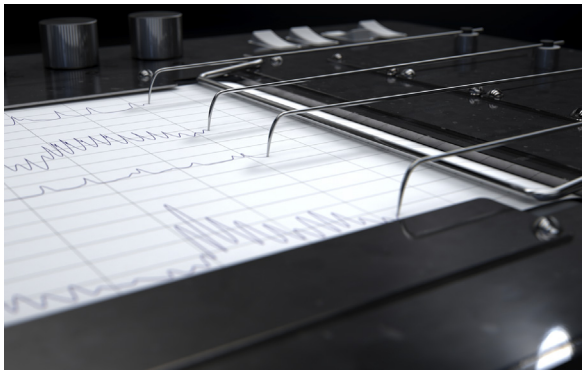


FIGURE 13.6
A polygraph examination can whittle down the number of persons who had the opportunity to commit the crime under investigation. *From iStockphotos.*

The theory behind the polygraph technique holds that a conscious mental effort to deceive made by a normal, healthy person will cause certain physiological changes detectable by the polygraph instrument. These changes are driven by the autonomic nervous system, which regulates the body's internal environment and is generally involuntary. The parasympathetic nervous system, a division of the autonomic nervous system, dominates in relaxed situations. It performs routine "housekeeping" functions such as digestion and maintenance of body temperature. No matter how hard an examinee might try, he or she will not be able to prevent physiological changes in respiration rate, blood pressure, and galvanic skin resistance.

Polygraph Accuracy

Hundreds of studies conducted over the years to determine the accuracy of the polygraph technique have produced less than conclusive judgments. Still, a preponderance of the data indicates that when properly trained examiners utilize an established testing procedure, the accuracy of their decisions is generally in the range of 85%–95% for specific-issue investigations. Few studies have been made to determine the range of accuracy for preemployment testing.

One of the problems in judging overall accuracy is a misunderstanding of the term inconclusive as it used in the reporting of test results. An inconclusive result simply means that the examiner was unable to render a definite

conclusion. By way of illustration, if 10 polygraph examinations were administered and the examiner was correct in 7 decisions, wrong in 1, and had 2 inconclusive test results, the percentage of accuracy is 87.5% (7 out of 8). Others would say the percentage is 70% (7 out of 10).

Polygraph Errors

Polygraph errors are nearly always human errors. They tend to center on the examiner's failure to prepare the examinee for the test and correctly read the data on the polygraph charts.

A false positive test report occurs when a truthful examinee is reported as being deceptive. A false negative report occurs when a deceptive examinee is reported as truthful. It is widely believed that negatives occur more frequently than positives, perhaps because examiners would rather let a deceptive individual get by than to declare an innocent individual deceptive.

THE DEPOSITION

A deposition is an out-of-court proceeding conducted for the purpose of preserving the testimony of the investigator-witness for later use in court. The setting is often the conference room of an attorney's office. The persons present are the investigator, lawyers for the concerned parties, and a reporter using a stenotype machine. In some cases, the deposition will be recorded using audio or audio/video equipment.

The deposition begins with the investigator being placed under oath. The lawyers take turns in asking questions. A lawyer may skip a turn or take more than one turn. The proceeding is relatively informal, although serious to the final outcome of the case. The reporter takes down everything said and the reporter's record is later typed and bound in a document called a transcript.

The deposition is essentially a discovery tool for opposing lawyers. Each side wants to learn what the investigator's testimony will be at trial. In a civil suit, for example, the plaintiff's lawyer in deposing the investigator wants to:

- Discover what the investigator knows concerning the facts involved in the matter being litigated.
- Discover if the investigator knows of any facts that may be damaging to the defendant (e.g., that the defendant may have been careless or failed to do something).

- Commit the investigator to the statements made under oath so that at trial his or her testimony cannot be changed, at least not without difficulty.
- Look for ways to discredit the investigator.
- Use the investigator's testimony to discredit other defense witnesses.
- Attempt to learn the basic theory and strategy the defense will rely on at trial.

Although a deposition can embarrass or even damage the reputation of the investigator, this is not a legitimate purpose of the proceeding. When it happens, it is often the result of inadequate preparation.

DISCOVERY

In American law, discovery is the pretrial phase in a lawsuit in which each party through the law of civil procedure subpoena or through other discovery devices. These other discovery devices can include requests for production of documents and other evidence from other parties and can compel the production of material held by the other side.

Discovery can require the production of interrogatories, motions or requests for production of documents, requests for admissions, and depositions.

The common or traditional forms of discoverable materials include reports, photos, medical images, drawings, reconstructed video, video and audio tapes, e-mail, fax, archives, and data drawn from a variety of sources.

However, the increased use of technology has produced new forms of discoverable materials such as that drawn from the following:

- Servers.
- Hard drives.
- PCs.
- Laptops.
- USB flash sticks.
- iPods and similar devices.
- Any material that appears to have been deleted from a hard drive but can be captured by computer forensic specialists.
- Internet sites such as YouTube, Facebook, and MySpace.

Because personal information is not discoverable, the attorney and the investigator can avoid giving up some forms of information.

PRETRIAL PREPARATION

Getting ready for trial will include one or more meetings between the investigator and friendly counsel. Details are examined so that both parties have a clear and shared understanding of the case. The investigator wants to ensure that the attorney knows all the facts, favorable and unfavorable. The attorney will want the investigator to know what to expect while on the witness stand, during both direct examination by the attorney and crossexamination by the opposing attorney. As a matter of strategy, the attorney may be very interested in some facts and less interested in others. The attorney may lead the investigator through a practice run of questions he or she will ask and questions likely to be asked by the opposing attorney. Rehearsal of this type is perfectly proper provided the investigator is not influenced to deviate from the truth.

Testimony cannot be effective without solid preparation. Notes, sketches, reports, photographs, and physical evidence are carefully studied. Because the time between the closing of an investigation and the opening of a legal proceeding is normally quite long, the investigator needs to expend considerable effort in memory refreshment immediately prior to appearing on the witness stand. Preparation is often difficult when there is a long period of time between completion of the case and prosecution of it.

Day after day of highly competent investigation may be wasted when testimony is poorly presented.

The investigator has three fundamental obligations. First is to tell the truth, even if the truth hurts. This is an obligation that stands above the outcome of the trial. Second is to be fair. This does not mean the investigator has to give equal favor to both sides, only that he or she does not overstate or color the facts. Third is to be accurate.

TRIAL PROCEDURES

The principal parties are the judge, jury, defendant, prosecuting attorney, defense attorney, and witnesses. A civil trial will have, in addition to the above principals, a person or entity called a plaintiff. The plaintiff is the complaining party and the complaint will allege one or more torts (civil crimes). Jurors stand out because they weigh the facts presented. When a person is

called for jury duty, the service is usually not optional: one must attend or face strict penalties.

Once a potential juror has entered the courthouse, he or she must fill out a jury questionnaire. After the form is filled out, the potential juror waits until called to a courtroom. The judge and attorneys for each side will use the *voir dire*, a series of questions designed to determine if a juror is acceptable for the case being tried. The prosecution and defense may dismiss potential jurors for various reasons, which may vary from one state to another. Also, the opposing attorneys may be allowed a number of arbitrary dismissals that do not have to be for specific reasons. The judge may also dismiss potential jurors.

At trial, the questioning of a witness is carried out in accordance with established rules. Among these are the taking of an oath, direct examination by the attorney who called the witness, and crossexamination by the opposing attorney. Redirect and recross questioning may follow.

Securing information from a witness is by a question-and-answer method. The questioning by an attorney (friendly counsel) on direct examination guides the witness. After direct examination, the witness may be subject to crossexamination by opposing counsel.

Questions on crossexamination have the opposite purpose of those asked on direct. Crossexamination questions may be devious, deceptive, or innocent in appearance, masking the opposing counsel's real objective, which is to discredit or minimize the effect of the witness's testimony.

The jury enters the proceeding with no prior knowledge of the matter to be decided. The picture the jury gets will depend largely on the ability of witnesses to tell the story.

The opposing attorney will do everything legally permitted to distort and twist the testimony of the investigator witness. If the investigator appears confused, hazy, or unsure of important facts, the jury will be similarly confused and hazy. An opposite and positive effect results when the investigator presents facts clearly, calmly, and fairly. A verdict favorable to the investigator will be happily received, but will accomplish little in the long run if inaccurate testimony affords opposing counsel grounds for acquittal, a new trial, or for reversal on appeal.

Rapport

Rapport is an affinity between persons. In the immediate case, we are discussing rapport between the testifying investigator and the jury and judge. Establishing rapport depends on making a good first impression, which

consists of three intertwined characteristics: appearance, speech, and body language. Experts say that the strength of appearance is first, body language second, and speech last. This is not to say that one without the other two is acceptable. All must be apparent during the investigator's testimony.

Appearance

A good appearance is demonstrated either positively or negatively by the following:

- Grooming.
- Hygiene.
- Body piercings.
- Flashy jewelry.
- Tattoos.
- Hair care.
- Makeup.
- Five o'clock shadow.
- Body odor.
- Too much perfume, cologne, or after-shave lotion.

The clothing of the investigator should be as follows:

- Conservative.
- Clothes that conceal perspiration.
- Be of a neutral color.

The attire of the investigator should not be as follows:

- Outdated.
- Worn.
- Stained or faded.
- Baggy or sloppy.
- Brightly colored.
- Faddish.
- Flashy and trendy.
- A cowboy belt, cowboy boots, or bolo tie (unless testifying in an area where such attire is normal and expected).
- A brightly colored tie or a tie with a pattern that could draw a juror's attention away from the testimony.
- A tie pin in the form of handcuffs or other type of authoritative design.
- White socks.
- Shoes that do not match or blend with the color of the clothing worn.
- A hat.
- Moccasins, sandals, or other nonconservative shoes.

Body Language

Body language is next important in making a good impression:

- Look at the jury when making a point.
- Don't cross the legs or slouch in the witness chair.
- Remain calm and cool, especially during cross examination.
- Enter and depart the courtroom with a confident walk.
- Do not press the forehead or make similar gestures that suggest confusion or lack of memory.
- When asked a critical question, ponder over it even when you know the answer.
- Do not look at the jury when entering or leaving the courtroom.
- Do not point unless told to.
- Restrict unnecessary hand movements.
- Do not use gestures or sounds as a substitute for words.
- Restrict facial expressions.
- Do not chew, drink, or eat anything while on the stand.
- Keep the mouth free of toothpicks or similar items.
- Do not fiddle with a pen, jewelry, buttons, necktie, or anything else that could draw attention away from the jury.

Speech

Speech is also important in making a good impression. The testifying investigator should:

- Speak loudly and clearly.
- Give testimony chronologically, if allowed by the nature of questions asked.
- Be as accurate as possible concerning times and places, where evidence was found, important words spoken by actual witnesses, and other details that help the jury form a picture in their minds.
- Use proper pronunciation; refer to a dictionary in advance if unclear on the pronunciation and meaning of unfamiliar words that may need to be spoken while testifying.
- Do not mumble.
- Avoid lazy speech or speech suggestive of a poor education.
- Practice anticipated testimony in front of a mirror, another person, or with use of an audio or video recorder.

CONCLUSIONS

Investigating is a complex and sophisticated function. The CSO, who manages investigations, does not need to be an expert in the details. It is

sufficient that he or she be able to recognize when intervention is needed to get an investigation back on track or to keep it from straying outside the boundaries or company rules or the law. The investigator's focus is on basic tasks that bring a single issue to a satisfactory conclusion. The CSO's focus is on the major goal of aligning the investigative function with loss-prevention activities. Also of importance to the CSO's role is ensure that investigators be fully prepared to testify at depositions and trial.

REVIEW QUESTIONS

1. What is the purpose of an investigator?
2. Explain the difference between constructive and reconstructive investigation.
3. Give an example of a standard.
4. What is an administrative inquiry?
5. What is possibly the most frequently investigated incident in the business environment?
6. Name three actions that management must take to curb employee theft.
7. Fraud is not necessarily crime committed by employees that wear white-collars. Explain this statement.
8. State the theory underlying the polygraph technique.
9. Differentiate between bribery and kickback.
10. What is a compliance investigation?
11. Name the methods of industrial spies.
12. What is the purpose of a deposition?
13. What is discovery?
14. Name the sequence of questioning at a trial.

References

Bologna, J., Shaw, P., 1997. Corporate Crime Investigation. Butterworth-Heinemann, Boston, MA.

Broder, J.F., 2000. Risk Analysis and the Security Survey. Butterworth-Heinemann, Boston, MA.

Ferraro, E., 2000. Undercover Investigations in the Workplace. Butterworth-Heinemann, Boston, MA.

Hemphill Jr., C.F., 1976. Management's Role in Loss Prevention. American Management Association, New York.

Muus, J.P., Rabern, D., 2006. The Complete Guide for CPP Examination Preparation. Auerbach Publications, New York.

Reyes, A., O'Shea, K., Steele, J., Hansen, J.R., Jean, B.R., Ralph, T., 2007. Cyber Crime Investigations. Elsevier, Inc, New York.

San Luis, E., Tyska, L.A., Fennelly, L.J., 1994. Office and Building Security. second ed. Butterworth-Heinemann, Boston, MA.

Tyska, L.A., Fennelly, L.J., 1998. 150 Things You Should Know About Security. Butterworth-Heinemann, Boston, MA.

Further Reading

Forbes, January 17, 2016 @ 11:01 AM. Cyber Crime Costs Projected To Reach $2 Trillion by 2019. <http://www.forbes.com/sites/stevemorgan/2016/01/17/> (accessed 27.10.16).

CHAPTER 14

Preemployment Screening

What You Will Learn

- The rationale for preemployment screening.
- Negligent hiring and its consequences.
- Federal legislation relevant to screening and hiring practices.
- Major provisions of the Fair Credit Reporting Act (FCRA).
- The nature of a background inquiry.
- Tests used in preemployment screening.

INTRODUCTION

Employers conduct preemployment background checks because laws and regulations place a duty on them to maintain a safe and secure working environment, including the duty to protect workers, guests, and the public from the harmful acts of employees.

When harm occurs and the employing company cannot show it acted reasonably to maintain a safe and secure working environment, severe penalties can result from civil lawsuits and sanctions by watchdog agencies.

Harmful acts committed previously by prospective employees cover a wide number of crimes such as murder, rape, assault, and drug dealing. Prior harmful acts can include on-the-job safety violations that injured or killed coworkers. Job applicants with a potential to commit harmful acts can be filtered out of the hiring process through preemployment screening.

Employers also find that background inquiries (BIs) can improve productivity and reduce costs. Job applicants with poor work habits and excessive absences from the job can be dropped from consideration, along with persons who drive up medical insurance costs due to injuries to themselves and others.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00014-1

When a security department has few or no investigators, the preemployment screening function is farmed out to a company skilled in performing the function. A private investigative is the common choice.

NEGLIGENT HIRING

Capwell (2007) defines negligent hiring as the employment of a person who poses dangers to others. Negligence is shown when the employer failed or did not try to know of an applicant's undesirable background at time of hire, and at a later time, the hired person caused harm to another.

Civil suits alleging negligence in hiring have never been more numerous, and abatement is not seen on the near horizon. Severe workplace violence, assault, employee theft, sexual harassment, injury-causing accidents, and other incidents occurring in the workplace that lead to the filing of a lawsuit are anathema to employers. Negligent hiring lawsuits are extremely costly to defend, and if the plaintiff is successful, a multimillion dollar award is not uncommon. A well-conducted examination of an applicant's background can save an employer a great deal of grief and money.

The Latin term *respondeat superior* means "let the master answer." In law, it is often the basis for negligent hiring allegations. Under this concept and under certain circumstances, an employer can be held liable for the unlawful act of an employee.

A company runs a risk when it relies solely on information provided by the applicant in a résumé or a job application form. It is almost certain that an applicant will be less than perfectly truthful in his or her representations. Of course, some less than truthful facts will be minor. It is the major lies the employer needs to worry about such as lies relevant to rape, assault, theft, and incidents involving illegal drug use. If there is any one act of a security nature that an employee should do is screen every applicant.

EMPLOYMENT APPLICATION FORM

The employment application form is the main administrative device for capturing prior employment and personal references information. Quite commonly, dishonest applicants provide some truth in their references. For instance, they might provide the correct name of a former employer and change the location or provide the proper city and state of their school but change its name. These deceptions can come to light by simply using the services of long-distance information.

D'Addario (1993) cautions the application reviewer not to place great reliance on work references provided by the applicant. Work references given by a criminal are likely to produce excellent recommendations that may be totally false. The reviewer should ask to speak to past and present coworkers other than persons named on the form.

Tyska and Fennelly (1998) make the point that certain questions cannot be asked on an employment application form, or for that matter in any manner connected with a hiring decision. For example, an applicant can be asked about criminal convictions but not about arrests. Prohibited questions relate to:

- Religion.
- Age.
- Marital status.
- Number of children and number of times married.
- Ethnicity.
- Disabilities.
- Political leanings.
- Sexual orientation.

VERIFYING APPLICATION INFORMATION

The standard practice is for an employer to obtain a completed employment application before considering the applicant for a job. An employment application will almost always pose questions that are designed to aid in the hiring decision. A well-designed application will do three things:

- Rule out improper questions that can violate the various laws and rules pertaining to job selection.
- Obtain the applicant's signature indicating that he or she understands that prescreening may be necessary and willingly consents to screening such as accessing public records and interviewing people.
- Inform the applicant that false information or omitted information can result in a refusal to hire.

From an investigation standpoint, the desirable criteria for application entries are as follows:

- Full name and aliases.
- Social security number (SSN) and/or driving license number.
- Place of birth.
- Date of birth if age is relevant to the job (Obtaining a date of birth is permissible if the applicant is 40 years or older and the job requires a

certain level of strength or stamina or if the unique demands of the job require the worker's age to be in the range of a certain number of years.)
- Current address and chronology of previous addresses.
- History of prior jobs.
- Military history, this search is made to verify an applicant's military history. The information source is the National Personnel Records Center in St. Louis, MO. Go to www.archives.gov/facilities/mo/st_louis/military_personnel_records.html.

Information on the form can aid the private investigator (PI) when checking criminal and civil records, verifying employment history, and crosschecking against other information sources.

Credit Headers

Certain information is essential to making a full credit heading search. The best possible types of information are complete name, aliases, date of birth, current or former addresses, and SSN. The last of these is most important.

Without facts to go on, a wider investigation will be necessary. If the investigator manages to obtain the SSN, it will lead to a credit header, which will contain missing information.

A credit header is at the top of a credit report that contains the subject's name, date of birth, and confirmation of the SSN. Credit headers are important preliminary investigative documents because they can provide leads to other relevant information. A credit header can provide the best and most reliable information about a subject's SSN, name, address, and telephone number. However, some information called from credit headers are considered personal information, and therefore prohibited by the Gramm–Leach–Bliley Act (GLBA). Not all is lost, however, because the law covers personal information, not public information. Information that relates to a subject's personal life is not allowed to be reported, but information of a public nature such as name and address are not covered.

Credit headers are sold by information brokers who routinely sell public information to anyone who wants to buy it such as police agencies, skip tracers, debt collectors, and professional investigators. The more common of the brokers are Merlin and Tracers.

Wherever possible, credit header information should be crossreferenced because, although valuable, it has been known to contain incorrect information. An easily available crossreference is police information compared against course records.

There is no national criminal database that contains all criminal record information. If there was such a database, employers would use it on their own without recourse to investigators. Public Access to Court Electronic Records (PACER) is an electronic public access service that allows users to obtain case and docket information online from federal appellate, district, and bankruptcy courts, and the PACER Case Locator. PACER is provided by the Federal Judiciary in keeping with its commitment to providing public access to court information via a centralized service. PACER is as close to a national database as can be found, but it contains federal offense information only.

By contrast, criminal justice agencies, such as the police and Federal Bureau of Investigation (FBI), have access to criminal information collected from their own investigations and information on file in state law enforcement agencies. This information is sent by the states to the National Crime Information Center. Some states have formed state-level criminal information centers for their own purposes.

The Social Security Number

The SSN is a nine-digit number that looks like this: 012-34-5678. The first three digits are an area number. Before 1973, the area number corresponded to the state where the individual obtained his or her social security card. After that, the first three digits were changed to correspond to the ZIP code of the mailing address shown on the individual's application for the card. The middle two digits are the group number. The last four digits are serial numbers. They represent a straight numerical sequence of digits from 0001 to 9999 within the group.

A SSN Check can provide the names and addresses associated with a given SSN, and that is all. It only indicates that the number is accurate. To make a check, go to www.socialsecurity.gov/foia/highgroup.htm.

A separate file, called the Social Security Death Master list, can be accessed at www.ntis.gov/products/.

Although originally used to administer social security benefits, the SSN has nearly become a national ID number.

Employer Preferences

An outside investigation agency might provide preemployment screening services to several employers. In all likelihood, each employer will have its own set of preemployment screening policies and practices, and while these guidance documents will be in different words and formats, they must conform to the Fair Credit Reporting Act (FCRA) and other laws and rules. It is within

this one area that the investigation agency can perform a valuable service, that is, make sure the employer does not go astray.

Some employers will want verifications to be made in depth; other employers will not. Some employers will be willing to pay more to make sure they filter out the bad actors; some employers will be willing only to pay the rock-bottom price. Depth refers to how far back in time the employer will want to go and in looking for misdemeanors as well as felonies. It also means checking out "also-known-as" names and maiden names.

Persons applying for positions of trust and responsibility should be checked out thoroughly. An employer may specify that an applicant for the Manager of Accounting position be screened to a certain level and that the applicant for the Chief Financial Officer be screened at a much higher level. In any of these cases, an applicant's personal credit should be of particular interest.

An employer's policy may be to allow appeals that go beyond the FCRA rules such as to hold formal hearings so that the turned-down applicant can rebut findings or present explanations. If the private investigation agency has done its job properly, there should be no error that could be a foundation for an appeal.

A preemployment screen should address at least three issues:

- The credentials of the applicant: Does the applicant have the skill, knowledge, and attitude demanded by the job sought?
- The identity of the applicant: Is the applicant using a false name, perhaps to conceal a dishonest past?
- The personal history of the applicant: What has the applicant done in the past that could affect his or her job performance if hired?

The first issue is almost always resolved by a human resources specialist or the person who would supervise the applicant if hired. The PI has little to do with making these determinations.

The second and third issues, however, are in the purview of the investigator. The verification process used by the investigator must be able to answer two questions: Is the applicant really the person listed on the employment application? Has the applicant really done the things he or she listed on the application? For example, education attainment and job experience.

Although the investigator may have no role in judging an applicant's job qualifications, the investigator should understand the nature of the open position and be aware of such matters as visibility of the position, credibility of the incumbent, industry-specific expectations such as membership in trade associations. Having a handle on these matters can help the investigator craft a meaningful report.

The Background Inquiry

The BI is a follow-on inquiry to a preemployment screen when there is reason to believe the job applicant is lying. Usually, the BI is justified when the position to be filled is an important position.

A BI is a search for information about a person; the search does not seek to prove or disprove, only to bring relevant information to the surface so that an objective judgment can be made. The investigator dredges up the relevant information; the employer makes the final, objective judgment.

Employers and other persons who want BIs conducted are not necessarily seeking information about a job applicant. In this respect, the requesters vary widely because their motives vary widely, for example:

- A defense attorney wants background information about the defendant, key witnesses for both sides, the personal biases of a presiding judge, and the out-of-court personalities of jury members.
- A plaintiff's attorney wants the same information.
- An attorney wants to know the opposing attorney's history of courtroom strategy and tactics.
- A mother wants to know the background of a babysitter, nanny, or child care center.
- A businessman wants to know if his partner or chief accountant is spending beyond his means.
- An office building owner wants information about a prospective renter.
- A celebrity wants background information about a bodyguard, gardener, and housemaid.
- An investor wants background information on a broker and a company that appears susceptible to a takeover.
- A spouse or significant other wants to know if his or her partner is cheating.

Use of Private Investigators

PIs routinely provide preemployment screening services to businesses. The PI's usual point of contact is the owner or operator of the company or the company's manager of the human resources department.

The search for information follows the same course: the requested information is gathered and presented to the employer, and the employer makes the call. An employer can be in the private or public sector, i.e., operate a business or a government organization. When the employer operates a business, the PI and the employer usually have a direct relationship. When the employer is a government organization, the direct relationship usually is between the PI and a group under contract to the government.

Some employers screen applicants using in-house resources; some do not. In the latter category, the employer engages the services of a third party such as a private investigation agency specializing in the service. The employer's rationale in going outside of the company is usually twofold: less cost and better results. Preemployment screening done in-house resides in the human resources department most of the time, and the screening work requires one or more dedicated employees, work space, equipment, office supplies, and so forth. The cost of maintaining an in-house preemployment screening program can be quite high, yet the effectiveness of the program can be quite low. Human resource representatives are simply not skilled at conducting investigations. Hence, the employer turns to investigation professionals.

A private investigation agency interested in performing preemployment screening on behalf of an employer would be well served to:

- Gain an understanding of the employer's enterprise such as its operations, equipment, core business functions, administrative processes, hours of operation, products produced or services rendered, number of employees, types of jobs performed, employers, environmental issues, organizational culture and compliance with safety and security rules.
- Identify the assets of the organization that are at risk.
- Consider all the potential costs, direct and indirect, financial, psychological, and other hidden or less obvious ways in which a poor hiring decision can impact the enterprise.
- Estimate the probability that an adverse event related to a poor hiring decision may occur in the future.
- Configure a preemployment screening program that fits the unique needs of the employer.
- Demonstrate with hard figures the benefits to be derived versus the costs to be experienced.

Prior to receiving a Consumer Report from a private investigation agency, the employer must certify to the FCRA in writing that it will:

- Use the information for employment purposes only.
- Not use the information in violation of any federal or state equal employment opportunity law.
- Obtain all the necessary disclosures and consents as required by the FCRA.
- Give the appropriate notices in the event an adverse action is taken against an applicant based in whole or in part on the contents of the Consumer Report.
- Give the reason why a Consumer Report needs to be expanded to an Investigative Consumer Report when such is the case.

Before hiring a private investigation agency to conduct a preemployment inquiry, the employer must inform the applicant in writing of the intent to do so. If the applicant agrees to the inquiry, the employer must obtain the applicant's written consent. The disclosure and the consent can be separate documents or be combined in a single document. They must not contain extraneous information and must not be part of another document such as an employment application form.

When a private investigation agency informs the employer that the preemployment inquiry disclosed inconsistencies or facts of a suspicious nature, the employer can choose to expand the inquiry. In this case, the employer must use a second (and different) disclosure form to advise the applicant in writing of the decision to expand the inquiry. If the applicant agrees, his or her written consent must be obtained. If the inquiry goes forward, an Investigative Consumer Report is given to the employer at the conclusion of the inquiry.

Adverse Action

When a private investigation agency submits to the employer a Consumer Report or Investigative Consumer Report containing information of a disqualifying nature, the employer can choose to ignore the information or accept it. If accepted, the employer must issue a Notice of Preadverse Action. The notice states the intent of (not the fact of) the employer not to hire the individual. The notice is sent to the individual, along with a copy of the Consumer Report or Investigative Consumer Report. A Federal Trade Commission (FTC) document called "A Summary of Your Rights Under the Fair Credit Reporting Act" is sent with the Notice of Preadverse Action.

The employer must allow a reasonable period of time for the applicant to respond. When that period of time has passed absent a response, the employer is free to issue a Notice of Adverse Action. The notice is effectively saying that the individual's application for employment has been denied. When sent, the notice must be accompanied by another copy of the FTC document called "A Summary of Your Rights Under the Fair Credit Reporting Act."

As already stated, a copy of the Consumer Report or Investigative Consumer Report must accompany the Notice of Preadverse Action sent to the applicant. The notice must include the name, address, and phone number of the private investigation company that conducted the investigation. The notice must clearly state that the private investigation company had no part in making the decision not to hire the individual.

Because Consumer Reports and Investigative Consumer Reports contain private and sometimes highly sensitive information, it is obligatory upon the

private investigation agency to protect its files with stringently enforced policies and practices that include password-protected electronic data, locked-container storage, and controlled access to the premises.

PIs need to be familiar with the following:

- Drivers Privacy Protection Act requires driving license information be protected against unauthorized disclosure.
- The GLBA protects customers' nonpublic personal financial information held by banks and other financial institutions. The Act requires such entities to protect customer information, and the protection extends to Consumer Reporting Agencies (CRAs) such as private investigation agencies.
- Health Insurance Portability and Accountability Act (HIPAA) requires protection of certain health information. Punishment for violations can be serious.
- Various state laws that demand protection of worker compensation files, sealed or expunged court records, juvenile crime records, and others.

The FCRA prohibits private investigation agencies from including certain types of criminal information in their reports to employers. Strangely, some prohibitions concerning information acquisition apply to PIs but not to employers who conduct their own preemployment inquiries.

It is well known that the criminal justice system is in disrepair generally. There are many reasons for this, but the central point is the possibility records are inaccurate, not on file, or were mistakenly destroyed. The available information may be unreliable or could have been assigned a classification that allows release when such should not be the case. A PI who includes such information in a report to an employer may violate the FCRA.

While there are numerous statutes, laws, and regulations that dictate how preemployment inquiries should be conducted and what information should be released, employers must be reasonable in how they collect and use the information. Private investigation agencies that want to keep their clients out of trouble should carefully craft their reports to ensure that information given to their clients do not violate the many and various rules concerning what employers can and cannot use in making hiring decisions. While it is true that a private investigation agency can take the position that it is simply a data conduit and it is the employer's duty to use the information properly, the employer may not agree with that view.

It is also important that the private investigation agency not provide information obtained from questionable sources. Search engines do not always contain accurate information. There is always the possibility that Jeremiah

Jenkins, whose name appears on an Internet list of child molesters, is not the same Jeremiah Jenkins seeking the job in question. Keep in mind that a job applicant could be falsely and deliberately maligned on the Internet.

Although it may be argued that anything on the Internet is public, use of the information may invade privacy. An interesting twist on this issue is that an employer does not need to issue an Adverse Action Letter nor even explain why a job applicant was rejected when the disqualifying information was taken off the Internet.

EMPLOYEE RELEASE

Before the checking process can begin, the applicant must sign a release. A sample release form is depicted in Fig. 14.1. The release can be part of the employment application form or a standalone document. A release protects the employer and gives fair warning to the applicant. When asked to sign a release, an undesirable applicant is inclined to withdraw the application and look elsewhere for employment. Following is an example of the wording in a release: "I hereby authorize the ABCD Company, or their agents, to make inquiries of my background and to obtain, examine, and/or make copies of any and all records or reports pertaining to my employment, credit and financial status, criminal record, military record, education and training records, driving record, insurance records, business and personal references, and representations made by me in connection with my application for employment."

Some employers will accept online employment applications. However, preemployment tests, interviews to clarify points, and interviews by prospective supervisors require the applicant to appear in person with picture

AUTHORIZATION TO RELEASE INFORMATION

This release hereby authorizes _____, or his/her agents, to make inquiries of my background and to examine and/or make copies of any and all records or reports pertaining to my employment, credit and financial status, criminal record, military record, education and training records, driving record, insurance records, and business and personal references.

Printed Name of Individual Authorizing Release:_____

Signature of Individual: _____

Date: _____

FIGURE 14.1
Before starting to make a preemployment background inquiry, a form of this type needs to be signed by the applicant.

identification. An employment application made in any manner can fall into the "not considered at this time" category when a job vacancy does not exist.

REFERENCE CHECKS

Keep in mind, it is the applicant who provides employment and personal references, and people identified as references can be expected to answer glowingly when queried. Checking references by mail or e-mail is not as effective as checking in person or by phone. People tend to be candid in face-to-face and voice-to-voice situations. Facial expressions, pregnant pauses, and voice inflections can reveal a great deal. San et al. (1994) say that more can be learned from the manner of response than the content of it. Verbally asking "Would you rehire this employee?" is potentially more revealing than a form letter that comes back with a check mark in a box.

Interviewing Knowledgeable Persons

A first step in this method is to identify people who are likely to know the applicant and likely to be candid. Such persons can be present and former coworkers, neighbors, and police officers who may be aware of integrity issues not reflected in police or court records. Another good source can be the Chief Security Officer (CSO) of a company that previously employed the applicant.

It is helpful to corroborate negative information. If the applicant claims in a resume that he or she headed up a certain work project but a coworker says otherwise, the PI needs to corroborate that negative piece of information one way or the other. Note in this example that the issue was put forward by the applicant, i.e., that he or she headed up a project. The PI's function is to verify the truthfulness of that claim. If the claim is found by one inquiry to be untruthful, the investigator is obligated to check further, either to substantiate or refute.

At the opening moment of an interview, the PI must explain to the interviewee that any questions asked relates to a job application and that the sole reason for the interview is to verify information provided by the applicant.

Interviewing Techniques

The purpose of an interview is to prove or disprove suspicious entries in the job application. Opinions and value judgments are not proof or nonproof in nature, and for that reason, they do not belong in an inquiry report. Questions that begin with, "Do you believe. . ." or "Is there a chance that. . ." are the questions that prompt judgmental responses.

Negative questions also must be avoided; for example, "Do you know if Sandra ever shoplifted?" A question should be such that the answer is expected to be positive. If, however, the interviewee offers a piece of negative information without prompting, the investigator has to pursue it. Follow-up questions might be:

- "How long have you known Sandra?"
- "What is your relationship with her?"
- "Did you really see her shoplift?"
- "To the best of your knowledge, what stores did Sandra shoplift from?"
- "To the best of your knowledge, how many times did Sandra shoplift?"
- "Did she show you anything that she shoplifted?"
- "Did she ever offer to sell you shoplifted items?"
- "Who else would know about this matter?"

The truthfulness of the interviewee becomes an issue when negative information is offered. Does the interviewee have an axe to grind? Does the body language of the interviewee suggest animosity? Through skillful questioning, the investigator can put down on paper what the interviewee is saying with body gestures, eye movements, and voice inflections.

Remember that the purpose of the interview should focus on the suspicious information.

RECORDS OF INTEREST

Municipal Records

Police stations and city or town halls can be rich sources of public records. In most cases, the PI needs only appear and state the purpose of the visit. A clerk will either hand over a copy of the record or give instruction in where to look and how to retrieve the record wanted.

The municipality is very likely to keep records that identify residents. Often there is a list of voting-age residents and the streets where they live. These records are usually recorded in a "book" that provides, in addition to names, a delineation of wards or precincts, which can aid the investigator in locating the street of interest.

In addition, the "book" may identify all the people living on a street. But be careful because people tend to move without notice, making this portion of the "book" less than accurate.

Names of companies and company officers are usually on file, sometimes with addresses and phone numbers.

Some records on file, possibly for public safety reasons, will include notes that describe a person's tendency toward violence, eccentricities, and peculiarities.

"Doing business as" (DBA) records might be filed in a municipality or a county or both. They can be informative because the subject may not have wanted to register his or her company as a corporation, possibly to hide the true activities of the business, its assets, and its liabilities. When DBA and separate records contain different information, the investigator may be on to something.

Patience and curiosity are essential. Record offices vary from municipality to municipality. The investigator will need to take time familiarizing, looking, and asking questions. The counter clerk is unlikely to know all that the office contains, but when the roaming investigator spots a particular record, the clerk will usually be helpful in providing a copy.

County Records

Public agencies and private industry data banks are two main sources of records. Public agency records reside with law enforcement agencies, criminal and civil courts, licensing bureaus, the military, social security administration, and others.

Records that are generally available include the following:

- Criminal records.
- Lawsuits and judgments.
- DBA files.
- Divorce and marriage records.
- Property tax records, deeds, and mortgages.
- Uniform Commercial Code (UCC) liens and secured transactions.
- Voter registration files.
- Estate records and bankruptcy filings.
- Permits and inspection files.
- Motor vehicle registration files.

A voter registration record can be particularly helpful. It includes full name, current and former addresses, and other details. Information on a voter registration record may reflect data different than that provided by the applicant and also help the PI track the applicant's history through other records.

The Registry of Deeds lists people who own properties. A subject may own property that is required to have a deed on file. If the subject's present location is not known, information on the deed and its allied documents may be of help such as where tax bills are mailed. In addition, the nature of the

property registered can give a hint as to the subject's location. For example, if the deeded property is a yacht or a condo in Aspen, the investigator has places to look.

The Assessor's Office should not be ignored. It will contain a listing of property owners, the property owned, the assessed value, the payment or nonpayment of taxes, and the address of the owner.

If the taxed property, for example, is a truck, the investigator can assume that the subject is in the trucking business. From there, the investigator has another lead: chauffeur license issued by the Department of Transportation.

State Records

Records at state level are less in number but can be helpful in making a thorough check:

- Corporation filings.
- Workers' compensation claims.
- Professional licensing files.
- Driving license files.

Uniform Commercial Code

When an applicant pledges collateral on a loan, UCC filings tell you whether others have filed a claim against the same collateral.

The three major credit bureaus contain up-to-date UCC records filed with the Secretary of State. The UCC online search delivers the following:

- File number.
- Debtor's name and address.
- Secured parties' names and addresses.
- Collateral description (e.g., equipment, real estate, inventory).
- Amendments, terminations, and continuations.

Not all information may be available for all businesses. Some successful UCC searches may generate reports with no data at all. Even still, a report may contain useful information from computer databases. Some databases are easily accessible to the PI directly; in other cases, the PI works through a vendor.

DATABASE SEARCHES

Database searches can provide extensive information at low cost and are useful when the person of interest worked or lived in numerous counties or

states. A local search, such as one made at a county courthouse, will not reflect an individual's criminal conviction in another county or state. Success with a database service will depend on the quality and quantity of the identifying data provided by the employer. For each name run through a database, there may be hundreds of persons with the same name. Full and accurate information inputted at the front end can produce good information at the back end.

Not all records, however, are computerized or accessible by electronic means. For this reason, the investigator will have to go to the places where the records of interest are physically stored. Examples of record-storing places are state houses, county courthouses, and driving license offices.

Record checking might consist entirely of searching records in computer databases. Operating from a PC, the investigator enters the Internet and navigates to Web sites that contain pertinent databases. By downloading or cutting and pasting, the searcher is able to extract information. Results can be forwarded to the employer within hours through e-mail or fax.

Cost Avoidance

Cost-avoiding advantages can derive from preemployment screening. For example:

- Applicants who are felons, violence-prone individuals, drug abusers, and pose safety risks can be denied employment, thus reducing costs associated with theft, injury, accidents, and medical assistance benefits.
- Applicants with skills and knowledge that correspond to vacancies can be filtered in, thus reducing costs associated with training.
- Applicants who demonstrate the potential for long-term commitment can be filtered in, thus reducing costs associated with turnover.

Fair Credit Reporting Act

The FTC is mandated by the FCRA to ensure the accuracy and privacy of information used in consumer reports. A consumer report is information about a consumer that is sold to creditors, employers, insurers, and other businesses. A consumer report contains details as to where the consumer worked and lived, how bills and debts were paid, bankruptcy filings, criminal history, and civil actions. Companies that gather and sell this information are called CRAs. The most common type of CRA is a credit bureau.

Credit Information

Where fiscal responsibility is an issue, the employer may want to gather credit information about:

- Debt load.
- Payment history.
- Garnishments.
- Liens.
- Bankruptcies.

Consumer Report

Under the FCRA, a consumer has a right to obtain a copy of his or her consumer report. In addition, anyone who takes action against a consumer in response to a report supplied by a CRA, such as denying an application for credit, insurance, or employment, must give the consumer the name, address, and telephone number of the CRA that provided the report. The CRA also must provide a list of everyone who has requested the report within the past year. For employment-related requests, the time period is 2 years.

An employer or prospective employer cannot obtain or seek information from a CRA without the job applicant's specific consent. The same holds true for medical information requested by an employer, creditor, or insurer.

Investigative Consumer Report

A type of consumer report is an investigative consumer report, a detailed file containing interviews with the consumer's neighbors or acquaintances concerning lifestyle, character, and reputation. The investigative consumer report may be used in connection with insurance and employment applications. The FCRA requires that the consumer be notified in writing when such a report is ordered.

Negative Information

Negative information in a CRA file has to be purged at the end of 7 years unless the information pertains to the following:

- A criminal conviction.
- A bankruptcy action, in which case the purge is made after 10 years.
- An application for a job with a salary of more than $75,000.
- An application for more than $150,000 worth of credit or life insurance.
- A lawsuit or an unpaid judgment (when a statute of limitation applies, the information can remain on file until the limitation runs out).

Only people with a legitimate business need, as recognized by the FCRA, can obtain a consumer report.

Credit Application

If a consumer's credit application is turned down, the consumer can demand to know why. Another law, the Equal Credit Opportunity Act, requires the creditor to specify the reason the application was denied. In many cases, the reason will be that the consumer had no credit file or had a credit file reflecting delinquent obligations.

A consumer may sue in state or federal court for most violations of the FCRA. If the consumer wins, the defendant has to pay damages and reimburse for attorney fees to the extent ordered by the court. Credit reports can also be used to corroborate information already acquired, such as previous addresses and prior employers cited by the individual.

Local Records

Police stations, city halls, and county courthouses are rich sources of public records. In most cases, the person making the inquiry need only appear and state the purpose of the visit. The inquirer will be given a copy of the record (at reasonable cost for the copying service) or be told how to search for the record such as operating a microfiche machine or computer terminal.

The result of the records check should be recorded on a form to be used by the person making the hiring decision and then placed on file. A sample form is shown in Fig. 14.2.

FREEDOM OF INFORMATION ACT (FOIA)

All federal agencies are required under the FOIA to disclose records requested in writing by any person. However, agencies may withhold information pursuant to nine exemptions and three exclusions contained in the statute. The FOIA applies only to federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies. Accessible records include the following:

- Defense Locator Service (military records).
- Veterans Administration.
- Social Security Administration.
- Federal Bureau of Investigation.

REPORT OF CRIMINAL RECORDS CHECK

Name of Person: _____

Aliases: _____

Date of Birth: _____

SSN: _____

Address: _____

_____

Records of the _____ County Criminal Court, covering the period _____ were checked and the following findings are reported:

_____ No record was found.

_____ A record was found and the following information noted.

Name As Shown on the Record: _____

Date of Birth: _____

SSN: _____

Addresses: _____

_____

_____

Docket Number: _____

Date of Arrest: _____

Charges: _____

_____

_____

Disposition: _____

_____

Name of Person Submitting Report: _____

Name of Reporting Agency: _____

Date of Report: _____

FIGURE 14.2

Many variations of this form are in use but the purpose is identical: the form is used by an employer's representative when considering the hire of an applicant.

PRIVACY ACT OF 1974

The Privacy Act of 1974 protects certain federal government records pertaining to individuals. In general, the Privacy Act prohibits the unauthorized disclosure of the records it protects. It also gives individuals the right to review records about themselves, to find out if these records have been disclosed, and to request corrections or amendments of these records unless the records are legally exempt.

The purpose of the FOIA and the Privacy Act is to give the public access to existing government records. These records include consumer complaints, investigations, and administrative records.

THE GRAMM–LEACH–BLILEY ACT

The GLBA protects customers' nonpublic personal financial information held by banks and other financial institutions. The Act requires such entities to protect customer information, and it extends to CRAs. The Act addresses the practice of collecting personal information under false pretenses. Pretexters pose as authority figures (law enforcement agents, social workers, potential employers, etc.) and manufacture seductive stories, such as the victim is about to receive a sweepstakes award or insurance payment, in order to elicit personal information about the victim.

The GLBA says that pretexting is illegal and punishable. However, the Act addresses pretexting only as it pertains to acquiring financial information from consumers or financial institutions. On the other hand, when a person engages in "deception," the FTC can step in. The FTC is mandated by Congress to ensure that consumers are not victimized by unfair or deceptive business practices.

The GLBA regards pretexting as an attempt, whether successful or unsuccessful, to gain access to personal nonpublic information using impersonation. It does not matter if the impersonation is done face-to-face, over the phone, by mail, e-mail, or phishing (using a phony Web site to elicit information).

Although pretexting is addressed in the GLBA, the original and main purposes were to take action against information brokering, telemarketing fraud operations, deceptive spam and Internet scam practices, bogus advance-fee credit card offers, and identity theft.

Because much information about consumers is a matter of public record, there is no need for pretexting. Numerous open sources, such as databases and courthouse records, can provide meaningful facts such as criminal

convictions, civil suits, bankruptcy, unpaid taxes and loans, and home ownership.

The language of the law relied upon by the FTC to enforce the GLBA states, "Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect. . ."

Apart from the GLBA, it is a violation to obtain customer information by using the following:

- False, fictitious, or fraudulent statements or documents.
- Forged, counterfeit, lost, or stolen documents.
- Using another person to do the above.

Insurance companies and law enforcement agencies performing official duties, and court agencies collecting child support judgments, are exempt.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA requires protection of certain health information. Punishment for violations can be serious. Various state laws demand protection of worker compensation files, sealed or expunged court records, juvenile crime records, and others. A person whose information privacy rights have been violated can lodge a civil complaint within 2 years following his or her discovery of the violation. However, civil action is barred if the discovery is made after 5 years following the date of the violation.

APPLICANT TESTING

Drug and Alcohol Tests

Testing for the use of illegal drugs and the abuse of alcohol is widely used to screen job applicants. The most common method of drug testing is the analysis of urine. For alcohol, it is a blood–alcohol concentration test. In both cases, the applicant is asked to submit to testing. A signed consent form demonstrates the applicant's permission. If the applicant declines to consent or refuses to take or cooperate in the administration of the test, the application process ends for that job seeker.

FIGURE 14.3
The procedure in testing urine samples for the presence of illegal drugs moves through a two-step process. *From iStockphotos.*

Testing for illegal drugs and alcohol abuse follows a two-step process. The first step is a test called a screen; the second test is called a confirmatory test. If nothing is found in the screen, the confirmatory test is not necessary: the applicant has passed the test. If something is found, the specimen is tested a second time using a more-exacting technique. If the second test fails to confirm the screen, the applicant has passed the test. If the second test confirms the first test, the specimen is declared positive: the applicant has not passed the test. Fig. 14.3 is representative of a step in the analysis of a urine sample.

The employer in almost every case will decline to hire an applicant who cannot pass a drug or alcohol test. Some employers will suspend the application for a period of time and allow the applicant to go through the testing process a second time. A drug or alcohol test, unlike a paper-and-pencil test, can be the sole criterion for rejecting an applicant.

Paper-and-Pencil Tests

In a general context, testing methods in organizational settings fall into one of three categories: selection, classification, and intelligence. A selection test

simply helps a decision maker accept or reject a job candidate. A classification test, which is much more complex to administer and interpret, helps the organization decide if the candidate fits the criteria of a job. An intelligence test is often constructed for use by a single organization specifically. It may measure, for example, an applicant's knowledge of concepts related to the job or the applicant's potential to learn and intellectually grow in the job. Within these general categories are tests of a more specific nature.

Achievement Tests

Achievement tests assess current performance in a knowledge area. Theory holds that achievement is both an indicator of prior learning and of future success. An achievement test typically measures vocabulary, language competency, reading comprehension, arithmetic computation, and problem solving. To the extent that the competencies tested are essential to job performance, the achievement test is suitable.

Aptitude Tests

An aptitude test predicts future performance in an area in which the applicant is not currently trained. Employers often use aptitude tests when filling specific vacancies. A variation of aptitude testing helps clarify an employee's career goals. Another variation examines a broad range of skills pertinent to many different jobs. An example is the General Aptitude Test Battery, which assesses general reasoning ability, perception, motor coordination, finger and manual dexterity, and other attributes.

Intelligence Tests

A variety of intelligence tests measure specific proficiencies and/or the capacity of an individual to cope with life generally. The test scores, known as intelligence quotients, reflect the individual's position in comparison to a representative group of people of the same age. Primarily, standardized IQ tests are administered by psychologists or other trained professionals. A CSO should not expect that just anyone in an HR department can administer these tests to potential applicants. The CSO should also weigh the cost of having an outside consultant administer tests with the benefit of finding a qualified employee.

Interest Inventories

An interest inventory is a questionnaire in which the applicant chooses personal preferences from among a variety of activities. The questionnaire, for

example, may ask the job candidate if he or she would prefer to march at the head of a parade, in the middle, or watch the parade from the sidelines. The applicant's answer, when considered with answers to other questions, may give the employer a sense of the applicant's capacity for and attitude about leadership. Other attitudes, such as respect for property, are similarly measured. The attitudes reflected on the questionnaire generally reflect the expectations of the employer.

Interest inventories, while not predictive of job performance, can provide general insights. An applicant whose inventory reflects a penchant for dishonesty would not be the best choice for a cash-handling job.

Objective Personality Tests

These tests measure social and emotional adjustment. Items that describe feelings, attitudes, and behaviors are placed into groups, each representing a separate personality or style, such as extroversion or introversion. Taken together, the groups provide a profile of the personality as a whole. One of the most popular tests of this type is the Minnesota Multiphasic Personality Inventory (MMPI). Again, the MMPI is administered by psychologists or other trained mental health professionals.

Test Validity

The overall value of a preemployment test is the assistance it gives for making reasonable predictions about a job applicant's likely behavior in specific situations. When a test proves to be an accurate predictor, it is said to possess validity. For validity to be demonstrated, the test must yield consistent, reliable measurements.

Problems in Design and Interpretation

Challenges to preemployment tests are made for many reasons, some good, some not so good. Challenges sometimes mention complaints such as the words were too technical, the instructions were unclear, the test administrator did not like me, my pencil broke, and so forth.

Behind the complaints may be genuine problems: poor test design and poor interpretation of test results. Both issues are related to human error, and human error is never easily overcome. Because these testing deficiencies exist and because they impact the lives of the test takers, employers are cautioned not to base their hiring decisions solely on tests.

CRITICAL THINKING EXERCISE

Barry Coleman, CSO at Lithicol (a large chemical company), had seen his department shrink from 15 to 2 employees in less than a year. His only consolation was that similar trimming had occurred in other departments. The information technology (IT) department had been hardest hit. Nearly every technical function in the IT department had been turned over to Security Staffing International, an outside contractor.

In addition to seeing many new faces in the workplace, Barry began to see many new reports of theft, particularly of desktop PCs. In every case, one or more Security Staffing employees were among the suspects. A witness told him, "Look, these Security Staffing employees have free rein of the building. It is in the nature of their jobs to be always moving around, sometimes carrying PCs to offsite repair labs. There's no way to keep track. Another thing: the Security Staffing group faces change almost daily. Lithicol doesn't pay enough to Security Staffing to be able to keep good employees around for the long haul. At least half of the Security Staffing employees at any given time are looking for better opportunities elsewhere. Somebody quits without notice on Friday. On Saturday, the Security Staffing human services people are on the telephone desperately searching for a replacement. Come Monday, a replacement shows up for work, a warm body with no real talent. I hate to say it but that's how I was hired. They called me, and I was a complete stranger to them. I went to work at Lithicol the next day."

In one particular theft, Barry narrowed the suspect list to a single individual, Richard Johnson, a former Security Staffing employee. Johnson's last day at Lithicol happened to be the day of the theft. Barry called Security Staffing's human services director and learned that Johnson had not been a Security Staffing employee at all but an independent subcontractor who took odd jobs here and there. The human services director did not know where Johnson was currently working or where he had worked previously. Barry asked for Johnson's home address and telephone number but the human services director refused, saying, "It is against our policy to provide that kind of information."

Knowing that a door had been slammed in his face, Barry obtained a copy of the agreement between Lithicol and Security Staffing. It stated that in assigning employees and subcontractors to the Lithicol workplace Security Staffing was obligated to "exercise a degree of care equal to that exercised in Lithicol's hiring practices."

Barry went to Henry Tisch, the Lithicol executive who managed the Security Staffing contract. Barry cited the rise in theft accompanying the outsourcing arrangement, Security Staffing's apparently nonexistent background screening practices, and the refusal of Security Staffing's human services director to cooperate. Tisch told Barry he'd check into it.

A week later, Barry was summoned to Tisch's office. "The good news," Tisch said, "is that the Security Staffing human services department is willing to provide the information you wanted about Richard Johnson. The not-so-good news is that they firmly believe they are meeting their contractual obligation to exercise hiring practices at least equal to our own. Equal, they say, does not mean identical. They say that if they were forced to do exactly what Lithicol does, they would not be able to meet work deadlines imposed on them, with the imposer being me. On that point, I have to agree. I do, in fact, hold their feet to the fire on getting X amount of work performed in X amount of time." A look on Tisch's face told Barry that the X amount of work was not up to expected standards.

Tisch concluded the meeting by saying, "The biggest and most important task before me is to ensure the success of the Security Staffing outsourcing project. The CEO has committed to making it work. I simply cannot jeopardize the project by coming down hard on this preemployment screening issue. Also, from a purely business standpoint, the cost of the thefts is very minor compared to potential losses in productivity that might result if Security Staffing is pushed too hard."

What do you think Tisch should do now, if anything? What is the most basic information a company should know about a potential employee? What are some potential compromises between staffing needs and quality of employees hired?

REVIEW QUESTIONS

1. Why would a company engage in preemployment screening?
2. In what way can preemployment screening reduce company costs?
3. Give an example of negligent hiring.
4. What is an investigative consumer report?
5. List three sources you might consult for information about a potential employee.
6. What is pretexting?
7. Define *respondeat superior* and give an example of it.
8. In drug testing, what is a confirmatory test?

References

Capwell, R., 2007. Negligent hiring and due diligence. In: Fay, J.J. (Ed.), Encyclopedia of Security Management, second ed. Butterworth-Henemann, Boston, MA, pp. 232–235.

D'Addario, F.J., 1993. Preemployment screening. In: Fay, J.J. (Ed.), Encyclopedia of Security Management, first ed. Butterworth-Henemann, Boston, MA, pp. 560–563.

San, L., Tyska, L.A., Fennelly, L.J. (Eds.), 1994. Office and Office Building Security. second ed. Butterworth-Henemann, Boston, MA.

Tyska, L.A., Fennelly, L.J., 1998. 150 Things You Should Know About Security. Butterworth-Henemann, Boston, MA.

CHAPTER 15

Emergency Management

What You Will Learn

- How the emergency management process works.
- The difference between NIMS and ICS.
- The difference between probability and criticality.

INTRODUCTION

The proposition is well accepted that the organization's Chief Security Officer (CSO) is a key player in the management of emergency incidents. Even in the absence of indications that a serious incident is likely, now or later down the road, the CSO must anticipate the possibility, plan for it, prepare the security group to respond, and be ready to support overall response activities. Elements of the National Incident Management System (NIMS) and the Incident Control System (ICS) will be discussed as they apply to the private sector.

EMERGENCY MANAGEMENT PROCESS

Emergency management is the process of preparing for, mitigating, responding to, and recovering from an emergency. The emergency management function requires a master plan for all incidents that involve potential damage or destruction of critical assets such as sensitive data and IT equipment. Some of what is covered in this chapter is also repeated in the chapter dealing with the business continuity plan. Both have the same objective: protecting or removing from danger the functions that keep the organization operating.

Fennelly (2004) makes the point that a tested and workable emergency operating plan (EOP) must be updated quarterly or as needed by changing circumstances.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00015-3

Objectives

The overall objectives of emergency operations planning, according to Muus and Rabern, should be to

- Foster a systematic approach to emergency management.
- Support a capability for prompt coordinated response to emergencies and threats of all sizes simultaneously by all levels of the facility and corporate management.
- Provide an assured continuity of management and delivery of essential services for the duration of the emergency.
- Promote uniformity in principles, policies, concept of operations, and compatible departmental standard operating procedures that facilitate coordinated response.

Execution

Execution of the incident plans are coordinated and controlled by an Emergency Management Team (EMT). Many of the team members operate from an Emergency Control Center (ECC). Others operate from the emergency site. All members, regardless of location and function, feed information to the EMT. In this way, the EMT is better able to avoid duplication of on-site efforts, not miss activities that need to be addressed quickly, and concentrate on protecting the critical assets, which in all emergencies include people.

An important difference exists between ECC activities and activities performed on-site. EEC work is relatively safe and involves decision-making; on-site work involves danger and hands-on work. Persons working at the site of the emergency typically include the organization's general safety and hazardous material (Hazmat) personnel, maintenance staff, security officers, and fire wardens if the emergency is fire and requires rapid evacuation of employees.

A fully equipped ECC is typically located apart from the facility to be out of harm's way in order to perform its command and control functions. This approach is expensive because it means equipping the ECC with everything (and other things) that keeps business operations alive during a nonemergency situation. Duplicate equipment, utilities, and materials at the separated ECC can be quite expensive. Among the duplicated items are independent connections to utilities that provide basic electrical power, backup power, water, and sewage, air conditioning (not for comfort but for protection against smoke, noxious fumes, and airborne biological agents), sleeping accommodations, packaged food, and telecommunications.

A less costly option is placement of the ECC within a building within the facility, such as the executive offices building. This choice is often driven by reduced cost because the ECC can use utilities already in place, affect a speedy response, and save time.

The first option, of course, is to place the ECC well apart from the anticipated emergency site, even as far away as hundreds of miles. Such a distant location might be at a facility owned by a sister subsidiary, thus reducing costs associated with duplicating utilities. If this is the choice, transportation from the facility to the ECC will be necessary, as well as providing health and comfort supplies for employees sent there to perform the essential activities of business continuity.

Finally, and very importantly, is the course of action decided by the person directing the response. A good example of difference is the manner in which Rudy Giuliani directed the response to the 9/11 incident and the manner in which Ray Nagin directed the response to Katrina.

Again, dependent on the nature of the emergency, other notifications should be made, for example, to a public health agency when the emergency involves a bacterial agent, the municipal Hazmat team in the event of a chemical release, and a hospital triage team in the event of serious personal injuries.

Two last points need to be made. First, upon arrival of the fire department or departments, control of the emergency very likely will be handed over to the senior fire chief who will take over or assist ECC operations. This does not mean that members of the EMT can go home or that on-site responders can step aside. No, all of the organization's responders will continue to work but decisions and orders will be given by the outside agency. Second, radio communication must be on the same frequency with strict procedures as to priorities in sending and receiving messages. This was a valuable lesson learned from the 9/11 emergency.

Mitigation

Mitigation is a combination of measures taken in advance to minimize the consequences of an emergency incident. Mitigation measures vary: training people to respond, keeping at hand a variety of supplies and materials such as escape transportation, personal protective gear, first aid supplies and equipment, backup power, portable radios and lighting, and water and food. Mitigation can also mean protection in the form of fences and security lighting, sensors, guards, and weapons. Mitigation is important because it prepares the organization to resist the threat and reduce the consequences. As

FIGURE 15.1
Terrorist attacks against the United States can occur anywhere across the globe. *Author's personal file.*

depicted in Fig. 15.1, bombing a US military facility shows the results of a guarded facility that did not have sufficient mitigation measures in place.

Mitigation also includes measures taken during or in the immediate aftermath of an incident. The measures will vary: evacuation and shelter in place, triage and medical treatment, cleanup and repair of essential equipment, acquisition of temporary help, replacement of critical equipment damaged or destroyed, and movement to an alternate site. Mitigation is important because it is directed at helping people caught in a crisis and helping restore critical business functions as quickly as possible.

Anticipation

Judging the likelihood of an incident, predicting the nature of it, and assessing its probable impact reside at the center of risk management. Accurate prediction of specific scenarios is never possible. The CSO might anticipate that a hazardous chemical release is a possibility but cannot accurately predict the time, date, place, and manner of release. DePasquale (2007) says that the response protocols for such an event usually anticipate an industrial-level accident in which a container is punctured, resulting in a leak. However, a terrorist attack may result in more than a puncture leak; it may cause a massive rupture. The magnitude of the release would far outstrip the response protocols in place. The best that can be done is to abstract the anticipated incident in a general scenario that leaves room for a flexible response.

The anticipatory process is ongoing and often intuitive. In keeping abreast of bombing incidents around the world, the CSO may notice trends such as remote detonation of explosives packed in a parked vehicle or anthrax sent in the mail. Sources of information helpful to anticipate an incident might be found in the following:

- Magazines.
- Newspapers (such as Al Jazeera).
- The Internet, such as YouTube and similar websites.
- Literature that supports terrorism.
- Solicitations for funds to support organizations sympathetic to terrorism.
- Literature that denigrates American corporations.

A thoughtful evaluation can prompt the CSO to modify the organization's defense tactics; for example, instruct security officers to keep vehicles away from people-congested areas and train mail room employees to look for suspicious envelopes and packages.

Anticipation is also putting two and two together. The CSO in a lumber harvesting company should expect that the company's announcement of planned harvesting in a previously untouched forest will provoke reactions from militant environmental groups, and the CSO should expect fallout from terrorist groups when the company acts in a way that appears to be pro-Jewish. The possibilities can be numerous and subtle.

Preparation

The first step in preparing for an emergency event is planning, and the primary focus of planning is prevention of the undesirable incident. The secondary focus of planning is to reduce undesirable consequences when prevention does not succeed. These twin objectives cannot be achieved through the efforts of the CSO alone. Key contributions will come from many persons in and outside of the organization. Those persons will depend on the nature of the event; for example, the organization's property manager will be a key player in responding to a fire but not to a kidnaping.

By its very existence, an EOP expresses management's concern for its employees and property. The depth of that concern is demonstrated by management's commitment of resources such as manpower, funds, expertise, and materials. The elements of an EOP include the following:

- Assignment of responsibilities.
- Identification of likely incidents.
- Dedication of particular resources.
- Implementation of procedures.

Uzzell (1993) makes the point that no company can consider itself immune to emergencies and that no management is free of the responsibility of being prepared. Preparation provides for the protection of life and property and the containment of loss or damage. Being prepared is making sure the following:

- Duties are assigned to the right people.
- People are not given more duties than they can handle.
- Everyone understands what is expected of them and who is in charge.
- Persons in charge are not overburdened by having too many persons to supervise.
- Everyone knows his or her place in plan execution.
- Everyone knows whose orders to follow.
- Collected information is reported to the right people and in a timely fashion.
- Everyone knows and agrees with the objectives of the plan.

Procedures

The CSO is the principal author of some but not all plans and procedures. Those that unquestionably fall into the security domain are sabotage, kidnaping, civil disorder, workplace violence, and bomb threats. The CSO also may be a contributing author to plans and procedures that lie outside the exclusive realm of security. According to Federal Emergency Management Agency (FEMA), such incidents include the following:

- Chemical releases.
- Dam failure.
- Earthquake.
- Fire or wildfire.
- Flood.
- Hazardous material.
- Heat.
- Hurricane.
- Landslide.
- Nuclear power plant emergency.
- Terrorism.
- Thunderstorm.
- Tornado.
- Tsunami.
- Volcano.
- Winter storm.

Training

Training is another matter of importance specified in the plan. Classroom training, as shown in Fig. 15.2, is important in presenting knowledge but is less important than hands-on skill acquired through practice. The training program's curriculum should correspond to tasks assigned to plan responders. Developing and delivering incident plan training is not as difficult a project as one might suppose. The responders, after all, are professionals in their fields and not in need of training in the fundamentals. A counselor in a workplace violence plan does not need to be taught counseling, a negotiator in a kidnap plan does not need to be taught negotiating, and the CSO does not need to be taught the law on deadly force. The major focus of responder training is to ensure that the various response groups are all on the same sheet of music.

In the matter of violence in the workplace, the CSO has a double responsibility. First is to evacuate from the site of the violence anyone who may be hurt by it, and second is to seek assistance from local law enforcement, which upon arrival may take charge of the incident. The police might decide to summon a negotiating team or a Specialized Weapons and Tactics (SWAT) team, or both.

In a bombing incident, the local police should also be called, and if the incident appears to be genuine, the police will variously notify bomb experts from the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the US Secret Service, the FBI, and possibly an Army ordnance specialist.

Response

Response to an incident can take place all at once or in stages. Response to a fire is always immediate, whereas response to a hurricane may be done in

FIGURE 15.2
Effective response is not possible without training. *Istockphotos.*

stages. Fire does not arrive with advance warning and does not tolerate delay. A hurricane can be predicted, spotted, and tracked in terms of strength and direction of movement. A triggering mechanism of a fire plan is smoke or visible flame. Many response actions are undertaken simultaneously: the fire department is called, employees are instructed to evacuate, and an in-house fire brigade initiates a holding action until arrival of the fire department. A hurricane plan can have several triggering mechanisms linked to warning levels such as those issued by the US Weather Service. At a low warning level, the premises and valuable equipment may be physically strengthened; at a moderate level, nonessential employees might be sent home; at a high level, the premises might be attended by security officers and maintenance personnel; and at a dangerously high level, the premises might be abandoned.

A response is conditioned by the perceptions of senior managers and business owners. The cost of a response can exceed the value of the assets at risk. In circumstances influenced by religious beliefs, politics, and war, the perceived consequences of a response can rule out making any kind of response. Insurance plays a part as well. When the at-risk asset is people, the only acceptable option is a full and dedicated response.

External Support Agencies

In major emergencies, especially those that extend beyond the boundaries of the protected facility, external support organizations should be involved in relation to the nature of the emergency. This includes

- Law enforcement.
- Firefighting.
- Emergency medical agencies.
- Local hospitals.
- Local government agencies.
- American Red Cross.
- US Public Health.
- Community communications center.
- Civil defense.
- FEMA.
- Consultants and others on retainer.

Experience tells us, however, that representatives of external organizations are not able to attend every planning session. Special invitations should be extended when warranted. For example, the law enforcement representative should be urged to attend when a law enforcement issue is on the planning agenda. All should attend when mutual aid agreements are to be discussed.

The following entities also play various parts in responding to major emergencies. Members of these agencies may or may not be asked to join the planning team, but they are definitely coordinating points.

- Mayor or community administrator's office.
- National weather service.
- Public works department.
- Planning commission.
- Telephone companies.
- Power companies.
- Water plants.

Involving a large number of people and agencies can result in the following:

- Obtaining "buy-in" across the board and up and down the organization and within the local community.
- Apportioning tasks according to capabilities.
- Enhancing the visibility and stature of the planning effort.
- Providing a broad perspective to the planning team.

CRITICAL THINKING EXERCISE

Anita Fowler is the CSO of Hallen Air Tools, a company that manufactures avionic components for a new generation of Army helicopters. When the company decided to update the emergency operating plan, Anita was assigned a key role on the planning team. She pointed out to the team that the Army, which commissioned production of the avionic components, would certainly evaluate Hallen's EOP. At the same time, Anita noted that Harvey Schlicht, the company's chief financial officer, was vetoing certain critical security measures for reasons of economy. When Anita lodged opposing views, a consensus of the planning team agreed that Schlicht was right and that Anita should use existing in-house resources to meet the objectives of the EOP.

An Army inspection team subsequently tested the EOP with a tabletop exercise and a practice drill. The Army inspection team concluded that the EOP was flawed because it lacked the security measures that Schlicht had vetoed. Schlicht laid the blame on Anita because the flaws were related to the security group.

What do you think Anita should do? How should these flaws be addressed? What areas of support does Anita have to rely on? What lessons from previous chapters should affect Anita's decisions at this point?

DEALING WITH THE MEDIA

Sugar is to flies as a major emergency is to news agencies. Reporters from television, radio, and newspapers begin instantly to buzz around, asking questions, photographing, videotaping, and generally getting in the way of response efforts. The key responders, whose full attention is focused on the

emergency, cannot allow themselves to be distracted. Two characters in this scenario come to the fore: the Public Information Officer (PIO) and the CSO. The PIO dispenses the sugar while the CSO keeps the flies in a tight formation.

Priorities

The first priority is to deal with the crisis; the second is to communicate the facts; and both are done simultaneously. The public wants to know what is going on and what is being done about it. Business leaders are very aware of the public's interest and understandably wish to avoid the impression of placing profit above community interests, especially where public health and safety are concerned. When liability is a possible outcome, as would be the case when a worker is killed on the job, management tends to be overly circumspect. In addition to charges that may be brought in a criminal or civil court, the business may suffer public relations losses, fall out of favor politically, and face restrictions imposed by regulators and legislators responsive to the public mood.

Security Problems

Problems of a security nature can be anticipated in the postincident period.

- Curious persons may attempt to enter the scene before it is safe to do so.
- Criminal opportunists may attempt to steal property.
- Attempts by the media to obtain further information can disrupt cleanup and repair operations.
- Employees at the scene can unwittingly reveal sensitive information such as details that would disturb the public and/or damage the company's position in defending against liability.

The CSO, who is likely to be at the incident scene more than anyone else, will be a visible company official and therefore a potential source of information. The CSO's response to questions should refer the media to the PIO, a person trained to be sensitive to the needs of the media but at the same time careful about releasing details that could be harmful to the company's interests.

The quality of security support is examined, to the CSO's credit or discredit, at the conclusion of an emergency. In some form or fashion, the organization will assess the full situation from beginning to end and summarize the findings.

The CSO's job and reputation are at risk when security support functions are shown to have been inadequate.

Equipping Plan Responders

At this point, the writing of the plan has ended, at least for the moment. Now, it is time to equip and train the responders. Not all equipment needs to be issued in advance of the incident. Items of this nature are usually not essential for day-to-day operations. They are placed in locations that make them readily accessible to the users. Weapons, personal protection gear, sensors that "sniff" the air in search of chemical and biological agents, vehicles, portable lights, bolt cutters, special communications gear, and bull horns immediately come to mind. Keeping these items in storage also rules out loss or damage and facilitates periodic inspection such as lubricating weapons, checking the charge of fire extinguishers, and calibrating sensors. Equipment placed at the disposal of the CSO for issue or storage can include the following:

- Pistols, shotguns, ammunition, tasers, and stun guns.
- Vehicles.
- Flak vests, body shields, and mace.
- Helmets, clear face masks, and batons.
- Personal protective equipment and foul-weather gear.
- First aid supplies, defibrillator, and oxygen resuscitator.
- Bull horns, stretchers, stanchions, and yellow tape.
- Mobile communications center, handheld radios, and radio-equipped vehicles.
- Portable lighting, flashlights, and small tools.
- Water and food.

NATIONAL INCIDENT MANAGEMENT SYSTEM

The preceding discussions focused on the private sector. The Department of Homeland Security has developed a model for two sectors: government and private. Chertoff (2008), the author of NIMS, defines it as a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life and property and harm to the environment. The Department of Homeland Security, formerly led by Michael Chertoff, set a goal of bringing government agencies, public organizations, and private

businesses into alignment with the National Security Policy. That goal has not changed but a great deal remains to meet it.

NIMS works like a template to enable organizations to work together. The template can be used for dealing with all kinds of incidents, running the gamut from short-range occurrences at local levels to long-term incidents affecting the nation. NIMS is not an operational incident management or resource allocation plan. It is a core set of doctrines, concepts, principles, terminology, and organizational processes that enables effective, efficient, and collaborative incident management.

Preparedness

Ongoing preparedness efforts among all those involved in emergency management and incident response activities ensure coordination during times of crisis. Moreover, preparedness facilitates efficient and effective emergency management and incident response activities.

This cycle identifies specific steps that the EMT and responders from affiliated organizations should develop and incorporate into their overall preparedness programs and leverage their efforts within and outside the organization to the greatest extent possible.

INCIDENT COMMAND SYSTEM

A key part of the NIMS is the ICS, a program that prepares for and manages incidents at the scene. Unlike the NIMS, which is a conceptual program, the ICS is a hands-on program that determines response activities and implements them at the incident scene. It allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. The organization can vary widely such as a manufacturing plant, college campus, high-rise office complex, or government agency. The ICS enables a coordinated response among various public and private sector jurisdictions and functional agencies. It is flexible and can be used for incidents of any type, scope, and complexity. In addition to having dealt with the emergency through use of the ICS is postincident cleanup, as shown in Fig. 15.3.

A fundamental purpose of ICS is to enable incident managers to meet the urgent demands of an incident with cross-jurisdictional coordination and collaboration. The ICS approach is designed to:

- Meet the needs of incidents of any kind or size.
- Allow personnel from a variety of agencies to meld rapidly into a common management structure.

FIGURE 15.3
Cleanup efforts are only one part of aftermath efforts following a major emergency. *Istockphotos.*

- Provide logistical and administrative support to operational staff.
- Be cost-effective by avoiding duplication of efforts.

The ICS consists of procedures for controlling personnel, facilities, equipment, and communications. It is designed to be used from the time an incident occurs until it is under control. The plans and procedures developed by the CSO for the security group would do well to use the ICS as a primary source for developing a security group response program, and further, convincing management to incorporate the NIMS and the ICS into the company's EOP.

A basic premise of the ICS program is that all incidents begin and end locally. Although developed by the federal government, the program does not take command away from local authorities. It simply provides the framework to enhance the ability of responders to work together.

Coordination is critical when an incident requires response from multiple local emergency management and response agencies. The emergency responses made on September 11, 2001 demonstrated the need for such a program, hence creation of the NIMS and the ICS. When implemented properly, the ICS provides a flexible, yet standardized, mechanism for dealing with complex incidents, even those having national implications.

Copies of the NIMS and the ICS can be downloaded from Homeland Security Department websites using the Google search engine.

Mutual Aid and Assistance Agreements

Mutual aid and assistance agreements between agencies, organizations, and jurisdictions are highly recommended. These agreements provide a mechanism to quickly obtain emergency assistance in the form of personnel, equipment, materials, and other associated services. The primary objective is to facilitate rapid deployment of emergency support prior to, during, and after an incident.

BOMB INCIDENTS

The large number of disaster threats does not permit discussion of all threats. However, because of seriousness and frequency, we have arbitrarily selected bomb incidents, fire emergencies, medical emergencies, and natural disasters.

Bomb incidents are at the forefront of security concerns. The belief that terrorist-initiated bombing incidents might occur in the United States and its territories has been replaced by a certainty they will occur. The events of September 11, 2001 were extremely convincing in that regard. Devastation of the World Trade Center is shown in Fig. 15.4. Questions are raised by the expectation: When and where will terrorist attacks happen? Will the targets be physical assets or human assets? What tactics will be used and what terrorist groups will be involved?

Proactive Measures

An organization's program for managing bomb incidents includes proactive steps, such as:

- Coordinate with law enforcement agencies to learn the methods and operating locales of groups known to use bombs. Determine if the organization is a potential target.
- Stay current with new developments in bomb construction and concealment.
- Confer with security counterparts to learn the bomb incident experiences of other organizations. Set up information-sharing agreements.
- Liaise with bomb disposal experts who can be helpful in conducting training programs for employees whose duties would bring them into contact with bombs such as package or mail bombs.

FIGURE 15.4
The attack on the World Trade Center was not the first terrorist attack on U.S. soil, but certainly the most devastating. *Federal Emergency Management Agency.*

- Control suspect packages entering the workplace. Control can include examining packages in a separate building adjacent to the main workplace or at an off-site location.
- Identify strangers who enter the workplace, keep an eye on them, and prevent them from gaining uncontrolled movement within the workplace.
- Educate employees to look for and report strangers in the workplace and educate employees and visitors not to leave personal items, such as briefcases and gym bags, unattended in the public areas.
- Identify areas where a bomb could be planted with little chance of detection and where detonation would cause personal injury and interruption of operations. The areas to think about concerning

personal injury are lobby, cafeteria, work areas with high concentrations of people, and executive offices. Regarding interruption of operations, the places of concern are the telephone switching center, computer room, electrical power plant, and places where critical physical assets are located.

- Educate employees generally, and security and maintenance personnel specifically, to be alert for suspicious persons and activities.
- Require security officers during each tour of duty to make random checks of public areas to look for unauthorized persons who may be hiding or reconnoitering the facility.
- Ensure physical protection of key assets against bomb damage. Fire-resistant safes and vaults can protect sensitive documents, cash, small valuables, magnetic media, and similar materials.
- Educate fire wardens and other bomb incident responders to look for and report unusual activities that might signal the early stage of a bombing attempt.

Bomb Incident Management Program

A program to manage bomb incidents is similar to any other incident management program. It moves through three stages: develop a plan, prepare procedures that implement the plan, and train/equip persons who perform the procedures. The CSO, who is logically the principal developer of the program, identifies the following:

- Purpose and objectives.
- Major preventive, anticipatory, and response functions.
- Responsibilities for execution within the security group.
- Availability of and interfaces with outside response agencies.
- Equipment and training required.
- An approach for bringing various elements of the plan together to form a synchronous whole.

Bomb Incident Planning

The bomb incident plan should be sufficiently flexible to allow more than one response option at the outset and during the course of the incident. Because the plan commits to action a number of units and persons not employed by the security group, development of the plan will require the CSO to coordinate the plan with all interested parties—not least of which is the organization's emergency management office.

The interested parties inside the organization are likely to be the security officer force, building maintenance workers, and fire wardens. If the

organization is a tenant, the landlord or building management office will be involved in plan development and execution. Outside parties could include an explosives detection team, a bomb disposal team, fire control units, ambulance services, and postincident investigative agencies.

Strategy

A strategy takes into account the organization's exposure and vulnerability to a bomb attack. The CSO must obtain answers to the following questions:

- Is the organization a target of a militant adversary?
- Is the organization partnered in any way with an organization or government that is targeted? Will partnering include working with or providing products, materials, and assistance to another organization?
- Has the organization or its leaders contributed money to, provided support for, or been politically affiliated with any charity, aid program, cultural exchange, or educational program that could be construed as affiliated with a target of terrorism?
- Does the organization support political or social causes that would make it a likely target for radical hate groups?
- Has the organization refused to do business with, withdrawn from, or failed to successfully negotiate business contracts with companies, organizations, or governments that are affiliated with terrorist groups?
- Does the organization manufacture or produce military arms or equipment?
- Have any of the organization's leaders made public statements, been quoted or interviewed, or authored papers critical of terrorist groups?

Answers to the preceding questions can lead to further questions.

- Is the organization a target?
- What is the probability of an attack?
- Who are the likely attackers?
- What are the capabilities of the attackers?
- What will be the form and delivery method of the attack?
- Is the organization vulnerable to an attack?
- What are the organization's specific areas of vulnerability?

Now coming into play is the experience of the CSO and his or her ability to tap into valuable information sources: reports of government intelligence and law enforcement agencies, the expertise of consultants, the experiences of security peers, and the research capabilities of professional associations serving the security industry. Also helpful can be the findings of prior security inspections and surveys on file and the application of plain old common sense. News media stories also can serve as information sources.

As given in the determination of a strategy is the recognition that perfect security is impossible, no matter how much money and effort the organization may be willing to expend. The strategy will reflect a balance between cost and effectiveness. When the homework has been done, the CSO is able to calculate the increases and decreases of risk associated with proposed increases and decreases in security. For example, the installation of an electronic access control system has dollar costs that can be readily determined and placed into contrast with the reasonably estimated dollar costs of injury, death, property destruction, and loss of business opportunity that would result from a bomb explosion.

Bomb Incident Plan and Procedures

Although bomb incident plans vary widely among organizations, they typically contain the following:

- A statement reflecting management's concern about bomb incidents, support of the plan, and authority to expend resources needed for plan execution.
- The objectives of the plan. At least three objectives apply: provide for the safety of people, protect property against damage or destruction, and restore the organization to normal operations.
- A description of the threat and an assessment of risk.
- Definitions of terms important to understanding the plan and assigning accountability.
- A delineation of job positions and units, including external agencies, which have plan responsibilities. The delineation reflects lines of communication and formal authority.
- A description of the facility in terms of geography and demography, access routes, physical construction, entry points, utility interfaces, hours of operation, types of work activities, and numbers and types of persons within the facility.
- A description of the dedicated resources such as a security control center and public address system. This description could also mention evacuation routes and assembly areas.
- An identification of procedures that carry out the plan; for example, procedures used by
  - Maintenance personnel in shutting down utility systems.
  - Fire wardens in evacuating the facility.
  - Security officers in conducting bomb searches.

Procedures that flow from the plan provide detailed guidance to the responders. Procedures vary for the simple reason that responders vary. The CSO,

for example, develops procedures for security group responders, and the property manager develops procedures for maintenance employees.

Written procedures might be found smack dab in the middle of a plan or as an appendix at the end of the plan. Where they are located in the plan is less important than making them understandable to the people who carry them out. More than anything else, procedures are directives that leave no room for interpretation. This is so because the potential for severe consequences requires absolute clarity.

A plan can be tested partially or fully. A partial test might be a simulation exercise; for example, an unidentified caller has stated that a bomb has been concealed on the premises. The CSO orders that a search be made. Security officers conduct the search in accordance with the plan's procedures. Other security officers simulate notifying responders and communicating search findings. Practice of this type is hands-on training. Essential knowledge and skills are applied, and response equipment such as the public address system and radio communications system are put into use. Briefings and orientations for familiarizing the responders with the established procedures precede the exercise, and immediately following is a critique designed to improve future performance. Learning acquired in this manner is powerful and lasting.

The exercise is assessed objectively and an after-action report prepared. The response procedures, as well as the plan itself, are modified in light of lessons learned. But evaluation by the CSO does not end there. It takes place every day in the observation of security officers doing their jobs and of equipment operating in support of security. It is present when terrorist groups refine or alter their tactics and when bomb technology advances.

The Telephonic Bomb Threat

An elementary observation about bomb threats is that they are rarely made in person, sometimes conveyed in writing, typing, e-mail, and almost always made over the telephone. The bomber prefers the telephone, believing it presents the lowest risk of identification.

If the threat message has been written or typed, the document is handled carefully, touched by as few persons as possible, and the envelope and any other accompanying materials preserved as evidence. Observing these simple precautions will be extremely helpful to a postincident investigation.

If one is to assume that a bomb threat is real, it logically follows that the person communicating the threat has knowledge about the bomb. The immediate interest is in learning from the caller what the bomb is made of, where it has been placed, and when it will detonate. Knowing these facts can save lives.

Any bomb threat, hoax or real, has to be treated seriously and with great caution. In the American workplace, a very high percentage of bomb threats are hoaxes, but the other side of that reality tells us there is no way to be absolutely sure. Any bomb threat decision has to be heavily biased toward protection of life.

The opportunity of the CSO or other management person to make a close examination of a bomb threat received by telephone can be lost or severely diminished when the person receiving the call fails to capture relevant details. When a caller says, "There is a bomb in your building," a natural reaction can be panic. A good way to keep that from happening is to teach employees how to respond and provide them with a checklist that can be kept handy for use. Those employees most likely to receive bomb threat calls should be specially trained. In this group are switchboard operators, security officers, receptionists, and executive secretaries. The key points are as follows:

- Keep the caller talking for as long as possible.
- Ask the caller to repeat the message.
- Take notes. Write down exact words.
- Ask the caller to specifically state where the bomb is located and when it is set to detonate.
- Ask what part of the facility should be evacuated first.
- Ask for a description of the bomb. What does it look like? How is it packaged? What is it made of and how does it work?
- Ask why the bomb was placed and what group is responsible. Ask the caller if he or she was the person who placed the bomb. Ask where the caller is now.
- Tell the caller that the facility is occupied and that a detonation could result in death and serious injury to many innocent people.
- Listen closely to the caller's voice. Is the caller male or female? Calm or excited? Does the voice have an accent?
- Pay attention to background noises that may give a clue as to the caller's location. Traffic sounds, music, and voices heard in the background may be important.
- Keep the line open after the call has ended. It may be possible to trace the call.
- Notify the security control center immediately after the caller hangs up. Be ready to be interviewed and to hand over notes made during the call.

Evaluation of the Bomb Threat

The very first task of the CSO who has been informed of a bomb threat call is to evaluate it. Interviewing the person who received the call and examining notes taken during the call are the preliminaries to a judgment. The

evaluation takes into account the details and characteristics of the call itself, prior bomb threat calls, and similar threats that have been made in the community or against other organizations. Evaluation is essentially a process of judging the credibility of the threat; in other words, is the call a hoax or is it the real thing?

The CSO has to recognize that absolutes are never possible and that if error in judgment is to be made, it has to be made on the side of caution. For example, in considering the details of a call, the CSO may note that the caller was described as a giggling young girl, hard rock music was playing in the background, and the girl's answer to the question as to motive was that "you people are so, so uncool." In this case, the CSO may conclude that the call is probably a hoax. Another case can have entirely different indicators such as an adult male who expresses anger against the organization, reveals knowledge of the workplace, and knowledge of bomb construction. This threat could be genuine. In still another case, the indicators may be few and unrevealing, a circumstance that requires the CSO to treat the threat as if it were real.

The CSO's evaluation is not always the only evaluation. The property manager of the facility may be tasked by policy or plan to share in making a joint evaluation or making the evaluation independent of another's judgment. The same can apply as well to the operations manager, the CEO, or the senior executive in the facility at the time the threat is received. Like too many cooks spoiling the broth, too many evaluators can spoil the evaluation and waste time that could be better spent conducting a search or evacuating the premises.

Evaluation of a bomb threat call falls into one of three categories: we think it is a hoax, we think it might be real, and we do not know. Other factors may apply as well. For example, a regulatory standard of a safety-sensitive industry may require immediate and full evacuation no matter how management views the threat, or a collective bargaining agreement may require that employees be informed, and those who wish to leave may do so. Another influence may be management's worry about liability arising from injuries sustained by employees as they evacuate the facility.

Time is the enemy when deciding what to do when a bomb threat is received. Decision time is reduced when the decision-maker has participated in drills and practical exercises that tested the bomb incident plan.

Evacuation Options

Three options are available. The first is to search without evacuating. This option is appropriate when the threat is very, very likely to be a hoax. It allows upgrading to evacuation when, for example, a suspected bomb is found or when a subsequent determinative threat call is received.

The second option is to evacuate partially or fully and then search. This option is appropriate when the threat might be real. The caller may have said the bomb is located in a particular area, in which case that area and its surrounding areas would be evacuated and then searched. Alternatively, the caller may have described multiple bomb locations or a bomb that is devastating, in which case the entire facility would be evacuated and then searched.

The third option is to fully evacuate and not search: This option is appropriate when the threat appears to be very, very real. The caller may have revealed knowledge of bomb construction, mentioned revenge, or said that he or she is a member of a militant group known to be in opposition to the organization. Events that occurred prior to the call may be relevant such as successful or unsuccessful recent attempts at arson or sabotage. This option reflects the management's belief that the best course of action is to get out of the facility right away. If detonation does not occur within the next 12 h or so, a conclusion can be made that a detonation will not occur. This conclusion should be made by a person knowledgeable in bomb construction.

The Search

Bomb searching is in most cases conducted by persons familiar with the workplace and almost never by police officers. Public safety policy often discourages the participation of police officers in bomb searches on private property, unless probable cause exists to believe that a bomb is in fact present. Probable cause can be established by the details of the bomb threat call or by the discovery of a suspect bomb. With a belief established, the police are more likely to want to be actively involved in making or directing the search. Although employees at the workplace have a greater familiarity with the possible places of bomb concealment, officers trained in bomb disposal know how to avoid booby traps and mistakes that can lead to detonation. Fig. 15.5 depicts the use of a specially trained dog to make a bomb search.

Searching has to be thorough, and thoroughness is affected by the size and configuration of the workplace. It is fair to say that making a thorough search is not easy in any working environment. Even small environments uncomplicated by multiple workstations, equipment, and labor-intensive activities present problems. Large and complex environments, such as manufacturing plants and high-rise office buildings, are searchable on a genuinely thorough basis only with substantial expenditure of effort and time. A 20-story office building, for example, might require 48 h of uninterrupted looking with a 20-person team before it can be said with assurance that a bomb is not in the building.

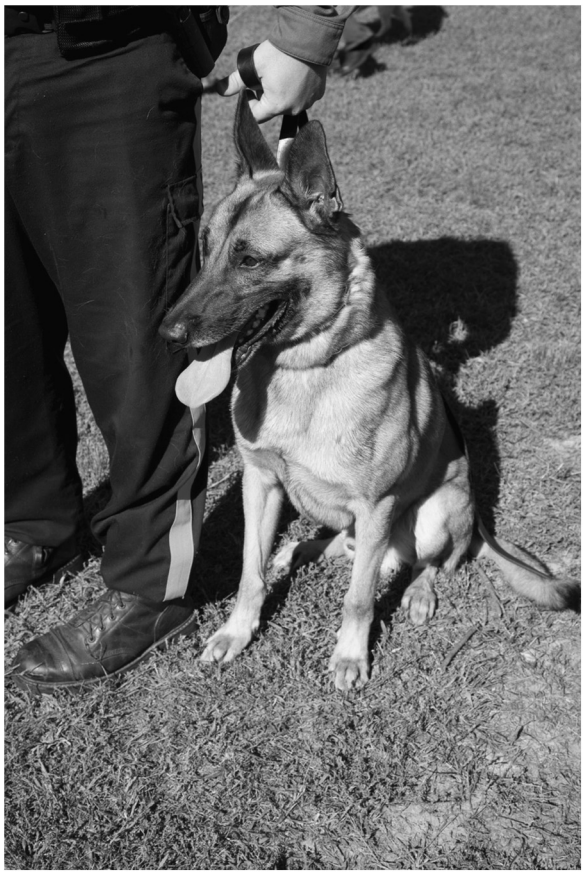


FIGURE 15.5
Sniffer dogs are a common resource for searching potential bomb sites. *Istockphotos.*

It is seldom possible in a large and complex environment to conduct a comprehensive search because time does not allow looking into false ceilings, examining every file cabinet, and removing panels from equipment. Neither is it acceptable to disrupt or shut down work operations for two full working days while a search is in progress. A practical solution might be to prioritize, as part of the planning process, those places that should and can be thoroughly searched within the time available for searching. What this means is that searching with thoroughness remains firm, but with attention to areas that would have been accessible to the person who planted the bomb.

Searchers have to be careful. To exercise care, searchers must know what a bomb looks like, or more accurately be able to spot and be wary of innocuous-appearing containers and contrivances that could be booby traps.

Anything of a suspicious nature has to be approached with great caution. A searcher who discovers what may be a bomb should be a safe distance away, warn others to leave, and report the circumstances immediately. At the other end of the line is a security officer prepared to act according to procedure, which may be to make a public address announcement, notify the fire department, summon emergency medical assistance, inform the police, and ask for the services of a bomb disposal team.

Probability and Criticality

In deciding what to search, two factors are pertinent: probability and criticality. How probable is it that a bomber would be able to penetrate the organization's security defenses? If the probability is high, how probable is it that a bomb or bombs would be placed in some areas as opposed to others? An evaluation of probability might lead to a search priority that concentrates on areas that are outside the umbrella of security control such as lobbies, garages, and other areas easily accessible to the public.

Criticality takes into account a priority for searching areas where the greatest damage can be done. Probability and criticality need to be balanced. For example, it may not be sensible to set a high priority on searching the computer center when the probability is low that a bomb could be brought into the computer center without detection. On the other hand, the computer center may demand a search because of its criticality to business operations.

Discovery of a Suspicious Object

The size and location of a suspect bomb has an influence on the extent of evacuation. For example, a suspect bomb about the size of a cigarette pack that is found in a storage room on an empty floor might not merit evacuation, partial or otherwise. As a general rule, 300 ft of lateral area around a suspect bomb should be cleared of all nonessential response personnel. The vertical areas above and below a suspect bomb should also be cleared. For example, if a suspect bomb is found on a floor of a multistory building, the floor involved plus the floor immediately above and the floor immediately below should be cleared.

Total evacuation is mandatory when a suspect bomb is judged to be genuine and capable of inflicting injury. In the absence of that judgment, certain employees (such as security officers and maintenance employees) may remain to perform essential life-protecting and shutdown tasks.

The rule about not touching a suspicious object is a rule that cannot be ignored. The rule, however, cannot apply until an object is seen, evaluated, and determined to be suspicious, all of which can be done in the blink of an

eye. Because a bomb is likely to be concealed in places such as cabinets, drawers, and trash receptacles, the searchers have to probe and touch. But at the instant a suspicious object is detected all touching must stop. Actions that follow can include the following:

- Questioning employees who may be able to account for the presence of the suspicious object.
- Ordering a partial or full evacuation.
- Notifying the bomb disposal team.
- Notifying the fire department.
- Readying first aid supplies and calling for standby medical personnel and equipment.
- Asking the police to assume command of the situation.

The bomb disposal team leader or the fire officer in charge may ask for further information about the location of the suspect device relative to stored fuels, chemicals, flammables, power plant, and fire exits. Because of the possibility that more than one bomb has been planted, orders may be made for the search team to continue examining areas that have not yet been searched.

Aftermath of an Explosion

Excellent advice is given by Bevilacqua and Stilp (2004). The aftermath of an explosion, regardless of size, will have a severe impact on local emergency services. Severe structural failure of the building of impact and surrounding exposures all may require specialized search and rescue teams. Because of the overwhelming medical consequences, there may be a requirement to set up field hospitals, lessening the impact on local medical resources.

FIRE EMERGENCIES

Dealing with fire emergencies is a preincident collaborative process that involves the manager of the protected property, a fire marshal or inspector, and the CSO. Collaboration can also include professionals representing the safety and risk management disciplines.

Criminal and civil liabilities that can arise from a fire emergency place a grave responsibility on the property manager, a responsibility that dictates a prominent role in developing the fire response capability and in leading the fire response effort pending arrival of the fire department. The fire marshal or inspector ensures that response procedures meet fire code requirements. In some communities, the fire department provides instruction in how to identify and correct fire hazards, operate extinguishing equipment, and evacuate a building.

The CSO represents the interests of his or her employer. The employer can own or rent. If the employer is the building owner, the property manager and the CSO are on the same payroll (except when the owner has outsourced the property management function, in which case the property manager is a contract employee). Regardless of the arrangement, the property manager and the CSO, each operating from separate disciplines, are attentive to ensuring the integrity of the premises and the safety of the occupants.

Fire Control System

Preparing for a fire emergency takes into account the property's fire detection and suppression system. If the property is a modern office building, the system will feature a combination of manual pull stations, ionization detectors, overhead sprinklers, fire extinguishers, alarm horns, voice speakers, pressurization fans, firefighter telephones, and an emergency generator for backup power.

A fire alarm sounds when an electronic sensor detects heat or smoke or when a human manually activates a pull station or similar device. Typically, in a high-rise building, an alarm will sound on the floor where the sensor or pull station is activated, plus the floor above and the floor below. This procedure avoids evacuating the entire building when a fire condition is minor or not actually a fire at all.

In addition to automatically sounding an alarm, a fire control system can be set to open and close louvers and activate fans. The effect is to force smoke out of the building and bring fresh air into stairwells.

Floor Wardens

A chief responsibility within the purview of the property manager is a floor warden (or fire warden) program. A program of this type usually designates one or more wardens per floor, depending on floor population, size, and configuration. The wardens are trained initially and periodically. Initial training provides skill development in using handheld fire extinguishers, administering cardiopulmonary resuscitation (CPR) and first aid, operating defibrillation and oxygen resuscitation equipment, and avoiding the risks of bloodborne pathogens. Periodic training refreshes these skills and provides complementary knowledge in subjects of current concern.

Fire drills, which are often monitored by a fire department representative, provide an opportunity for practice and improvement.

A floor warden is almost always a volunteer and rarely rewarded monetarily. Acceptance into the program is predicated on physical agility, stamina, and a

work schedule that provides reasonably high assurance that the warden will be present for duty when fire occurs. Cooperation of the floor warden's supervisor to permit attendance at training and practice sessions is a must. A floor warden's tasks include the following:

- Educating coworkers concerning their individual responsibilities for fire prevention, reduction of safety hazards, how to report a fire, how to evacuate, and where to assemble following evacuation.
- Preventing, reporting, and correcting fire and safety hazards by inspecting the floor daily.
- Exercising leadership during an evacuation by directing coworkers down stairwells and ensuring that no one has been left behind.
- Providing first-responder medical assistance.
- Knowing the locations of the fire stairwells, pull stations, and escape routes.
- Posting an escape route diagram and related information on bulletin boards and other conspicuous places.
- Enlisting the services of helpers to direct employees away from the elevators and down the fire stairwells in fire emergencies.
- Briefing every new person on the floor concerning what to do in the case of an emergency.
- Keeping a list of persons on the floor for head counting purposes immediately following an evacuation.
- Identifying persons with medical conditions, such as asthma or pregnancy, who may need help during an evacuation and arranging to provide the needed help.
- Being alert for fire hazards (e.g., overloaded electrical circuits, unattended cooking appliances, and materials blocking stairwell doors).

An observation by Uzzell (1993) is appropriate: "One of the many problems in an emergency is confusion and the panic that can easily follow. Everyone in the facility from management down to the line employee must know what to expect. Each person should know what he or she is to do, who is in charge, where to go if evacuation is ordered, etc."

Fire Conditions

A fire condition is not necessarily a fire. It may be the result of a malfunctioning detector, smoke from a coffee maker, or heat that should not be there. On the other hand, a fire condition can be the result of an actual fire, the indicators of which are moderate to heavy smoke, flame, and intense heat.

When an alarm sounds, floor wardens begin immediately to look for a fire condition, starting with coffee and copying rooms (places where fire is most likely to occur). If a search reveals unexplainable smoke, flame, or intense heat, the warden pulls a manual pull station, the effect of which is to confirm the electronic detection made seconds earlier. This dual reporting, one by a scientific instrument and the other by a human action, is registered by sound and sight on a panel of fire control equipment that is most often located within a security control center or the property manager's office.

The fire control system automatically signals the fire department. Also, the security officer monitoring the panel telephones the fire department to ensure the message has been received.

Simultaneously, an announcement is made over the fire control system's public address component. The announcement can be made by a taped voice message or a message spoken live. If live, the property manager or designee orders the message to be sent. Message content can inform employees that a fire condition has been detected in the building and that employees are to take one of the following three actions:

- Stand by at the work station for further instructions.
- Proceed to the nearest fire exit and stand by for further instructions.
- Immediately evacuate.

Meanwhile, the floor warden who verified the fire condition and activated a manual pull station should also call the security control center and fire department. (A cherished preference of fire departments is to receive multiple calls.) The diagram in Fig. 15.6 shows actions taken when a fire alarm is pulled.

The telephonic report to the fire department dispatcher is done quickly but clearly. The person making the call reports the pertinent details: name of the company, street address, where the fire is located specifically, and whether or not people are trapped or have been injured or killed. The caller should expect the dispatcher to ask for the caller's name and return phone number, and to keep the line open.

When a Fire Condition Is Serious

When a fire condition appears uncontrollable, the floor warden instructs employees to exit even when the public address message may have told employees to stand by or await further instructions. When the floor is apparently empty of people, the floor warden makes one last check to see if this is so. If so, the floor warden notifies the security control center by telephone, by handheld radio issued to the floor warden for use in fire

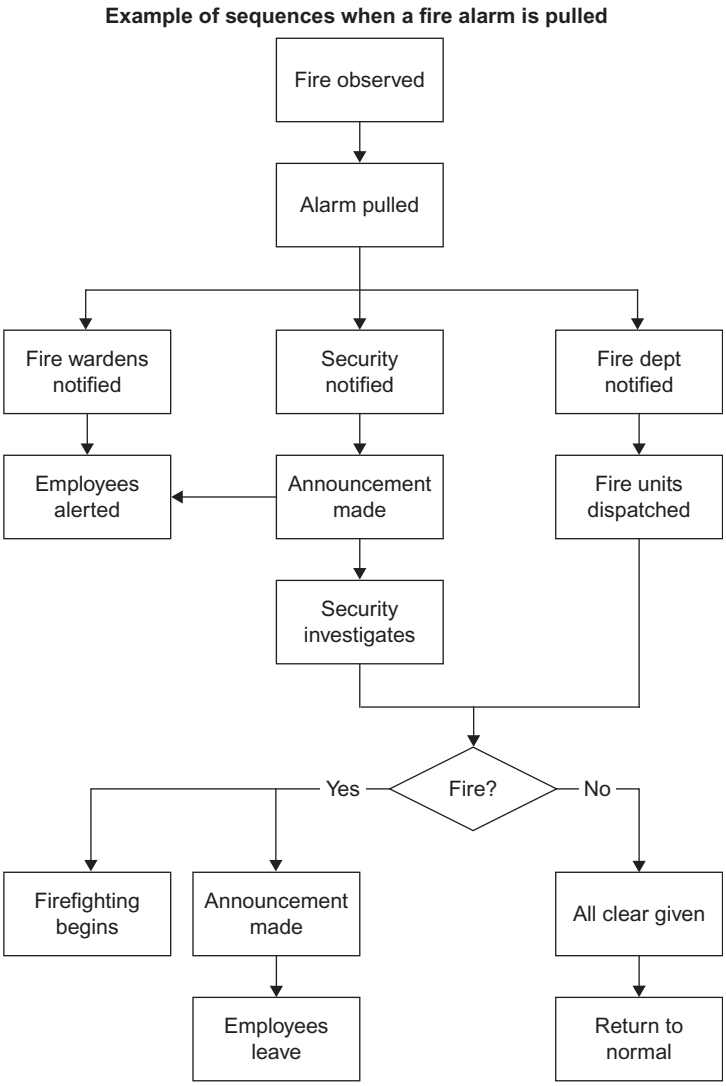


FIGURE 15.6
A fire alarm signal initiates a predetermined process.

emergencies, or in person. A security officer or security supervisor inside the security control center keeps track of which floors have been fully evacuated.

By this time, the property manager and the CSO are in the security control center. The property manager is making on-the-spot decisions, and the CSO is ensuring correct performance of security officers.

Fire Control Team

The property manager also organizes and supervises what can be called a fire control team. Team members consist mainly of building engineer staff, with possible augmentation by security officers. Duties of the team include going without delay to the scene of the reported fire condition to determine the presence or absence of fire, and if fire is present, attempt to contain, suppress, or extinguish it.

If the fire spreads or increases in size, the extinguishing attempt is aborted. Heat generated by a moderate to large fire will activate a sprinkler system, assuming that a sprinkler system is installed.

If fire is not verified, the team determines the reason for the false alarm. A malfunctioning or overly sensitive fire or smoke detector is often the culprit. A smoke detector that is perfectly functional may confuse dust with smoke. San Luis et al. (1994) urge emergency managers to inspect smoke detectors annually. Batteries in portable units should be replaced at least once a year.

The fire control team makes a report of findings to the property manager. Depending on the fire control team's report of findings, the property manager uses the public address system to communicate one of the following three messages:

- Evacuate. (A serious fire is in progress.)
- Stand by for further instructions. (The fire control team is unable to make a definitive judgment, or the fire is minor and being extinguished.)
- Return to normal work activities. (There is no fire.)

If evacuation is ordered, the fire control team's next task is protection of human life by fighting or containing the fire, directing employees to leave, and helping incapacitated occupants out of the building.

Security Officers

The efforts of floor wardens and members of the fire control team are supplemented by security officers. And this is where the CSO has a prominent role. The CSO develops, and ensures through training and practice, procedures that guide security officers in the following:

- Detecting and correcting fire hazards.
- Reporting fire conditions.
- Monitoring and responding to annunciations of the electronic fire detection equipment.
- Assisting or filling in for floor wardens and fire control team members.

- Directing traffic to allow unhampered access of firefighting vehicles and equipment.
- Operating radio and telephone equipment for command and control purposes.

An effective fire response capability relies on a 24 h/day human presence augmented with sensing and communicating equipment. The human presence ideally consists of security officers trained to perform fire response duties. In the scheme presented here, the sounding of a fire alarm after hours sends a security officer to the affected area to look for a fire condition. In essence, the after-hours security officers assume floor warden response tasks.

Occupants

A fire response plan includes provisions for educating occupants as to their individual responsibilities with respect to reporting fire hazards, preventing fire, and following instructions during a fire emergency. Fire drills, which normally occur at 6-month intervals, are part of the education process.

An excellent method of educating employees is one-on-one and small group briefings by floor wardens. Every occupant should be thoroughly briefed at least once, preferably on the first day of employment. Briefing points are mentioned in Fig. 15.7. They include the location of detectors and pull stations, escape routes, and stairwells; the procedural steps of an alarm and the order to evacuate; the rule against using or trying to use an elevator to evacuate; the rule against running during an evacuation; and the location of the evacuation assembly area.

NATURAL DISASTERS

A natural disaster, in the context used here, is an event that causes death, injury, and significant property damage. The common natural disasters most dreaded by business organizations, and therefore anticipated by their planners, are floods, earthquakes, hurricanes, tornadoes, and volcanic eruptions. Hurricanes and tornadoes seem to occur with greatest frequency, and flooding is often a consequence. In some instances, flooding results from heavier than normal volumes of snow that melt in the spring. Earthquakes are not nearly as common but should be seen as a serious threat along fault lines. Volcanic eruptions are rare and usually foreseeable.

Businesses along the Louisiana and Mississippi shorelines knew Katrina was on the way, and although severity of it was announced, few businesses did not expect Katrina would cause the damage it did, and for some of them, the consequences were unavoidable given the limited resources they had

Building Evacuation Checklist

Y	N	On the Floors
☐	☐	Are there at least two primary means of escape from each floor?
☐	☐	Are same-floor escape exits separate from each other?
☐	☐	Do escape routes avoid dead ends?
☐	☐	Are escape routes posted?
☐	☐	Are escape routes highlighted with strobe lights or other markers?
☐	☐	Are escape exits marked and lighted?
☐	☐	Are escape stairwells equipped with emergency lighting?
☐	☐	Are escape stairwells free of obstructions?
☐	☐	Are escape stairwell floors covered with a nonskid surface?
☐	☐	Are arrangements in place to help handicapped persons escape?
☐	☐	Are life-saving equipment and supplies (e.g., stretcher and first-aid kit) on hand?
☐	☐	Are escape stairwells fire resistant?
☐	☐	Are escape stairwells equipped with blowers to keep out smoke?
☐	☐	Is there a procedure for crossing from one stairwell to another?
☐	☐	Does each floor have an adequate number of floor wardens?
☐	☐	Are floor wardens trained in evacuation procedures?
☐	☐	Are floor wardens equipped, e.g., with a flashlight and bull horn?
☐	☐	Are building occupants educated as to evacuation procedures?
☐	☐	Are evacuation drills conducted at least every 6 months?
☐	☐	Are fire alarm pull stations operational and conspicuous?
☐	☐	Are smoke/heat detectors operational and placed appropriately?
☐	☐	Can the public address system be heard everywhere on a floor?

FIGURE 15.7

On their first day of employment, new hires should be briefed on the manner of building evacuation. A checklist can be helpful.

In the Security Control Center

Y	N	
☐	☐	Does the SCC have a dependable back-up power source?
☐	☐	Is the fire detection panel in the SCC?
☐	☐	Is the public address system in the SCC?
☐	☐	Are the security officers trained to operate SCC equipment?
☐	☐	Do the security officers test the equipment once a month?
☐	☐	Do the security officers make monthly checks of fire extinguishers?
☐	☐	Does the SCC have on hand emergency medical supplies?
☐	☐	Are security officers trained in evacuation procedures?
☐	☐	Are evacuation procedures in writing and current?
☐	☐	Do security officers enforce fire zone parking rules?
☐	☐	Do security officers direct traffic to assist arriving emergency vehicles?

In the Property Management Venue

☐	☐	Does the property manager prepare and keep current an emergency response plan that incorporates the activities of floor wardens, security officers, maintenance employees, and others?
☐	☐	Has the emergency response plan been approved by the fire department and coordinated with the police department?
☐	☐	Does the property manager manage ongoing programs of safety awareness for building occupants and specific training for response employees?
☐	☐	Does the specific training program include fire prevention, evacuation procedures, and first responder medical assistance such as CPR and First Aid?
☐	☐	Does the property manager assume overall control of a building emergency pending arrival of fire or police departments?
☐	☐	Are maintenance employees trained to operate fire suppression systems and to activate/shutdown ventilation and other systems as needed?
☐	☐	Do maintenance employees periodically inspect heat/smoke detectors, water sprinkler systems, stand-pipe equipment, and back-up power systems?
☐	☐	Are maintenance employees equipped with radios and do the radios interface with the SCC?

FIGURE 15.7
(Continued).

available to deal with the storm. In New Orleans, a city surrounded by a rim, was a huge bowl into which Katrina dropped an incredible amount of water. Again, the CSOs of New Orleans' businesses were not prepared to deal with the magnitude of the flooding, especially since they had no reason to believe some of the drainage ditches designed to carry water out of "the bowl" were not functional.

These events are sometimes referred to as "Acts of God." As a point of law, it is ordinarily held that a person or entity cannot be charged with responsibility for the injuries or losses resulting from an "Act of God." For example, a failure to complete a construction schedule on the date agreed because lightning knocked out a key piece of construction equipment does not create a liability. With or without liability, a company's management has to be prepared.

The CSO is one of several persons charged by management to plan and prepare for natural disasters. The organization's emergency management group, in which the CSO plays a key role, will invariably network with external emergency response agencies that exist at county, state, and federal levels. At the federal level is FEMA. This agency is concerned with earthquake hazard reduction, dam safety, natural and nuclear disaster, and the consequences of terrorist incidents. FEMA's main functions are to anticipate, prepare for, and respond to major civil emergencies by deploying civil defense systems and other available resources.

Partner agencies of FEMA at the local level are civil defense and emergency management offices. The main goal of FEMA and local agencies is to protect lives, property, and the means of economic production threatened by large-scale emergencies. Civil defense includes the organization and training of volunteers, maintaining warning systems, providing shelters, stockpiling food and medicine, firefighting, performing rescue operations, removing wreckage, and restoring order. The main responsibility for peacetime civil defense lies with each state government. A civil defense organization that is part of a local branch of government can be a business organization's most important partner in preparing for and responding to large-scale disasters.

A local emergency management office typically operates a command and control center, tracks impending disasters, such as hurricanes and rising floodwaters, and communicates conditions to first-responder agencies.

MEDICAL EMERGENCIES

A chief reason for employing security officers is to have readily available a capability to respond when an employee or visitor is injured or becomes

FIGURE 15.8
The responding security officer or security supervisor must understand when a call for medical assistance is necessary. *Burns International Security Services.*

seriously ill. Calling an ambulance to the scene, as depicted in Fig. 15.8, is a call made on the side of caution.

Just having security officers at hand is not enough. They need to be trained to deliver assistance in situations involving asphyxiation, cardiac arrest, severe bleeding, unconsciousness, poisoning and drug overdoses, burn, electric shock, heat exhaustion, and bone fractures.

In these situations, the victim is cared for until arrival of skilled medical professionals whose assistance is focused on saving a life or improving pulse, temperature, and breathing (vital signs). In minor emergencies, security officer's actions may prevent a victim's condition from worsening and provide relief from pain.

The nature of the assistance corresponds to the victim's needs. Delivery of the assistance depends on the responder's knowledge and skill. Knowing what not to do in an emergency is as important as knowing what to do. Moving a person with a neck injury, for example, can lead to permanent spinal injury and paralysis.

Fundamental Practices

Several fundamentals apply to all medical emergencies. The CSO is responsible for spelling them out in the standard operating procedures of the guard

force and ensuring competent performance of them through training and practice. The fundamentals are as follows:

- Call for professional medical help without delay.
- Determine that the scene is safe before attempting to provide first aid.
- Move the victim only as necessary to prevent further injury.
- Inform the victim, if conscious, that medical aid has been requested.
- Assess the scene, asking bystanders or coworkers about details of the injury or illness, any care that may have already been given, and preexisting conditions such as diabetes or heart trouble.
- Look for a medical bracelet or card that describes the victim's special medical conditions.
- Assess the victim to determine if life-threatening conditions exist, for example:
  - Examine the airway to see if it is open and unobstructed.
  - Look, listen, and feel for breathing.
  - Feel for a pulse.
  - Look for external bleeding.
  - Check skin color and temperature for indications of circulation problems.
- Place the injured person's head in line with the body.
- If no evidence exists to suggest potential skull or spinal injury, place the injured person in a comfortable position.
- If nausea is a condition, position the victim on one side so that vomit does not obstruct the airway.
- Look for the indications of shock that are typically manifested by anxiety or restlessness; pale, cool, clammy skin; a weak but rapid pulse; shallow breathing; bluish lips; and nausea.
- Treat shock by covering the victim with blankets or warm clothes and elevating the feet.

Untrained or poorly trained first responders can make serious mistakes when confronted with medical emergencies. Mistakes can be avoided or mitigated by referring to written guidance such as that shown in Fig. 15.9.

Exposure to AIDS and Hepatitis B

The acquired immune deficiency syndrome (AIDS) and hepatitis B diseases merit serious worry to providers of first aid, CPR, and defibrillation. The chief concerns are infection through contact with blood and other body fluids. Persons at a high-risk level are security officers with first-response duties.

Because AIDS and hepatitis B infections occur in the workplace, the Occupational Safety and Health Administration (OSHA) has developed

Guidance to First Responders

Asphyxiation. Cessation of breathing can cause brain death within 4 to 6 min unless relief is administered. The most common technique for preventing asphyxiation is artificial respiration. In a case of drowning, artificial respiration should be attempted even if the victim appears dead. People submerged in cold water for more than 30 min have responded to artificial respiration and recovered.

Cardiac Arrest. Position the victim face up on a firm surface and clear the airway. Tilt the victim's head back and lift the chin forward. Give the victim two breaths by mouth. If no pulse is detected at the carotid artery (located in a groove beside the windpipe in the neck), kneel next to the victim and place the heel of one hand on top of the other over the lower half of the sternum. Depress the chest about 2 in, which forces blood from the heart into the victim's arteries. When the pressure is released, blood flows back into the heart. Apply pressure in short, rhythmic thrusts about 15 times every 10 s. Continue until the victim revives.

Severe Bleeding. Welling or spurting blood is a clear sign of severe bleeding. If a major artery ruptures, a person may bleed to death within a minute. Shock usually follows loss of blood, and must be prevented as soon as the bleeding has been stopped. Bleeding is stopped by applying pressure directly over the wound and, when possible, elevating the bleeding body part. Hold a sterile dressing or clean cloth firmly over the wound. If the bleeding is from an arm or leg, reduce blood loss by applying pressure at a point adjacent to the bleeding. Arteries pass close to the skin at these points and can be compressed against underlying bone to reduce bleeding.

Loss of Consciousness. This condition occurs when the brain does not receive enough blood. Elevate the unconscious person's feet or lower the head below the height of the heart. Make the victim warm to prevent shock. Loss of consciousness may result from a variety of causes, including head injury and epilepsy. If the victim is breathing, provide comfort until medical help arrives. If the victim is not breathing, administer artificial respiration.

Poisoning. A poisonous substance introduced into the body causes symptoms such as nausea, cramps, and vomiting. First off, prevent further poisoning, such as by removing the victim from a toxic environment. Next, identify the poison, for example, by asking the victim to name it or look for suspicious containers or call the nearest poison control center. Knowing the poison determines the appropriate treatment. Unless instructed to do so by the poison control center or medical professional, emergency treatment does not include giving the victim anything to eat or drink, nor inducing the victim to vomit.

Drug Overdose. Drug overdose is difficult to diagnose because the symptoms vary widely and often appear connected to an illness or injury. Symptoms include dilated or contracted pupils, vomiting, difficulty in breathing, hallucinations, and in severe cases unconsciousness and slow, deep breathing.

Burn. First-response actions are: remove the source of the burn as quickly as possible; immediately cool the burn with cold water; on less serious burns apply a clean, cold wet towel or dressing to ease pain and protect against contamination; treat a chemical burn by continuously bathing it with running water for at least 20 minutes; do not use wet dressings and ointments; apply dry, sterile dressings held in place by bandages; and obtain prompt medical attention.

Electric Shock. Contact with electrical current is often fatal. Do not touch the victim's body before the source of the shock is turned off. If the victim has stopped breathing and has no pulse, administer CPR.

Heat Exhaustion. Exposure to excessive heat depletes body fluids and body salts. Symptoms include pale and clammy skin, heavy perspiration, weak pulse, shallow breathing, headache, and vomiting. A victim should rest in a cool area with feet elevated. Further cooling can be achieved with cool water compresses and a fan. Fever-reducing medication should not be used. A victim may feel nauseous at first, but after resting for a period, he may be able to sip minimally salty water or an electrolyte solution to replenish lost salt.

Bone Fracture. Great pain, an inability to move the affected part, a deformed appearance, and pain or tenderness at a specific point indicate a fracture. Do not straighten or move a broken limb until medical help arrives. If a person is found with the head or body in an unnatural position, a fracture of the spinal column is a possibility. Do not attempt to straighten or move the injured person's body because of the chance of permanent paralysis or death.

FIGURE 15.9

Information of this nature can be used as a training aid or job tool.

recommended practices to protect against exposure. The practices include precautions for mouth-to-mouth contact and contact with blood and other body fluids.

The usual symptoms of acute hepatitis B infections are flu-like and include fatigue, mild fever, muscle and joint aches, nausea, vomiting, abdominal pain, diarrhea, and jaundice. A severe hepatitis B virus infection may be fatal. It is also preventable by the administration of a vaccine. The vaccine is recommended for persons at risk of infection, including security officers and other first responders.

Protective equipment and devices must be on hand for immediate use. These include:

- Gloves when blood, blood products, or body fluids may be touched.
- Gowns, masks, and eye protectors when there is a potential for splashing of blood or body fluids.
- Pocket masks, resuscitation bags, or other ventilation devices when CPR is administered.

Prudent practices for protection include the following:

- Wearing protective gear such as pocket mask and gloves.
- Cleaning up blood spills immediately with detergent, water, and household bleach diluted at 1 to 10 parts of water.
- Washing hands thoroughly after removing protective gear and immediately after contact with blood or body fluids.
- Informing coworkers and others concerning modes of transmission and prevention of infection. The key points are as follows:
  - Get a vaccination.
  - Treat all blood and body fluids as potentially infectious.
  - Obtain medical evaluation following an exposure incident.

An exposure incident is one that results from the performance of a job duty such as a security officer giving first aid or administering CPR to an injured or ill person. Exposure means contact between the infectious agent (blood or body fluid) and an eye, mouth, or other mucous membrane and nonintact skin.

The CSO or other responsible manager should prepare a postexposure report that documents details of the incident such as how the incident occurred, persons exposed, and the name of the source individual.

The source individual's blood should be tested for infection as soon as possible after consent is obtained. If consent is not obtained, that fact should be documented. Results of the source individual's testing should be made available to the exposed employee, and the employee informed of applicable laws and regulations concerning the identity of the source individual.

The General Duty Clause of the OSHA Act requires employers to provide employment and a place of employment free from recognized hazards. Employers must comply with OSHA standards or state standards. States with occupational safety and health programs usually embrace comparable standards.

CONCLUSIONS

The art and science of emergency management is undergoing revolutionary change resulting in the main from the terrorist threat. The security literature prior to September 11, 2001 contained very little concerning the management of terrorist-related emergencies. That omission continues to be corrected rapidly.

Change is also occurring in the technology of emergency management. State-of-the-art equipment coming off the production line can warn organizations of potential threats, thwart attacks, and increase protection of people and property. In the services sector, education, and training programs are teaching emergency management principles to security professionals, first responders, and a host of other practitioners now firmly connected to the emergency management function.

REVIEW QUESTIONS

1. What are the actual words for the acronyms EOP, EMT, PIO, NIMS, ICS, and FEMA?
2. What is the mission of FEMA?
3. Name the duties of a floor warden.
4. When a person in a high-rise office complex sees heavy smoke and flame, what should the person do first?

References

Bevilacqua, A., Stilp, R., 2004. Terrorism Handbook for Operational Responders. second ed. Thomson Learning, Inc, Clifton, NJ.

Chertoff, M., 2008. National Incident Management System. U.S. Department of Homeland Security, Washington, DC.

DePasquale, S., 2007. Emergency management planning. In: Fay, J.J. (Ed.), Encyclopedia of Security Management, second ed. Butterworth-Heinemann, Boston, MA, pp. 83–84.

Fennelly, L.J., 2004. Handbook of Loss Prevention and Crime Prevention. Butterworth Heinemann, Boston, MA.

San Luis, E., Tyska, L., Fennelly, L.J., 1994. Office and Office Building Security. Butterworth Heinemann, Boston, MA.

Uzzell, R., 1993. Emergency management planning. In: Fay, J.J. (Ed.), Encyclopedia of Security Management. Butterworth-Heinemann, Boston, MA, pp. 28–286.

CHAPTER 16

Business Continuity

What You Will Learn

- The nature and purpose of a business continuity plan.
- The nature and purpose of a business impact analysis.
- Major assets intended to be protected by a business continuity plan.
- Options for relocating critical business operations when they are threatened by a major emergency.
- The use of a security vulnerability assessment to identify critical business operations at risk.

INTRODUCTION

When management is dealing with a major emergency, it is focused on dealing with the emergency and not always with how the business will continue to function during and after the emergency. Even when an emergency operating plan (EOP) includes or overlaps with a business continuity plan (BCP), the exigencies of the emergency can block out consideration of life safety, preserving structures, equipment, materials, and technological data that are essential for the business to continue its operations, albeit at a reduced level of operations. Richards-Gustafson (2009) says it is not pleasant to think about the worst case scenarios when it comes to planning a business' future. However, when it comes to business continuity, not thinking ahead is foolish.

POLICY

The commitment of management to create a BCP, and support its implementation when needed, is demonstrated in the expression of a statement of policy. Fig. 16.1 is a sample policy. Paraphrasing Krouslis et al. (2009),

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00016-5

CHIEF EXECUTIVE OFFICER'S STATEMENT ON BUSINESS CONTINUITY

Purpose

A Business Continuity Plan (BCP) will be created for the purpose of facilitating a quick and coordinated return to the essential business operations of the company during the immediate aftermath of a disaster or catastrophic event impacting corporate headquarters. The BCP will complement and serve as a follow-on plan to contingency plans already in place, e.g., fire protection plan, bomb threat plan, and severe weather plan. The BCP will pick up where those plans end.

The BCP will take into account the company's heavy dependence on information, e.g., leading edge software, computer technology, and telecommunications. A disaster or catastrophic event will have a severe impact on computer programs and telecommunications services, which in turn will severely impact critical business functions. For this reason, the Chief Information Officer (CIO) will be in charge of developing the BCP and ensuring that plan objectives are carried out.

The managers of critical business functions will be responsible for developing procedures within their units that

- Assess the degree of loss of critical functioning
- Notify key people
- Deploy resources needed to restore critical functioning

Key points in such procedures will vary from manager to manager, but may include a mission statement, scope, decision-making responsibilities, assignment of key tasks, resources required, a process for communicating with employees immediately following a disaster or catastrophic event, a list of persons to be notified, the composition of recovery teams, recovery priorities, working interrelationships, work flow diagrams, decision trees, and training. Each set of procedures will be attached to the BCP, which managers will keep ready for use as needed.

Assumptions

Some catastrophic events, such as a nuclear explosion, will be so severe as to fall outside the scope of the BCP.

The catastrophic event impacting corporate headquarters is likely to be a wind storm, such as a hurricane or tornado, more so than other business-disrupting events, such as major fire, earthquake, bomb, civil unrest, or labor strike.

The time required to bring corporate headquarters back to normal operating routines will take not less than 2 days and not more than 30 days.

Temporary working space, equipment, data, supplies, and vendor services needed to carry out critical functions will be available within 48 h following the event. This assumption recognizes that when other companies are impacted by the same event (e.g., a hurricane), extraordinary demands will be placed upon the community's business services infrastructure, thereby placing the company into competition with other companies for needed facilities, equipment, supplies, and services. Advanced planning and preparation by service groups, such as IT and building management, will be essential.

Key employees will be available to implement the BCP. Recognition is given, however, to delay that might result from the need of all employees to first attend to the needs of their families should the catastrophic event extend into the community at large.

Objectives

Restore the most critical of all critical functions within 2 days

Restore all or most all of the critical functions within 7 days

Restore all business functions within 30 days

Business Continuity Team

Information Technology (Team Leader)

Real Estate

Procurement

Human Resources

External Affairs

Security

FIGURE 16.1

This sample business continuity policy can serve as a model for companies taking their first step in preparing for the consequences of a disaster.

management should issue a clear policy statement on business continuity planning. The policy should address the following:

- Mandatory development of a BCP; identification of the scope of the BCP.
- A method for projecting business time lost, business functions that will be out of service until full restoration, and the projected date of full restoration (all of which depend on the nature of the emergency and its severity).
- Identification of critical business functions.
- Identification of assets essential to performance of critical business functions.
- One or more alternate workplaces for performance of critical business functions; identification of responsibilities and the persons charged to carry them out.
- Periodic training and testing of the BCP, and revising it in light of lessons learned.
- Updating the BCP to meet changed circumstances.

RISK ASSESSMENT

According to Broder and Tucker (2012), risk-assessment analysis is a rational and orderly approach, as well as a comprehensive solution to problem identification and probability determination. Said another way, risk assessment is a management tool designed to assess the probability of an adverse incident, and the probable consequences to business operations should the incident occur. Determining the probability of occurrence is more subjective than objective. It often relies on the judgment of persons familiar with adverse incidents and the risk-assessment process. Among these persons is the chief security officer (CSO). The CSO will look at the organization's history of adverse incidents and incidents that with high frequency and close proximity can pose current threats. For example, the CSO will be aware of incidents that have occurred elsewhere, particularly within the organization's industry or correlated industries. Also of interest to the CSO will be incidents of a criminal nature, especially those that have occurred nearby the organization, and incidents generated by interest groups that oppose the organization. The assessment of probability can be enhanced when the CSO can acquire incident-related information from industry peers, law enforcement at all levels of government, and public sources of information such as the news media and Internet.

The assessment of probable consequences almost always uses dollars as the measuring stick. It is possible, although without precision, to estimate the

financial loss associated with the occurrence of an adverse incident. The estimate is often based on assumptions such as the incident will be less than fully catastrophic or mitigation measures in place will reduce adverse consequences.

An adverse incident, often called a threat, is different than risk. Threat is the cause of risk. Threats can be categorized as follows:

- Natural disasters such as hurricane, earthquake, and flooding.
- Man-made incidents such as crime and terrorism.
- Accidents such as fire and release of hazardous substances.

Threats impact:

- People.
- Physical assets (including money).
- Information assets.

To arrive at a reasonable assessment of threat, the CSO will conduct a vulnerability study, which in many venues is called a vulnerability assessment (VA). A VA will

- Identify the assets at risk.
- Prioritize the assets according to criticality. Criticality can be determined by estimating financial loss resulting from deaths, personal injuries, loss/destruction/damage to essential equipment, and depletion of supplies and raw materials. The estimate computes dollar losses related to interruption of operations, reduction of income, loss of business opportunity, and other undesirable consequences.
- Identify security measures in place to prevent occurrence of the threat and mitigate its effects in the event of occurrence. In rare cases, the VA might reveal the presence of more security measures than are needed.
- Recommend to management security measures that are necessary to counter the threat or offset consequences. Recommendations are often accompanied by a statement of cost, availability of the measures, such as security officers and physical safeguards, and a schedule for implementation.

A VA can be made of a single asset, a group of assets, a facility (which in itself is an asset), a facility containing assets, a complex of facilities, and facilities separated by distance. A single facility is usually the subject of a VA, and the VA is usually made by the CSO or the CSO with assistance from a small number of security professionals. However, when the facility contains highly complex assets, a team effort is the answer. The team would consist of a leader (who may or may not be the CSO), one or more engineers with knowledge of asset components, Hazmat technicians, architects (to read

blueprints and interpret structural documentation), and persons familiar with the type of operations performed at the facility. It is good practice not to use persons who work at the facility.

VA activities can include taking photos during the day and night; evaluating ingress procedures during the day, night, and weekends; examining physical safeguards at the perimeter and within the facility; testing sensors and the capabilities of the CCTV and access control system; testing the fire control detection and suppression system; examining locks, file containers containing sensitive information, safes, and vaults; reading security incident records and records of security officer training; testing security communication equipment; observing security patrol activities; and interviewing employees, janitorial staff, and vendors who regularly enter the facility.

Then there are internal workings of the organization, especially the core functions. Many believe the most important function performed is the information technology (IT) function.

CRITICAL THINKING EXERCISE

Sam Cox is the CSO of Hydrox, Ltd., and Frances Weldon is the chief information officer (CIO). Sam is the most senior of the two. Sam has received instructions from the home office to conduct a vulnerability assessment of the entire subsidiary. Because Sam is strong on physical security but not information technology (IT), he asks Weldon to take a hard look at the criteria for determining which information and which information processing equipment is critical, and which is not; report past problems in protecting critical information and equipment and how those problems were resolved; and identify protective measures currently in place. Cox also wants Weldon to identify vulnerabilities in the protective measures and recommend procedures and equipment necessary to eliminate the vulnerabilities. Finally, Cox sets a deadline for completing the work.

The deadline arrives and Weldon has not responded with a report. Cox asks Weldon for the report. Weldon says he has been so busy with other things that he's had no time to do what Cox said he needed. Cox asks him when he can expect to receive the report. Weldon shrugs his shoulders and walks away.

How should Cox handle this matter? Keep in mind he has little knowledge about the IT function.

THINKING AHEAD

The primary goal of the BCP is to get the business organization back up and running quickly and efficiently. The BCP is integral to the EOP but the emergency, as opposed to the conditions caused by it, is of less concern. The actual effects of the emergency are the focal points of the BCP. Effects can

include destruction and inoperability of essential equipment, loss of electrical power, injury to or deaths of persons with needed expertise, and the crashing of a computer system or entire network. These are the results of the emergency, not the emergency itself.

A BCP prepared in the midst of an emergency has little effective value and may be an impediment to the recovery effort. The BCP has to be created in advance of the emergency and with consideration of the EOP. For example, if a fire emergency calls for extinguishment by water in or near a computer center, the developers of the BCP will have to modify the EOP and make preparations to deal with the possibility that water may damage IT equipment. Fig. 16.2 provides a list of tasks that should be considered when thinking ahead.

Key Points in Disaster Preparation

Contact the local offices of the Federal Emergency Management Agency and Civil Defense to assure that your organization's disaster emergency plans are in harmony with the local government's comprehensive disaster plans. A key point is the emergency communications network.

Confirm that insurance coverage is adequate and in effect, that current photographs of insured property are on file, and that any specifications required by your insurance policy have been met and are confirmed in writing.

Confirm that response-related supplies and materials are on hand or will be available when needed.

Communicate response procedures with employees, contractors, customers, and other interested parties.

Conduct drills and practice scenarios.

Concentrate on disasters that are likely.

If located in a multiple-occupancy facility, communicate plans and procedures to co tenants.

Prepare detailed maps depicting key items such as utility equipment, power shutoff points, sources of auxiliary power, potential hazard areas, emergency equipment and supplies, communication equipment, first aid stations, and escape routes. Prepare process diagrams and decision trees.

Designate and equip a command and control center at the facility and a back-up location.

If computer operations are critical to the business, set up an alternate site and make arrangements for the transfer and storage of back-up data.

Ensure that responders understand the operational processes, physical layout, and equipment.

Assign to employees specific responsibilities for areas and operations of the facility. Designate teams and make them responsible to key people.

Conduct and record frequent inspections, correct problems immediately, and involve your insurance agent.

Prepare and maintain disaster preparedness gear. Items can consist of radios, walkie-talkies, batteries, first aid supplies and equipment, flashlights, bullhorns, lumber, portable generators, special clothing, oxygen tanks, defibrillators, rope, hand tools, and repair supplies.

Develop a method for cascading information to employees.

FIGURE 16.2
This chart can be useful to persons charged with preparing a BCP.

A BCP is nothing more than a multipage document, but it can be the key to preventing the death of an organization. Loss of former and future business, loss or damage to critical equipment, loss of key personnel, medical costs, loss of essential records and proprietary data, interruption of important functions, costs of moving to an alternate site, clean-up costs, loss of employee morale and public confidence, and the risk of civil liability, all add up to a price the business might not be able to pay.

CONTINUATION AND RESUMPTION

Business functions displaced by an emergency must have a place to go. One such place is called a hot site. It is so called because it has in it a ready-to-go assemblage of equipment for resuming functions without delay. The equipment can duplicate everything currently in use at the company site plus supplies to sustain personnel sent to the hot site to keep critical operations alive, even if only to a lesser degree. Such equipment and supplies can consist of telephone and Ethernet connections, lighting, back-up power, HVAC, furniture, safe and storage containers, office supplies, water and sewage, and eating and drinking supplies (at least for a limited period of time). Also, if the site is at a considerable distance from the homes of the key workers, hot-site sleeping accommodations or the services of a nearby hotel may be necessary.

In many cases, the hot-site equipment is IT equipment, and for a good reason. Few, if any, critical business functions can be performed without the use of computer equipment of some type. Notice in Fig. 16.3, computer

FIGURE 16.3
A hot site makes it possible for continuing or restoring critical business operations. *iStockphotos.*

equipment and a place to work are available. A hot site will also contain, or readily have available, documents that were backed-up within the previous 24-h period, provided that the organization has a document retention program that retains back-up media at the hot site or a storage location away from the organization's place of business.

Other forms of documentation will be taken to or kept at a hot site. These are internal agreements, such as those relating to joint ventures, salary, bonuses and stock options, accounting statements, licenses and certificates, and deeds, and external agreements made with organizations such as financial institutions, insurance and investment companies, licensing and regulating agencies, vendors, and courts.

A hot site can be owned or rented. In either case, the cost of a hot site is greater than the costs of a warm site or cold site.

A warm site contains a lesser assemblage of equipment and supplies; the usual reason being that the organization expects it can move the absent materials before the brunt of the emergency occurs.

A cold site provides space only. The time required to bring an organization into operation at a cold site is considerably longer than the hot site and warm site options.

When a company has more than one operating site, and they are far enough away from one another to reasonably expect that a threat occurrence could damage one but not the other, a fourth option is the answer. It is called a mirror site, which simply means that critical operations shut down at one site can be transferred to the other.

BUSINESS IMPACT ANALYSIS

A business impact analysis (BIA) is a methodology for establishing the value of a unit within an organization but not of the entire business. The methodology helps management identify units that merit maximum recovery effort. This is not to say that less important units are entirely ignored, only that some units are essential to business continuity while others are not.

Broder and Tucker (2012) say the BIA will help the company establish the value of each business unit and business process as it relates to the organization and not to itself, illustrating which functions need to be recovered and in what order. It identifies the financial and subjective consequences to the organization of the loss of its functions over time, highlights interdependencies, and establishes the function's "outage tolerance." An outage tolerance is that point in time when a function begins to deteriorate or fail entirely. This

is significant because the failure of one function can cause the failure of another function. Think of this analogy: A robotic device in an assembly line operation went out of whack. All of the other devices in the assembly line worked perfectly, but when the robotic device failed, the assembly line came to a screeching halt.

An alternate term for outage tolerance, according to Broder and Tucker (2012), is recovery time objectives (RTOs). These are helpful in determining which functions are the most critical, the times when they are most critical, and cost-effective strategies to prevent and reduce downtime.

The BIA is similar to the VA. For example, it will identify the following:

- Critical in-house resources on hand and ready to be used in a recovery situation.
- The totality of resources needed to carry out a recovery program.
- Which units or processes are critical to keeping the company operating?
- An outline of what the BCP must be able to do.
- Weaknesses in normal operations that would cause a breakdown and/or impede recovery efforts.
- Laws and regulatory rules that must be observed.
- Estimated costs of the recovery program.

The estimated costs of recovery are based on RTOs. When the recovery time is short, the cost of recovery is low, at least in comparison with a recovery time of longer duration. The obvious goal, then, is to recover as quickly as possible. Essential to meeting the goal is having a BCP that focuses on making RTOs as short as possible. Plan development will require studying the processes of business units, compiling information gleaned from the study, analyzing the information, constructing a recovery program based on the analysis, testing the program (which is best done by a practical exercise), and revising the program when test results do not meet expectations.

A BIA is not a one-time affair. A company will change for one reason or another; for example, introduction of a new product, emergence of a strong competitor, acquisition of or merging with another company, retooling, relocation, and so forth. A BIA should be done periodically, at least annually, and after every significant change in the way the business operates.

RECOVERY PROGRAM

The essence of a BCP is to get ready. The recovery program is a follow-on action program for sustaining execution of critical processes, mainly IT processes. The recovery program is a shift from thinking about recovery and

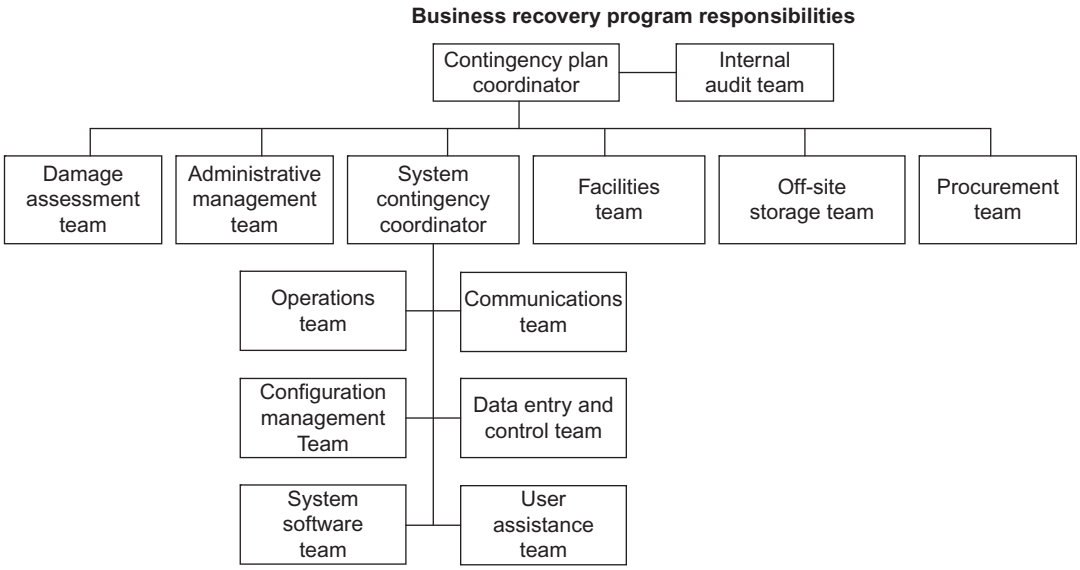


FIGURE 16.4
This sample chart depicts a typical division of functions assigned to teams responsible for a business recovery program and their interrelationship.

doing something about it. Fig. 16.4 is a sample organizational chart of persons involved in a recovery program.

According to Swanson et al. (2009), the best outcome of a recovery program is to make it possible for the company to continue "business as usual."

A recovery program can be seen to move through three steps. Actions associated with the steps are as follows:

Respond

- As much as possible, suppress and control threatening conditions.
- Preliminarily assess the nature, severity, and extent of the emergency.
- Identify needs to suppress and control threatening conditions.
- On an ongoing basis, collect and report information to those in charge of directing operations.

Recover

- Evaluate the operating capabilities of time-sensitive business operations.
- Report the status of the situation.

- Define assistance required to maintain business operations.
- Activate service level agreements in which vendors provide replacement equipment per previous agreements.
- Activate mutual aid agreements in which other companies provide quid pro quo assistance.

Restore

- If possible, continue critical business operations, or portions of them, on site.
- If needed, relocate critical business operations to separate locations such as cold, warm, hot, and mirror sites.
- Implement restoration of procedures necessary to mobilize operations.
- Inform employees, external agencies, and others as to the status of restoration.
- Assess damage.

The three steps are performed through teams comprised of individuals with step-specific skills and responsibilities.

For a recovery program to meet optimum expectations, it must have the commitment of senior management, be adequately equipped and funded, work with responding agencies and recovery teams, and be clear as to who is in charge.

CONCLUSION

Business continuity planning is a well-practiced plan for how an organization will recover and restore critical functions as quickly as possible, preferably within a predetermined time.

Business continuity is a methodology for governing the logistical steps that a business must take before or during or in the immediate aftermath of a disaster. Failure to have a BCP and the capacity to carry it out can have severe consequences to the business, even to the point of putting the business out of operation. Disastrous incidents include building fires, flooding, earthquakes, hurricanes, tornadoes, terrorist attack, warfare, crime, and pandemic illnesses.

BCP is more than just a plan. It is an organizational process ready to go into effect every day of the year. The practice of information security (i.e., protection of sensitive data and the equipment that produces and stores it) is essential to maintaining core functions at a level that will allow continuity of the business. The protection of primary and critical assets require emphasis in the BCP for one principle reason: The heart of the business depends on

information to continue its operations. Because of its importance, the BCP must be a main component of risk management.

REVIEW QUESTIONS

1. What might a business include in their policy statement regarding business continuity planning?
2. Describe why risk assessment is important in creating a business continuity plan.
3. Name two critical assets addressed in a business continuity plan and explain why they are important.
4. Explain the difference between a business continuity plan and a recovery program.
5. Describe the purpose and workings of a vulnerability assessment.

References

Broder, J.F., Tucker, Gene, 2012. Risk Analysis and the Security Survey. fourth ed. Butterworth-Heinemann, Boston, MA.

Krouslis, W., et al., 2009. Disaster Planning, Emergency Preparedness & Business Continuity. Nonprofit Coordinating Committee of New York, Inc, New York.

Richards-Gustafson, F., 2009. Protect your business continuity with a disaster plan. Ezine Articles. Retrieved from <http://ezinearticles.com/?Protect-Your-Business-Continuity-With-a-Disaster-Plan&id=3694274> (accessed 19.05.10).

Swanson, M., et al., 2009. Contingency Planning Guide for Information Technology Systems. National Institute of Standards and Technology, Gaithersburg, MD.

CHAPTER 17

Managing Information Security

What You Will Learn

- The practical management problem of balancing information system security risk and return.
- The importance of senior management's commitment to executing a systems security plan.
- The role information technology (IT) governance plays in implementing systems security "best practices" throughout the enterprise.
- Means of assessing risk, engaging in threat assessment, implementing safeguards and countermeasures, and evaluating the effectiveness of safeguards and countermeasures.
- Strategic, tactical, and operational roles involved in managing systems security.
- Common threats to corporate intellectual property and the common activities undertaken to secure intellectual property.
- The future of security ubiquitously wrapped in cloud computing, stronger regulatory controls, and better systems design, yet still, the importance of system security management.

INTRODUCTION

Security is a subjective feeling, reflecting our confidence in the safeguards we've implemented to protect our possessions. As shown in Fig. 17.1, moving from an insecure to a secure state is a process that questions our assumptions about the risks we face and how we've responded to them. And in the context of our discussion, security is the confidence we have in safeguards we've put in place to protect our information system assets like hardware, software, telecommunications, and data. Many people can have strong opinions about whether something is secure or isn't. Because security is just a

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00017-7

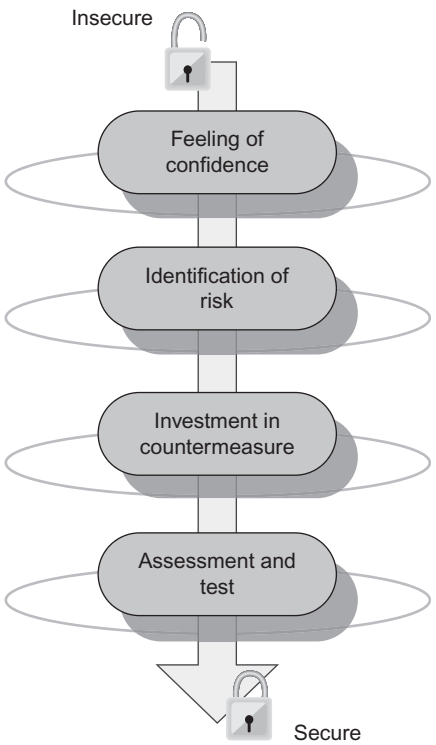


FIGURE 17.1
Security is a feeling—a perception of confidence that we have in our assessment of risk and our safeguards.

feeling, there is no absolute level of confidence that is appropriate to you, your business, or anybody else's business, except for what you define as adequate, reasonable, and important. There's no right or wrong answer. Your job then, as a manager, is to determine what is reasonable to your business in the context of the risks facing your assets.

Resources aren't infinite. In business, you do not have an unlimited budget so you make a value judgment weighing the relative risk versus the relative reward. At the end of the day, you must justify the expenses you've made and demonstrate that you've taken reasonable precautions to safeguard your systems. You cannot possibly safeguard all assets from all risks all the time. However, you can reasonably secure those assets, given your strategic priorities and competencies. The art of managing system security requires a practical understanding that security isn't absolute and that tradeoffs between risks, costs, and countermeasures must be made.

This chapter will help clarify the process that evaluates risk, selects safeguards and assess their usefulness, corrects implementation flaws, and rationally justifies their expenditure. We'll also examine how a systems security management—as practiced by modern information technology (IT) departments—can respond to and mitigate risk.

MANAGEMENT INTENTION

Intention

Everything starts at the top of the organization. It's true from a political standpoint because executives must agree that spending on systems security is appropriate, right, and necessary. And it's true from a functional standpoint because nobody would approve of such expenses unless the executive team believed it was a priority. So, we'll start from the top. That's where information security begins. And unfortunately, it's also where it might end.

Politics is the process of convincing decision-makers to spend scarce resources on *ideas*. Systems security is such an idea. Executive management must be encouraged to embrace and promote systems security before they are going to finance it. Hence, the first hurdle to face is management's conviction on the topic: *Is security a priority or not*? And if the answer is "not," well, the issue is dead. It's really that simple.

That said, most modern management teams would, in fact, "buy-in" to the idea that risks to information systems represent a legitimate hazard and demand a coordinated response to send a clear and unambiguous message: *We believe corporate information assets are at risk and steps must be taken to safeguard them*. In fact, most executives certainly wouldn't want the opposite message to be sent: *We choose to neglect information security by ignoring the jeopardy of IT assets and we've no compelling strategic interest in doing anything about it*. That idea may be quite politically unfavorable to their stakeholders.

Senior management can show their support for technology projects in myriad ways. In a practical sense, senior management provides direct funding allocations for security projects; they provide personal visibility and contribute their time to promote security projects by making investments in dedicated staff and positions; and through direct participation in industry communities and events promoting information systems security (Anttila, 2006). It's through the visible actions of senior management, their direct involvement with the process, and their approval of resources that makes security a priority for a firm. Just as Fig. 17.2 illustrates, it's the voice of

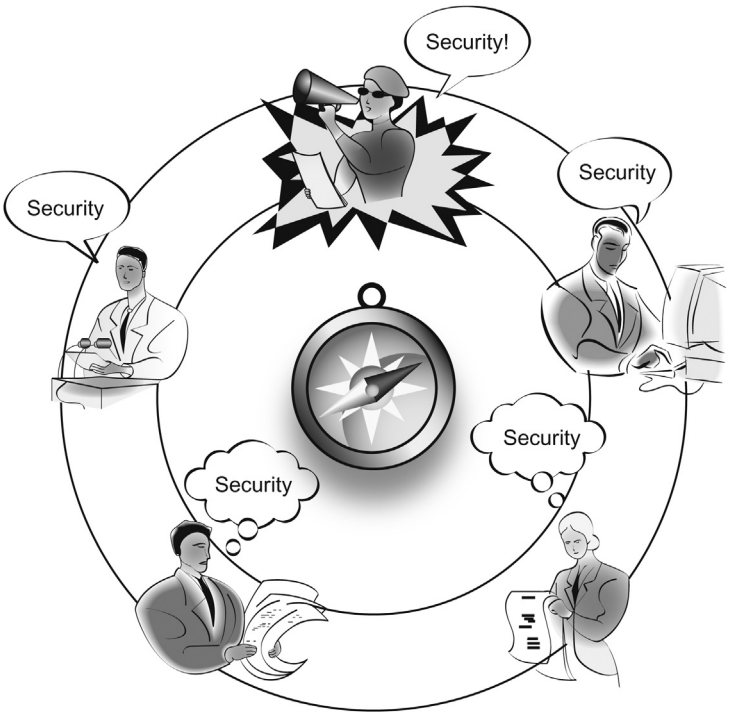


FIGURE 17.2
It's senior management's role to actively promote a culture of information security and to make security a visible strategic priority.

senior management that sets the pace and priority for managing information security.

Some organizations, though, do not look at system security as a strategic priority. That isn't necessarily bad. It's just a difference of opinion. However, that decision would allow us to question management's perception of how technology is used to execute business strategy. In some companies, computers are used to process spreadsheets, browse the Internet, and manage e-mail—nothing more. Their loss isn't demonstrative to fulfilling orders, satisfying customers, containing labor costs, creating new intellectual property, or automating business processes. Their perspective is that technology spending isn't *strategic*. So why protect IT?

It is difficult to imagine a business strategy not dependent on IT. Executives committed to IT will not hesitate spending scarce resources to reduce risk to protect IT assets. They will send a clear message that controlling system risk is a strategic priority and that doing so is their *intention*.

Due Care

Management's intention to manage IT risk can be measured by a legal concept called "due care." Due care is a measure of reasonableness. It is the care that a person operating under a similar set of circumstances and information would take if they were confronted with the same problem. It's a legal yardstick that measures the relative competency of a decision in order to determine legal duty or negligence. Due care also speaks to the application of industry best practices as a standard: Management is expected to at least recommend actions required to protect the company's computing environment (Cantrell, 2007).

In some instances, it may be argued that management must take more than a passive interest in information system security to set up firewalls, install antimalware defenses, patch and upgrade their servers, and create acceptable use policies governing the appropriate use of their assets. If a case were brought by a plaintiff before a judge or jury although management did not take any of these appropriate precautions—these "best practices"—then it could be argued that management was negligent in performing its due care obligations to safeguard its IT assets. Management may therefore be found negligent. Since it is the responsibility of management to do these things, and if management *intended* to do nothing, then their competency and intention can be questioned. Such a ruling could lead directly to the award of civil or criminal penalties, or tort rewards resulting from rulings or settlements.

Management's commitment to secure information assets cannot be understated. Not only does our regulatory climate demand that management take a serious and significant interest in protecting their information systems, consumers also expect management to vigorously safeguard the privacy of their personal private information (PPI). It is undeniably damaging when a company makes front-page news because it unintentionally lost or destroyed PPI associated with their stakeholders or customers. There could be civil and criminal penalties for the incident data under municipal, state, and federal government regulations. Therefore, management intention is paramount in demonstrating a commitment to protect PPI.

CRITICAL THINKING EXERCISE

Cherri has just assumed the role of chief operations officer (COO) for a mid-range private company with 250 employees and $25 million in annual sales. It's come to Cherri's attention that her predecessor delegated all matters concerning systems and system security to an internal IT manager. Inasmuch, the systems security process received hardly any executive oversight, and Cherri is unfamiliar with the company's current strategic capability to safeguard its intellectual property.

How has delegating the security problem away from senior management harmed the company's competitive position?

IT GOVERNANCE

IT governance is a term that describes the policies, procedures, and practices employed to manage IT assets. Management is left to govern their IT resources in a manner that they deem fit. Uninterested in reinventing the wheel, though, most companies tend to adopt universally accepted governance models reflecting industry best practices. Fig. 17.3 represents a general model to govern technology assets. Governance models provide a framework for identifying risks, assigning roles and responsibilities for managing those risks, setting broad policy and procedures to respond to those risks, establishing an assessment practice to ensure compliance, and ensuring correct performance. Plus, most management teams would want their practices to be objectively defensible. Implementing a governance model instills credibility; instead of just "winging-it," management can choose to adopt a standard model for handling IT risk.

- Identifying risks: Best practices dictate that management routinely think about risks that threaten their technology assets. There are many ways that assets can be destroyed, stolen, infiltrated, inadvertently shared with unauthorized parties, or lost. Management then identifies the

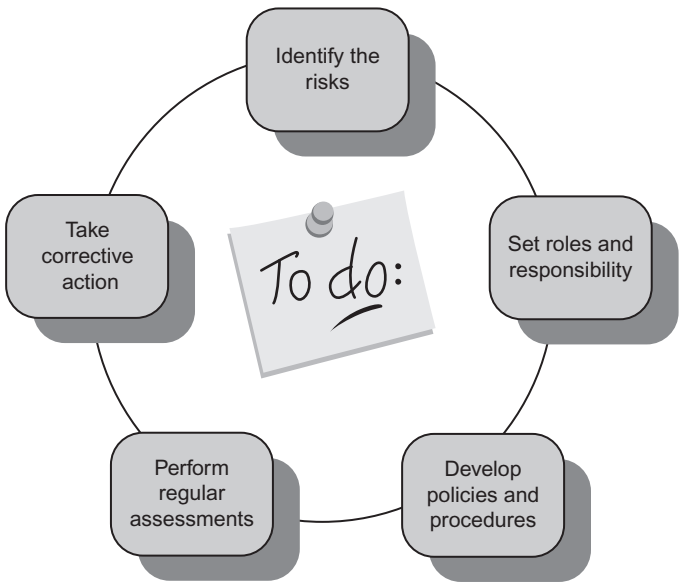


FIGURE 17.3
A traditional approach to tackling information security risks involves a continuous cycle to identify risk, delegate responsibility, implement controls, assess the implementation, and take corrective action. Afterwards, the process starts all over again for risks to information assets are never static.

assets that are at risk and the business processes that rely upon them. From there, management can get a reasonable picture of the consequences related to asset loss. This is a conscious process that attempts to identify and measure risk in terms like dollars, lost time, or threat level.

- Roles and responsibilities: Governance models will deliberately pin accountability on somebody. Stakeholders responsible for implementing and testing governance processes are identified. They have the authority to review practices, update procedures, and take corrective action if practices are out-of-alignment with management's expectations.
- Policies and procedures: Good governance starts with management's intention as codified by policy. Although it's done in various ways, governance frameworks encourage a controlled document management strategy. Those documented expectations then become the baseline for compliance.
- Assessment practice: Good IT governance tries to dispel assumption through forcing an assessment practice. It's not enough to just presume management's intentions are being carried out. Good governance dictates that we've got to audit practice to baseline: Is the company really doing what it says it's doing? These audits can be performed internally through a discipline of self-assessment or conducted by a licensed or authorized third party in the form of an independent assessment.
- Corrective action: Corrective action fixes the gap between expectation and practice. Documented corrective efforts become a means of demonstrating continuous improvement—an ongoing record of management's due care obligation over their IT infrastructure. Under all governance frameworks, corrective actions are identified, executed, tracked, and reassessed to ensure that management's intention is being carried out. A history of corrective action and the steps management took to resolve problems speak loudly about their commitment to best practices and oversight. Corrective action may also become a process to clarify management's intentions, redress policy, and even introduce better safeguards.

IT Governance Models

Governance models are needed for managing a global IT organization to support clear decision-making, oversight, and visibility into what's happening across time zones and continents (Pastore, 2008). Clearly, though, we'd want to ask ourselves: Why reinvent the wheel if we don't have to? Why not select a governance model that fits our business and align our business activities?

There are many IT governance models to choose from. Each has their relative strengths and weaknesses. There is a distinction, however, between commercial models, open models, and public models of IT governance. Commercial models require fees for certification and for conducting the assessment practice which would be independently performed by a well-compensated third party. Open models of IT governance do not require fees for certification. And public models of IT governance reflect best practices as outlined by government agencies or institutions.

According to the IT Governance web site (www.itgovernance.com), "The Calder–Moir framework has six IT governance issues:

IT Strategy
Change
Information & Technology
Operations
Business Strategy
Risk Conformance & Compliance

These are the broad issues that the board and executives need to get right to ensure value delivery, compliance, and risk control in their information systems."

Management may feel it's important to have a third-party conduct audits. Independence has an air of integrity to it, and in some cases, commercial certification may actually be a precondition for securing business with key clients. Other firms may want to smugly proclaim their adherence to stringent business practices to demonstrate their competency with IT security. Yet, on the other hand, some organizations might feel that self-assessment to an "open" model of governance is perfectly reasonable. Finally, if you're going to do business with the government or if you're setting governance standards for your firm, you may feel inclined to meet the data processing expectations of the public sector.

Examples of commercial governance frameworks:

- SAS 70: SAS is a "Statement on Auditing Standards" prepared by the American Institute of Certified Public Accountants, which provides guidance to auditors when evaluating the internal controls of service organizations. SAS 70 is an auditing report and is applicable to the controls placed over the presentation of a firm's financial statements, and also—by amendment—very interested in the role IT plays in securing facts that feed into the financial reports.
- ISO/IEC 27000: This is a series of IT governance and security standards introduced by and maintained by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Examples of open governance frameworks:

- COBIT: These are control objectives for information and related technology that represent a collection of best practices, processes, metrics, and policies created by the Information Systems Audit and Control Association.
- OCTAVE: This acronym (Operationally Critical Threat, Asset, and Vulnerability Evaluation) reflects methods for risk-based information security strategic assessment and planning.
- CMM: The Capability Maturity Model is a trademark of Carnegie Mellon University. It represents a best practices approach to managing software development.

There are several other open frameworks explained on the IT Governance Web site including information on risk management and cloud governance.

Examples of public governance frameworks:

- NIST/Information Assurance: NIST (National Institute of Standards and Technology) sets IT governance standards for the U.S. federal government. The National Security Agency/Central Security Service audits agency adherence to those standards as a practice of "Information Assurance"—a phrase that means information delivered by the federal government can be trusted because its technology infrastructure adheres to best practices ensuring confidentiality, integrity, availability, nonrepudiation, and authorization controls.
- ITIL: The IT Infrastructure Library gives a comprehensive set of published manuals, checklists, and practices for various aspects of IT governance, published by the United Kingdom's Office of Government Commerce.

The matter of which model to introduce into an organization is very dependent on size and complexity of the company, its strategic interest in promoting its compliance activities to vendors and customers, and the degree to which IT is regulated within the company's industry. Generally speaking, small- to mid-range businesses do not have the same compliance expectations as large enterprises. Adopting a self-assessment model like OCTAVE or COBIT, and then modifying it for their own purposes, is a perfectly reasonable course of action for the small business. The enterprise though may deem it absolutely necessary to attest to the highest level of management assurance. Either way, choosing a governance model is a strategic decision that aligns a company's IT management activities to recognized best practices.

No Intent and No Framework Means No Governance

Combined, the lack of intent and lack of a sound IT governance framework means no management control. If management doesn't intend to secure its

IT assets, it won't; policies and procedures won't be created; controls won't be implemented; assessments won't be conducted; corrective action will be nonexistent; and the IT function will be left wholly unattended. In doing nothing, management effectively delegates those security expectations to be performed elsewhere and disavows a strategic interest in managing IT risk.

Importantly, it is not enough to simply provide lip-service to the problem of IT security. If management accepts the need to manage their IT problem, they'd want to implement industry-recognized best practices to govern their resources. And lastly, without the discipline of assessment and corrective action, management would lead purely by assumption: management would assume that their procedures, their threat assessment, their assets, the motivations of others, and the state of technology remain constant and require no further analysis or response from them. And that would be a regrettable mistake. These notions are patently unacceptable and may lead management down a road of ignorance and complacency concerning IT risk. Passive management is almost as bad as no management at all.

THE IMPORTANCE OF TRANSPARENCY

Effective IT governance is more than just implementing a strong procedural mechanism to manage technology risk. Effective IT governance also provides for a way to peer into business processes. Looking back through the data collected by our information system is like cracking open a time capsule. We should be able to look back at the collected assortment of data to witness exactly how we conducted our operations and how we arrived at the decisions we took based on the information we had at the time. The information system should be a window through which we can observe the mechanisms of our business processes and governance decisions.

It is inappropriate, if not impossible, to talk about IT governance without focusing on transparency, writes Steve Romero, IT Governance Evangelist at Computer Associates. The term is used again and again and has become an aspiration for IT organizations that increasingly understand the importance of providing and sharing information with the business. This is critical for the decision-making process (Romero, 2008).

This is the concept behind transparency—or, as Romero calls it, *visibility*. Transparency is a critical facet of regulatory compliance. Regulations that impose transparency upon organizations seek to understand the decision-making that went into securing information assets because it's in the public's interest to know. It is through instruments of law that society deems it necessary and important to force companies to adopt certain standards of IT governance and to routinely demonstrate compliance with such expectations.

Whether or not a company deals with the private health data of patients, the financial records of consumers, or the confidential information of employees and students, the need for transparency and compliance is practically the same. You must—by law—implement best practices and engage actively in managing IT resources.

There are four major pieces of federal legislation that force businesses to enact strong IT governance practices to protect classified forms of information:

- Health Insurance Portability and Accountability Act: HIPAA specifically calls upon those who manage the private health information (PHI) of consumers to set up controls to safeguard those assets. Directly, these organizations and agencies are the doctors, hospitals, insurance companies, clinics, and their business associates who may come in contact with such information. Indirectly, this also includes corporations who must manage the PHI of employees within the scope of administering group medical coverages.
- Sarbanes Oxley Act (SOX): SOX was the political and legislative response to the outrage felt by the collapse of Enron. In an attempt to forgo a repeat of similar excess and fabrication by American firms, SOX compels public U.S. companies to ensure the accuracy of their financial reporting to the Securities and Exchange Commission (SEC). The requirement for transparency has been set on the backs of public American firms through the SOX, and specifically, SOX Section 404 attempts to describe the requirements that must be taken by these firms to safeguard their data assets. The purpose of SOX is to ensure the investing public that the financial statements submitted to the SEC are accurate and reliable. And in the enterprise, SOX noncompliance is simply not an option: SOX represents an expectation on behalf of the public trust and investor relationships. Certainly, given the financial tumbles of recent times, the call for even greater transparency can be likely expected.
- Family Educational Rights and Privacy Act: One of the earliest acts of federal classification of information, FERPA, compels academic institutions that receive federal dollars from financial aid programs to safeguard their students' transcripts.
- Gramm–Leach–Bliley (GLB): GLB was enacted in the midst of the dot-com bubble and attempts to classify the financial information of consumers as a protected form of information. GLB compels those who may possess the financial information of consumers to safeguard the data and prohibits the buying and selling of such classified consumer information.

For reasons both practical and obligatory, large organizations operate in a world of maximum transparency. The public enterprise is accountable to a slew of stakeholders that include consumers, regulatory investigators, financial auditors, and shareholders. This doesn't mean that small- to mid-range businesses are off the hook. There are still a host of regulations that they, too, must abide by. True, small- to mid-range businesses may not have the regulatory pressure to maintain their information systems in a way prescribed by SOX 404. Still, even small businesses are accountable to private investors and to consumers who expect that information assets are properly maintained, safeguarded, and critical information are preserved. Although there is no federal compulsion to regulate the small- to mid-range businesses (note: Cybersecurity Act of 2009), it may only be a matter of time before either voluntary compliance standards are reached or the federal government intervenes to set a common acceptable standard for safeguarding electronic information. It can be reasonably argued that we will continue to operate in a world of increasing transparency and not less. Therefore, transparency is the factor that consistently preoccupies our thinking in these matters.

THREAT ASSESSMENT

Thus far, we've illustrated that management decisions concerning IT assets don't happen in a vacuum. Intention is now paramount, models of governance have been adopted to ensure demonstrative best practices to industry norms, and transparency has become both a requirement and an expectation.

Another principle associated with good security management is threat assessment. Generally, there is an evaluation process for identifying IT assets, identifying potential threats to those assets, determining their vulnerabilities, and implementing reasonable safeguards. To address those vulnerabilities in Fig. 17.4, we see that the assessment process begins with the asset and moves outward to consider a myriad of possibilities that could bring harm to it. This process may also be referred to as a vulnerability assessment or, generally, a risk assessment. Risk assessment is a management practice that identifies the following:

- Assets: Property under the direct control of the IT department would be classified as assets: hardware, software, telecommunications, and databases. Routers, switches, firewalls, and repeaters would also be considered technology assets. Assets aren't just physical things. They're also intellectual property like copyrights, patents, and trademarks, and the data collected within files or databases. The loss of an asset could mean the loss of vital capability necessary for the business to function.

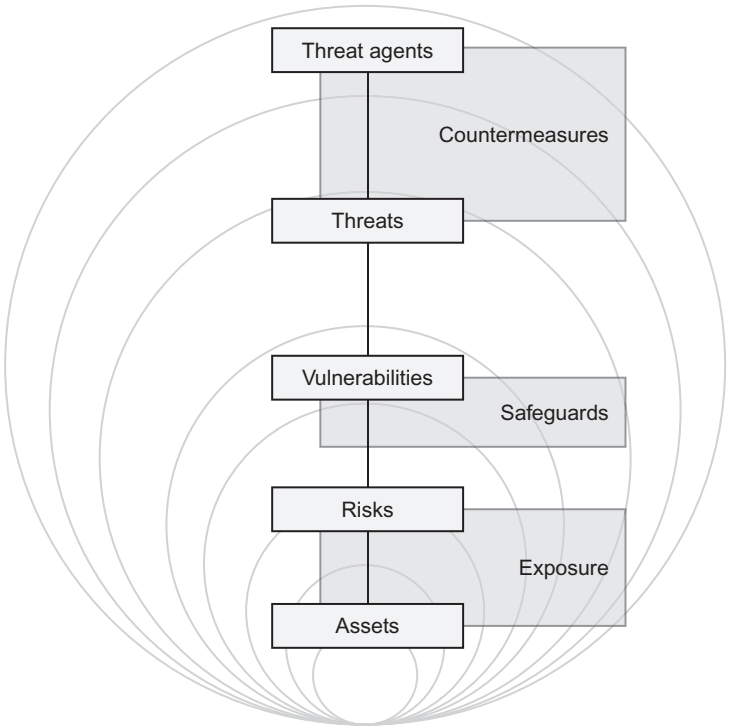


FIGURE 17.4
Threat assessment is an analytical process that works backwards from the asset to consider the degree of exposure should agents capable of exploiting the asset's known vulnerabilities be successful.

- Risk: Risk is the possibility an asset could be exposed to loss, compromise, or ruin. Every one of our assets are under a certain degree of risk. Example: there's an obvious risk of total destruction, whereas there's a less-obvious risk of crippled capability for a limited duration. There's always a risk of a device going down for some random mechanical failure. There is also risk of declassification, unauthorized exposure, theft, penetration, violations of data confidentiality, or system integrity. Each of these risks and their financial/operational impact is distinct. Thus, a reasonable threat assessment practice attempts to evaluate the many threats posed against our IT assets so that we may weigh the cost of loss against the cost of countermeasures and plan for multiple contingencies.
- Vulnerabilities: A weakness in the confidentiality, integrity, and availability of an asset is called vulnerability. Vulnerability may be exploited to incur some of those threat listed earlier. As an example, a microcomputer server is vulnerable to fire, water, electrical discharge

that would fry its components, extreme temperature, and blunt trauma; it's also vulnerable to accidental data loss, sabotage, a programmatic back door, an operating system failure, or unauthorized access. These forms of vulnerability—should they be exploited—could introduce more risk.

- Threats: Threats are the potential conditions under which vulnerability can be exploited. Again, let's consider the microcomputer server. It may be housed in a facility under a threat of hurricane activity. A hurricane could possibly engender vulnerability to water, extreme temperature, and blunt trauma suffered by 130 mph winds. Should the threat be realized, the risk of total destruction is likely. When conducting threat assessments, there is an attempt to identify numerous threats that could exploit various vulnerabilities.
- Threat agents: A threat agent is simply the person or event that would impose the threat. In our earlier hurricane example, we have no one to blame but Mother Nature, so in that case, Mother Nature is the threat agent. In the case of a hacker, though, threatening our assets by hacking them, the threat agent is much clearer. An employee may accidentally fail to close the door that leads into the data center, giving rise to the threat the asset could be stolen, thus making the employee a threat agent. A threat agent could also be a virus, a vendor, or an arsonist.
- Exposure: In an attempt to quantify what would happen if a potential risk occurred to an asset, we try to measure the impact of exposure. By computing the cost of loss and estimating the time the asset would be unavailable provide a measure of potential loss. Measuring exposure in dollars gives management insight for prioritizing prevention and response.
- Safeguards/countermeasures: The controls we implement to secure our information assets are referred to as safeguards and countermeasures. These may be in the form of administrative, technical, and physical controls—(ATP Controls).
  - Administrative controls: Policies, procedures, work instructions, guidelines, standards, and procedures are administrative controls, which explained previously, are elements of an Acceptable Use Policy.
  - Technical controls: These safeguards prohibit unauthorized access, log violations, unauthorized user activity, and unauthorized deletion of data activity. A good example of a technical control is the required entry of a username and password followed-up with group-level permissions that prohibit access to a shared folder of files on a server.
  - Physical controls: Devices and technologies that allow us to prevent the loss, destruction, or theft of an asset are types of physical control. Good examples are a lock on a door, an intrusion detection system (IDS), and a biometric scanner that controls access to a building or room.

It is through the threat assessment process that we might become aware of risks not immediately addressed by our ATP controls. Threat assessments are

very specific to the company, its assets, its business model, and its existing management practices. Yet absurdly, it is quite fashionable for many in the information security industry to suggest that they have a single product, a software, a process, or a solution that secures everything—in the same way—for every company, every asset, from every threat, everywhere. Unfortunately, there is not a magic pill: there's not one single solution, device, software product, or process that can make all technology assets everywhere secure and defend against all risk. This is why threat assessments are so vital. As a practice, they help to move the management team away from assumption to generate an awareness of very real possibilities and dangers unique to their conditions.

ESTIMATING COSTS OF EXPOSURE: QUANTITATIVE VERSUS QUALITATIVE RISK ASSESSMENT

Within the scope of performing a threat assessment, management would be very interested in converting the assessment into something tangible to help them prioritize a response. Tangibility can be expressed in some form of measurement, and generally, there are two means of measuring exposure: to quantify it or to qualify it.

Quantifying Risk

The most common means of estimating exposure is quantifying the costs, time, or loss value associated with an asset's compromise. The process is pretty simple: we take a portion of the value of the asset or the cost of downtime, or that time associated with deficient capability. Some risks may not total the asset but only partially disable it so that it suffers, say, a 30% loss, represented as a proportional cost. This approach typically allows managers who are nontechnical to evaluate risk in terms that they can easily understand (such as in dollars or in lost time), and it's practical in the sense that it converts risk into a tangible numeric figure that makes risk easier to understand, compare, and objectify. However, it is very difficult to place a dollar value on the loss of life or the impact of consumer data compromise on your company's brand and reputation. These matters may be priceless.

Qualifying Risk

We can also use a different means of a valuation based on subjective criteria: high, medium, or low; probable or improbable; critical, common, or rare. After conducting some level of investigation or having entered into a means of collecting opinion from key stakeholders, we may attempt to tabulate and categorize our relative subjective risk. This approach offers an alternative to evaluate risk beyond simple quantification. It attempts to take into consideration the unmeasurable feelings, impressions, or dire consequences.

In reality, it is difficult to say that management makes decisions exclusively of one or the other approach; both are necessary to adequately perceive risk. A reasonable Computer Security Officer (CSO) would be hard-pressed to ignore the qualified opinions of his or her staff. However, it is reasonable to presume that management would find it easier to relate to quantified approaches because it more closely relates to daily decision-making. Expressing exposure as dollars just makes sense to managers. Further, qualified approaches may have a tendency to become bogged-down by consensus, ambiguity, and interpretation. It is for that reason that companies choose quantified practices for more objective quantification of risk.

HOW MANAGEMENT CAN RESPOND TO RISK

To recap, management responds to risk by taking ownership of the systems security problem and through implementing controls to manage it. To govern effectively, management may wish to adopt a preexisting IT governance model to implement best practices to manage its assets and to provide transparency over their decisions. And within the scope of governance is the practice of risk analysis and management's response to justify the costs of safeguards.

Threat analysis is the thread of how well potential risks and failures have been analyzed and then addressed (Ellison, 2006). There should be a close tie between the outcomes of analysis and the requirements of countermeasures to be considered (Ellison, 2006). Thus, threat analysis is the study of threatening forces and mitigating responses introduced by management.

Security managers deal with risk in the following ways:

- Risk Assumption—A risk contingency plan can be developed for the project that defines the actions taken, the resource plans, and the factor that triggers an action should a given risk occur. This option accepts the potential risk and continues assuming the contingency plan lowers the risk to an acceptable level (low cost). Risk Avoidance: We can circumvent the risk by removing the cause or reducing the consequences (some cost).
- Risk Limitation—To limit the risk by implementing specific changes planned activities in the project. (This approach should be pursued when the risk cannot be dealt with any other way or will be too costly to the project.) (some cost).
- "Risk Transfer"—We can transfer the risk by using other techniques to offset the loss. One example would be to purchase insurance. The potential impact of a risk event can be transferred by insuring a product or department against the liability of damage.

- Risk Probability—The likelihood the risk event will occur.
- Potential Consequences—The severity of the consequences on cost or schedule should the risk occur.
  Risk event impact = risk probabilityxpotential consequences.
- Choose the risk elements that have the greatest possible impact on cost or schedule. The risk probability is a number between 0 and 1, and the consequences are expressed in dollars so the risk event impact is in dollars.

Risk Management—Risk management incorporates an understanding of the vulnerability of the project to the consequences of various threats and hazards. The goal is to decrease the exposure of the project to risks through management actions.

Risk Mitigation—Risk mitigation is a systematic methodology; the project team can use to reduce overall operational risk. Risk mitigation can be achieved by applying one or more of the following risk mitigation options: Phase is to have a proven risk management process. This process is a primary deliverable of the planning phase and is kept current until project closeout. The key elements of this process are as follows:

- A centralized repository of risk information and associated documentation of risk items and resolution strategies,
- Summarizing information on a risk type,
- Assigning a member of the project team as risk manager,
- Including a risk summary discussion in the status meetings,
- Providing a uniform evaluation of risk items and risk strategies that includes identifying the risk, evaluating the risk, and defining a resolution strategy.

The procedures for prioritization risk are the following:

- Create a list of about one to five risks with the highest probability of occurring. For large systems, each subsystem may be tracking this number of risk items.
- Determine the following items for each risk:
  - Risk event description—A statement of what might happen in the project.

Chapter 8—Implementation of PPS—Planning Stage 282 Quality Monitoring. There are two basic techniques used in quality monitoring of security projects:

- Cost-Benefit Analysis—Cost-benefit analysis comprises estimating tangible and intangible costs and benefits of various project options, and then using financial measures, such as return on investment or

payback period, to assess the relative desirability of each alternative. The quality planning process must consider cost-benefit trade-offs. The primary benefit of meeting quality requirements is less rework, which can lead to reduced costs, higher efficiency, and increased customer satisfaction. The cost of meeting quality constraints is associated with project quality management activities; so the benefits must offset the costs.

- Benchmarking—By using the benchmarking method, the project team compares both actual and planned practices of the current project against other similar projects performed within their organization in the past or other organizations.

As long as the two projects have related processes with measurable results, the Project Manager will be able to determine the quality success of a project by comparing the two. Risk Monitoring: Another important aspect of controlling a project during the Execution Implementing Physical Protection Systems—A Project Management Guide 281 Scope Control. The Scope Control process is installed to identify and manage the people and requirements of the project that change the project scope beyond the defined need of the original, agreed upon Scope statement. Scope changes arise from someone identifying the need for a change in a project activity or deliverable that may affect the performance or some other attribute of the PPS. In most cases the scope change increases the amount of work needed to produce a deliverable. A scope change is a very vital occurrence and one of the Project Manager's major concerns. Scope Control System: In most cases, scope changes require additional project funds, resources, and time. Therefore, a committee consisting of stakeholders from all affected areas of the organization should be convened to hash out the change and its expected impact on the project. If a decision is made to accept the change and increase or reduce the scope, the change must be documented and signed as a matter of strict scope control. Also, revisions must be made to the planning phase processes and documents such as the WBS and project schedule. The scope revisions need to be explained clearly to the team members and how the change affects their roles in the project. Chapter 8—Implementation of PPS—Planning Stage 280 Status: Usually either unassigned, in process, approved, or disapproved. Resolution/comments: Briefly describe how the scope change was resolved. Change requests are reviewed by a Change Review Board, which evaluates the requests to determine:

- If the changes are feasible in terms of time, resources, costs, and other constraints.
- The impact of the changes on this project or other projects with which they interface.
- If the change should be implemented in the current project or a future project.

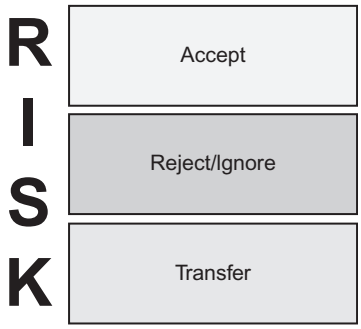


FIGURE 17.5 **Management has four options when dealing with risk: Avoidance (eliminate, withdraw from, or not become involved), Reduction (optimize—mitigate), Sharing (transfer—outsource or insure), Retention (accept and budget) to Accept it, to Ignore it, or to Transfer it.** It's unreasonable to presume that every risk posed to every asset can be financed by management. Instead, managers must make practical compromises based on the threat assessment.

The CRB identifies stakeholders that might be affected by the change and distributes the Change Request for their review. The affected parties each assess the costs and benefits of the proposed change from their individual viewpoints. The Review Board Members combine their assessments and prioritize the Change Request. They accept it, reject it, or defer it to a later time. The Review Board notifies all concerned parties about how the Change Request was resolved.

Fig. 17.5 illustrates the compromises management must make when deciding what to do about risk. Change Fig. 17.5 to illustrate 4 choices.

From FEMA's Building Design Course, "After determining how specific threats potentially impact an asset, the security practitioner can work with security and risk specialists to identify mitigation measures to reduce risk." Because it is not possible to completely eliminate risk, it is important to determine what level of protection is desirable, and the options for achieving this level through risk management. Risk management incorporates an understanding of the vulnerability of assets to the consequences of threats and hazards. The objective is to reduce the vulnerability of assets through various management actions.

Risk Mitigation

Risk mitigation is a systematic methodology used by senior management to reduce overall operational risk. Some risk mitigation options are as follows:

Risk Assumption

To accept the potential risk and continue security operations as they are or to implement basic measures to lower the risk. (No Cost)

Risk Avoidance

To avoid risk, we can take some action to eliminate the cause and/or consequence of the risk (e.g., moving assets to another location.) (Some Cost)

Risk Limitation

To limit the risk, we can implement controls that minimize the adverse impact of a threat's exploiting a vulnerability (e.g., use of preventive, detective, and response controls). (Some Cost)

Risk Transference

To transfer the risk, we can use other options to compensate for the loss, such as purchasing insurance. (Some Cost)

This is management's decision. Management can choose how it wishes to respond to risk. They are qualified to make their own decisions, but all decisions have consequences. The documentation that flows from the systems governance process will commit management to a course of action—permanently. Making a decision and going on record—unlike the other aspects of the risk management processes up to this time—can become highly politicized. Doing nothing, of course, isn't reasonable. Management must do *something*. And to further confound matters, there are some aspects of regulatory controls that could hold either company or the executive *personally* accountable in a civil or criminal fashion. In the face of compelling evidence that a critical asset governing federally protected information is at risk, and a senior officer of a company goes on record and does nothing about it, it could be suggested that inaction was a form of criminal negligence. Fines, jail-time, civil torts, and a career ruined are all within the realm of possibility. Here is where the proverbial rubber meets the road; here, the process will often slip and grind.

Ultimately, though, the decision to accept, reject, or transfer risk is management's to make. The law generally believes management is closest to their own problems and capable of responding to risk in the best way it deems fit. If the decision is considered and reasonable, and proven to be within legal tolerances, then it'd be difficult to question otherwise. But should the case be contended, prosecutors or plaintiffs would present subject matter experts to suggest that—in fact—management's expertise is questionable and their decision flawed, contributing to the outcomes which permitted the risk to occur. Any C-level executive would reasonably consider cautiously their decision to accept, ignore, or transfer risk, and that poses some difficulty to execution.

CRITICAL THINKING EXERCISE

Cherri has just assumed the role of chief operations officer (COO) for a mid-range private company with 250 employees and $25 million in annual sales. Lately, rampant system failures have plagued business operations, and the board of directors have grown increasingly concerned that the process of managing technical risks has been less than transparent. They question the adequacy of the company's threat assessment and mitigation practices.

What are some steps that Cherri can take to increase the board's confidence in her management of the systems problem?

SECURITY MANAGEMENT

Organizational Strategy

Should management accept risk and determine that it's in the interests of the company to directly respond to it, we're now capable of rationalizing expenses to support an internal IT organization.

Increasingly, information systems departments have been tasked with managing security for electronic and digital systems. These organizations are called upon to recruit, hire, and maintain experts in systems security. IT departments are usually responsible for the physical security of data and electronic assets managed within their data center. To some extent, information systems departments have been responsible for the security surrounding telephony, microcomputer networks, and wide area network devices. And over recent years, responsibilities concerning the safeguarding of microcomputer assets and their exposure to untrusted networks have become the unfortunate preoccupation of IT departments almost to the exclusion of all other matters. This makes the practices of systems security somewhat myopic because it excludes other areas of potential risk. An IT department may spend all day fighting viruses, spam, and malware when they should be considering how to secure core intellectual property, or investigating internal fraud committed by employees.

So when not obsessed with the Internet problem, IT departments provide several unique services to the organization related to managing IT security: product evaluation, implementation of safeguards to best practices, engineering, support, audit, and corrective action. Depending on the complexity of the organization, IT departments may feel it appropriate to outsource one or more of these functions as a check-and-balance or as a means to control their costs. This is why outsourcing mundane functions, like e-mail and spam filtering, is attractive to the IT department. Without a doubt, cloud computing offers an opportunity for the IT departments to transfer security risks away from their budgets and to the budget of a vendor.

FIGURE 17.6 Systems management is separated into three layers representing the reach of decision making.

Security decisions made at the operational layer may have an immediate impact that wouldn't last for more than a couple of weeks; tactical decisions may impact an organization for up to a year; strategic decisions could indefinitely enable—or prohibit—the company's ability to execute its business plan.

The internal response to information system security may be a measure of how security is related to the execution of the business plan. IT departments may have a relatively large commitment to information system security if, for example, the business strategy is heavily dependent on proprietary and custom information systems developed from scratch or is totally dependent on unique intellectual property. If that were the case, we may see such a company make investments in each systems management layer, as shown in Fig. 17.6. In this event, security is absolutely essential to the ongoing operations of the business, if not the brand and reputation of the business; public failure in this area is simply not an option. Meanwhile, other companies may choose to outsource system management layers they wouldn't consider to be their competency.

Therefore, in tackling the problem of securing IT assets, management must decide if implementing security will become a core competency. Management may conclude that the internal IT function must be fully staffed, capitalized, and professionally managed and will go about installing all of the roles necessary to protect their assets.

Operational Response to Security

Operational roles may include the engineering, analytical, and support expertise necessary to carry out the governance plan. Operational requirements are

those talents necessary to appropriately select, configure, and deploy technical controls, and therefore, the talent is particularly niched. Should a company perceive system security as a core competency, then it will invest in and retain operational personnel necessary to implement their requirements. Operational decisions are constant and have immediate impact on delivery of IT services and security. The risks of failure are quite high. Misconfiguration of a firewall or a bug in an application's code could expose IT assets to great risk. Operational decisions may be peer-reviewed by other experts so that a double check can be made on the configuration.

Common Operational Questions

- Should the router be configured to allow Port 25 from all inbound traffic from an untrusted network or just a few known IP addresses?
- What's the right network operating system solution to this security risk?
- What levels of permissions should I assign to this user group to allow for read-only access, and how can I monitor whose looking at these files?
- What's the best design goal here for this system: convenience and speed or robust controls to ensure confidentiality?
- What's the best encryption method to use in this situation?

Operational Roles

The Security Analyst

The security analyst performs work similar to the typical systems analyst except the security analyst has a background in information security. The role of the security analyst is to inspect the risks posed to electronic assets, investigate relevant threats and vulnerabilities, and recommend safeguards appropriate to the size, scale, and complexity of the business. Usually, the security analyst will have at least a bachelor of science degree in mathematics, engineering, or computer science, a business or industry background, and technology or industry certifications. The security analyst may not have direct hands-on experience with implementing security countermeasures, and it is not unusual for an analyst to transition to engineering work in the course of their career.

The Forensic Analyst

The forensics analyst is a specialized offshoot of a security analyst who is specially trained to secure electronic evidence for presentation in a court of law. More than just an engineer or an analyst, the forensics specialist has been trained how to handle hardware and software so that they can be legally admissible in the court of law as evidence. The forensic analyst may even have an academic or practical background in criminal justice. The forensic analyst may work internally to an organization and conduct

investigations into employees and vendor activities conducted on corporate assets. Otherwise, he or she could be external talent brought in for unique projects.

The Security Engineer and/or Support Technician

The security engineer is usually an individual who maintains networking and computer technologies. He or she is likely to have a background in network and systems administration, a BS degree, and industry certifications in vendor products. Certification and experience with vendor products provide an edge in the labor market. A security engineer may also have practical experience with securing the network of an organization.

Tactical Response to Security

The tactical response to security management would be to select vendor solutions to carry out the governance plan. Mid-level management would coordinate with vendors and staff to implement security controls that reflect management's intention. Tactical decisions affect commitments under a 12-month timeframe and are likely to meet constraints imposed by the organization's budgeting and forecasting process.

Tacticians oversee operations and carry out strategic direction. This level of decision-making is acutely aware of cost overruns, overcommitments of their resources, and "scope creep." Tactical decision-makers must possess sufficient project management capabilities to allocate scarce resources efficiently. Thus, tactical professionals are highly vested in metrics. Metrics are simply measurements of business processes and outcomes. Metrics measure the company's progress in achieving its objectives and develop a benchmark for assessing progress. Thereafter, the company could compare the results of its progress following its last audit or against comparable industry benchmarks.

Common Tactical Questions

- Are we building the right relationships with our vendors? Are they capable of meeting our strategic goals?
- How well are our scarce resources managed? Are we as efficient and productive as we could be? Is there cost savings or an economy of scale in any of this?
- How are our operational procedures and work instructions aligned with senior management's security plan?
- Do we have the right resources internally—the right staff, training, and talent?

Tactical Roles

The Security Manager

The security manager usually possesses a BS, possibly MS in education. They have a background in managing technology services, perhaps around 10 years in the industry, and specialization in safeguarding electronic equipment and information systems. The security manager is responsible for the analytical and engineering personnel implementing the safeguards prescribed by IT governance policies. The security manager is not a unilateral decision-maker—this is to say they are responsible for implementing the intentions of executive management and aren't necessarily the sole decision-maker concerning security inside of the organization. Inasmuch, they're often in the role of facilitator coordinate human resources (like auditors, engineers, analysts, and consultants) to meet technology and strategic objectives. The security manager may also have a background in project management and is usually an effective communicator. They have to be: They often must reach across the table to negotiate and compromise and to explain complex problems in ways that many people can understand.

The Project Manager

Managing the scarce resources of personnel and capital is something an IT department needs to be very good at. So, it's not out of the ordinary to see IT departments hiring Project Management Institute-certified individuals to help manage the deployment of technology. Project managers serve as a gatekeeper for the limited resources available to IT and help to optimize delivery of services so that they might arrive on-time, on-budget, and with the features that were promised. The project manager is an exciting tactical position in IT because they are generally responsible for coordinating complex problems with a diversity of stakeholders, and the outcomes of important IT projects are very visible. Usually, project managers are groomed for senior management roles because of their ability to communicate, negotiate, and balance the many interests involved in a technology project.

Strategic Response to Security

Strategic planning is very long term—acting on problems that will affect the company for many years. Fundamentally, the strategic problem attempts to look at four conceptual areas:

1. Risk assessment: What are the assets at risk in the organization, their valuation, and the cost of mitigation? How frequently do the risks change and how vital is an assessment practice to execution?
2. Policy: Does the company wish to accept risk, ignore risk, or transfer risk?

3. Execution: Should the company perceive systems security as a core competency and something it should own and do for itself, or should it outsource its security requirements? Is the firm appropriately capitalized?
4. Standards and compliance: Is the company executing its security management strategy under the guise of well-known best practices, and is it meeting its compliance obligations?

Strategic work occurs at a very high level and has little to do with the day-to-day work in the trenches. At the strategic level, executives are very disconnected from the specific technical controls implemented to carry out management's policies; operational control has been delegated to tactical management.

A strategic response to system security may attempt to address the question of ownership: Should the firm own the problem or outsource it? Are standards and best practices being upheld? Should the company take responsibility and own the security function, then invest in talent to manage security? The strategic response may also be the development of a security plan that would complement the technology plan offered by the executive team. Specifically, this plan would outline how spending would relate to strategic security capabilities, how technology plans would become living documents, how to renew threat assessments, and how to change business requirements.

Common Strategic Questions

- What is our risk position anyway? How often is that changing?
- Should we own this security ball-of-wax and spend a bunch of resources on it? What pieces can be outsourced or contained through contracts, Service Level Agreements (SLAs), or defrayed through insurance policies?
- If systems security is to be a core competency—a discipline critical to the execution of the business strategy—how do we manage it? How are other companies or how is our industry managing it?
- If we own it, manage it, and we're spending scarce resources on it, are we doing it well and to the expectations of all stakeholders?

Strategic Roles

The Chief Security Officer

The CSO is a political and specialist offshoot from the chief information officer (CIO). They may have advanced degrees, industry certifications, and decades of information or facility security experience. Traditionally, authority for managing information security would be vested in the comprehensive role of the CIO. However, some organizations may feel it necessary to delegate those responsibilities to a quasiindependent authority who has specialized knowledge of security protocols: It may be that this position already exists to manage facility security issues, too. Politically, should the position not already exist, it may be useful to have an "IT security czar" seen in an internal

advisory capacity to the CEO. The CSO may even have a direct reporting relationship to the board of directors. Such an appointment suggests that security is so very important that the company needs this dedicated senior person responsible for its implementation.

The Chief Security and Compliance Officer

The chief security and compliance officer (CSCO) is a variation of the CSO's function except that this executive is also in charge of compliance activities. Some organizations look at federal regulations like HIPAA and Sarbanes–Oxley as significant obligations that scream for a dedicated executive overseer. Thus, hiring a security professional with a good understanding of the regulatory requirements seems like a strong strategy. These are professionals with decades of experience in security, facilities management, IT, regulatory control, audit and assessment, and managing complex IT projects.

The Chief Privacy Officer

The chief privacy officer (CPO) is a relatively new function that focuses on consumer advocacy inside organizations. Companies have become increasingly aware of the PPI that they maintain concerning consumers. As for their part, consumers have become increasingly interested in what happens to their PPI, and how it is maintained and used by organizations for business intelligence. The manifestation of the CPO reflects a commitment from the board of directors to instill yet another information security czar responsible for tackling the diverse problems associated with consumer privacy and the protection of intellectual property. Unlike the CSO, the CPO is more of a legal expert with an understanding of technology who then applies their expertise toward the privacy problem. Often, this position is responsible for the execution and oversight of privacy policies. The CPO can also be a public spokesperson responsible for communications with the media to communicate and the company strategic position when it comes to securing in maintaining the confidentiality of private consumer information. Organizations would opt to install a CPO to gain favor of stakeholders who'd applaud having a dedicated privacy person aside from the chief executive.

CRITICAL THINKING EXERCISE

Cherri has just assumed the role of chief operations officer (COO) for a mid-range private company with 250 employees and $25 million in annual sales. Concerned that her predecessor didn't spend enough time on systems security issues, Cherri is seriously considering recommending to her CEO to split-off systems security into its own organizational function to be headed by a CSO, or revamp existing practices through adopting better governance practices, or to entirely outsource the IT problem.

What would the strategic, tactical, and operational advantages be for any of these decisions?

INTELLECTUAL PROPERTY

The electronic information system is the lifeblood of the modern company. Intellectual property—be it in the form of copyrights, patents, trademarks, trade secrets or files, e-mail, CAD drawings, or databases—are critical to execution for many businesses. Automated business processes improve the speed, accuracy, and reliability of business functions. They also generate tons of data—another form of intellectual property. Analyzing data associated with business processes may yield intelligence on how to do business better and make effective, consistent decisions. If the organization's business plan is in any way rooted in electronic data processing, then it has a vested interest in protecting its intellectual property and safeguarding it from loss, harm, or theft.

Information security is a critical aspect of any company's *competitive advantage*, just as important as land, labor, and capital, and perhaps even more so given our place in the Information Age. A competitive advantage is described as the processes or capabilities that a company has to perform better than its industry competitors. If the company's arrangement of electronic data processing allows it to perform faster, at less expense, and exceed customer expectations—at a substantially lower costs than others—the company has a real competitive advantage.

ACTIVITIES TO SECURE INTELLECTUAL PROPERTY

Threats to intellectual property are real. Given the degree of risk that all organizations face, securing intellectual property against all manner of threats is an important aspect of managing system security. Internally, IT departments provide functional activities to help safeguard intellectual property.

Education Activities

Especially in combating threats like malware and spam and phishing, the only good defense is a well-educated workforce. IT departments will spend resources training employees on what to look out for and where to turn to for assistance. Education is the front-line in any defensive strategy.

Support Activities

Support activities may include services ranging from call center response for microcomputer support, to analytical reviews, to on-site engineering talent.

Access Controls and Permission Activities

It is the normal course of action for an IT department to set technical controls that restrict the activities of users. These controls are often built into software products and are orchestrated in a way that centralizes administration, so it's easier to manage many aspects of the computing environment.

Verification and Nonrepudiation Activities

IT departments will implement technologies that will confirm a remote party is who it claims to be before conducting business with the party. Controls of this nature would utilize technologies to verify remote access, transmit files, or allow administrative access to sensitive equipment.

Monitoring, Detection, Quarantine, and Deletion Activities

A wide array of software and hardware is used to patrol the network for threats. When threats are detected, suspect data are separated and tagged for administrative review and then eventually deleted. This automation is necessary: IT departments could not possibly monitor all aspects of their network in real time by hand. Instead, automated services are used to assist in "trapping" exceptions so that they can be investigated and eventually dealt with.

Filtering Activities

When connected to a vast untrusted network like the Internet, an incredible amount of time is spent filtering "noise." Filtering forces IT departments to manage rules describing what is and what isn't acceptable behavior on the network. For example, firewalls are filters that prevent questionable traffic from accessing our critical systems, and e-mail filters make sure spam and malware are rejected. Exceptions to filtering rules are always made and must be managed, racking up additional costs on top of the filtering problem.

Intrusion Detection and Prevention Activities

IDS is software or hardware that detects potential malicious activity on a protected asset. It does this by periodically examining system logs and network communications. The IDS scans for activities considered out of the ordinary or suspicious. An IDS is passive and will identify events after-the-fact so that further analysis can be performed and corrective actions taken. An intrusion protection system (IPS), on the other hand, is a more proactive form of intrusion detection that leverages IDS capabilities but responds in real time. Should the IPS detect a potential compromise or suspicious network activity, the device takes immediate action to prevent further compromise by shutting down network resources, paging a system administrator, disabling a running

application, broadcasting system alerts, or literally shutting down the server. The degree of sophistication associated with these solutions is directly related to their cost.

Data Backup, Archive, and Destruction Activities

IT departments are charged with managing information throughout its lifecycle—from generation to eventual destruction—and security professionals play a special role in this process, especially when it comes to managing electronic information. Data backups are the routine functions that copy mission critical data away from production equipment to other forms of media. Data backups and the management of changes made to critical data are a key aspect of recovering from catastrophic loss. In the context of audits, opportunity would be taken to investigate whether not the media had recorded the data as it was intended and may often be the subject of testing and verification—just to make certain processes are operating within tolerance and expectation.

Redundancy Activities

Redundancy has to do with providing duplicative services. In the event of failure, one service might be released in favor of another. Redundancy would often be built into the network design to mitigate the risk of connectivity failures. Redundancy would also be presented in a data processing platform so that a company might cut-over to a backup site should it lose power. Redundancy also includes concepts related to business continuity: installing duplicative systems to offer the greatest guarantee of uptime at a moment of catastrophe or systems failure.

Fault Tolerance Activities

Fault tolerance reflects the engineering decisions used to keep a system working even after a point of failure. A common form of fault tolerance is implemented at the drive controller level for hard disks in the form of a redundant array of inexpensive disks. Other forms of fault tolerance may be implemented at the facility level such as mirror, hot, warm, and cold sites. Fault tolerance may also include the substitution of power from electrical grid in the form of an uninterruptible power supply or a diesel generator.

Media Control Activities

Media control relates to the serialization and tracking of tertiary media that serve as backup for mission critical data. It is a common practice to individually track media as it moves through backup rotations so that losses of media

can be immediately spotted; the loss of media can result in the inadvertent exposure of intellectual property just as a breach and a firewall would. The collection, distribution, rotation, and eventual destruction of tertiary media are a part of systems security management.

Cryptography Activities

Most organizations must handle private, confidential, or sensitive intellectual property. Data encryption is used as a means to secure the confidentiality and integrity of data beyond providing authentication and access controls. Encryption methods can also be used to prove the true identity of an owner/transmitter of information. Organizations that invest heavily in encryption seek to secure data in terms of storage and transmission, requiring specialized engineering talent to deploy and maintain these solutions.

Computer Forensics and Investigatory Activities

Computer forensics is an exciting field concerning security analysis, engineering, and legal procedural knowledge used in collecting and preserving electronic evidence. Electronic evidence may include raw data, photographs, files, log data, network and software parameters, or computer state information. Since electronic information is volatile and subject to tampering, there are established procedures that must be taken to locate, extract, and preserve data so it may be admissible as legal evidence. Such is the domain of the forensic computer analyst. Some organizations may find it necessary to hire and retain their own internal team of forensic analysts to handle serious issues anywhere from employee theft, internal abuses of authority, sexual harassment, to corporate espionage. Electronic forensic investigations may also be necessary to collect information which could later be submitted to law enforcement such as logs from systems that were hacked or compromised. Companies with a vested interest in confidentiality, government work, or maintaining secrets may outright retain a team of professionals to handle such matters internally than involve outside resources.

Change Management Activities

Continuously, incremental changes are made to information systems to improve performance, release problematic computer processes from queue, patch and improve the security of the computing platform, or accommodate the needs of applications. Change/configuration management is an act of electronic record-keeping: If patches are applied to an operating system, we need to retain a record of that change and record the effects of the installation. In this way, management directives can be investigated, and the resulting engineering action that led to a configuration change on a production

system could be logged, repeated, reversed, or investigated. In intensely regulated environments, configuration and change management is an extraordinarily important task that requires electronic surveillance, electronic approval processes, system state preservation, and executive authorization constraints so that even senior management can be held accountable for operational changes. In some cases, it's not only necessary to be able to demonstrate the historical log of changes introduced to a secure platform but to be able to reverse the configuration to any previous point in the life of the asset. This is an extraordinary obligation and engineering challenge: It forces companies to justify and control nearly every update to critical servers, and forces them to implement technologies to return their servers to prior states and configurations. Yet, configuration and change management may be as simple as maintaining a paper log or an incremental backup process that stores the state of the operating system prior to the introduction of new patches and installation of applications.

Documentation Activities

Administering policy documents that govern the information system reflects another ongoing obligation in the security management practice. Policies and procedures are controlled documents: They're numbered and distributed in a way that allows tracking of their publication and receipt by key stakeholders. This way, auditors can be told definitively, "Everybody who needs a copy of this policy has it, and they have the most up-to-date revision." As we've already discussed, the threats posed to information system assets are not static; they are constantly changing within a very dynamic, interconnected environment. This demands constant review and republication of policies, procedures, and work instructions, and assurance that operational personnel are using them.

Assessment and Corrective Action Activities

Finally, the last problem is ensuring compliance: the ongoing auditing and assessment activity to verify operational compliance with management intention. This auditing activity may be conducted by internal IT personnel or an external audit team. Auditors may report to the CIO, or to a CSCO instead of the CIO, or an independent auditing board. In this way, discrepancies in the implementation of management's intention can be reported outside of the chain of command, providing an additional degree of objectivity and independence and credibility of the auditing process. Audits and corrective action would be seen as a normal part of due care. The documentation and the results of the auditing process would return to management as a key tool to assess whether or not policies have been implemented in accordance to

expectation. It also serves as a reasonable way of reflecting the company's dedication to investigating security-related issues and in questioning assumptions over their own practices.

THE RISK OF SCALE

Fig. 17.7 attempts to illustrate the plethora of security challenges facing the modern organization. Who's at greater risk when it comes to the challenge of systems security: the huge enterprise organization or the small mom n' pop business down the street?

Your first instinct may be to suggest the enterprise because the cache of intellectual property is so rich; you could argue that the smaller business has an abundance of less meaningful information and wouldn't make that interesting a target. However, if you look at the small business as a gateway to a larger information system (like a point of sale station is to a company headquarters or from the perspective of a credit card terminal to a bank), then your opinion might change. What are available to the agent are smaller assets that are relatively insecure as compared to the assets of a larger company because the smaller firm doesn't have the talent, motivation, or capital to manage systems security.

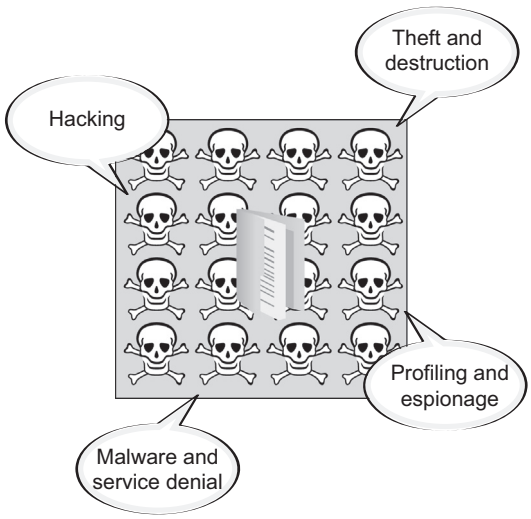


FIGURE 17.7 Information security risks are complex and are constantly evolving.
Smaller companies without a discipline of strong IT governance—without the requisite talent, financing, or culture to manage their information security problems—are the most vulnerable.

Thus, if you're a criminal, why struggle against the toughest ATP controls implemented by teams of knowledgeable professionals when there are far fewer in unregulated, smaller spaces? Isn't it easier to attack a firm that has few controls than one with many?

This is problem of scale and decentralized computing. Small- to mid-range organizations offer a higher degree of risk because they're typically not professionally managed in terms of systems security. Many companies of this size don't understand the risks or the regulatory obligations that are expected of them. Technology consultants who operate within the small- to mid-range community will often attempt to guide businesses toward implementing ATP controls in the same way larger enterprises do. A small business, though, can't possibly keep up with a tight regimen of all the IT functions we've discussed, so they cut corners.

And this puts the entire economy at risk. Small- to mid-range businesses comprise 80% of the total business landscape in the United States. This fact suggests that the very foundation of commerce in the information age is at considerable risk, of which hackers are well aware. However, three potential solutions are on the horizon:

1. Cybersecurity mandates: In addition to the federal classification of sensitive consumer data already in place, federal legislation is under review that would create a mandatory set of IT governance practices that all small- to mid-range businesses would need to adopt and certify against. This way, effective security management becomes just another cost of doing business.
2. Cloud computing: The private sector is responding by offering smaller organizations a way to transfer technology risks away from them and to centralize with much larger companies with a professional security management team.
3. Better engineering: Software, hardware, telecommunications, and databases are being built from the ground-up with security in mind. IPv6 is a great example. This will generally result in better, more reliable commercial products that mitigate exposure and risk to small businesses.

Ultimately, information systems security will become—for the most part—*ubiquitous*, and integrated into broad categories of system design. That doesn't mean security becomes a nonissue, and it doesn't mean that clever people who want access to our private intellectual property won't figure out a way to defeat our equally clever safeguards. We shouldn't naively believe that we've eliminated all risk from our operations. On the contrary, our role as information systems managers is to implement reasonable, cost-effective

controls governed by strict adherence to industry best practices as a means to *deter* threats. Certainly, better engineering, system tools, regulatory intervention, and practices like cloud computing will help in that effort, but in the end, success boils down to how well we manage the problem of information system security.

CRITICAL THINKING EXERCISE

Cherri has just assumed the role of chief operations officer (COO) for a mid-range private company with 250 employees and $25 million in annual sales. Just weeks into her new role, Cherri made significant improvements to the company's security posture and satisfied her Board of Director's immediate inquiries. However, Cherri looked at her immediate actions as of late as being just one step in a larger process toward increasing stakeholder confidence. Now's not the time, she feels, to turn away from it and hope the problems will get better.

Why do you think managing systems security never begins nor ends with a single project? Why is the systems security problem enduring, pressing, and ongoing?

REVIEW QUESTIONS

1. What is the relationship between systems security execution and management's intention?
2. How does the principle of due care relate to management's security decisions?
3. In your judgment, what is the largest threat to corporate intellectual property? What are some activities system managers can take to counter that threat?
4. How does a threat assessment expose and identify risks to company assets?
5. How do regular audits and corrective action ensure systems security?

S.773 THE CYBERSECURITY ACT OF 2009

The U.S. Congress recognized the importance of creating common criteria for assessing information technology risks for the public sector, particularly with small business. It reasoned that if we're to have an economy based on information and electronic commerce, then reasonable and specific precautions must be taken by all in order to strengthen national defense, national competitiveness, and national security. This piece of legislation — as to the time of publication — hasn't been implemented. It would create an IT governance expectation to NIST (National Institute of Standards and Technology) practices that all private institutions must live by. It creates regional cybersecurity centers to help implement and certify governance practices; it sets aside dollars for education grants and scholarships; it creates a specialized certification program for independent

(*Continued*)

(Continued)

auditors; it calls for a stronger DNS (Domain Name Service) system to prevent attacks; and it calls for the creation of a national dashboard to measure cybersecurity threats. To some, this may seem an invasive approach by the government to mandate best practices and good IT governance procedures to all U.S. businesses, but at the same time, if standards and obligations aren't set, then there will exist a legitimate risk to macroeconomic security. In an information age, we must trust our information systems. S.773 would compel business owners to adopt reasonable governance controls to ensure the confidentiality, integrity, availability, and transparency of their electronic assets.

What Are ATP Controls?

ATP controls are implemented to secure the confidentiality, integrity, and availability of information system assets — a concept known as CIA. Confidentiality refers to the idea that only authorized individuals should have access to information; integrity refers to the idea that what the system reports is true and factual, that we can trust what the system is telling us; availability refers to the idea that the information system needs to be available to the right person, at the right time, and at the right place in order to help with making a business decision. If any one of these dimensions are breeched, then we would say that the security of the asset has been compromised. It is important to note that ATP controls are the result of the risk analysis process, and they're not just arbitrarily doled out.

Core Competency and the Cloud

Arguably, managing complex technology assets isn't a core competency for many small- to mid-range businesses. They don't have the necessary staff, expertise, or capabilities to govern their electronic information system to the greatest extent possible. Cloud computing is a model for providing technology services directly from service providers who've a presence on the Web. Instead of running applications on local servers, companies would instead store data on the vendors' server; instead of managing the security of these applications, the vendor would manage it. This model of data processing represents an opportunity for the small business who could spend more time doing what they're good at rather than wasting resources on things they're not; meanwhile, the vendor is exceptionally good at managing information systems and has an army of people to manage the data for hundreds of thousands or millions of customers. Organizationally, cloud computing transfers some operational requirements away from the business and to a service provider; tactically, services can be acquired faster with much smaller up-front dollars on year one; strategically, cloud computing gives companies the chance to move the risk of running technology away from them.

The Technology Plan

The technology plan is a living document — a document that changes quite regularly — that outlines how spending on technology will help the business achieve its strategic objectives outlined in its business plan. Just as the financial plan is prepared by the chief financial officer, and the operations plan is prepared by the chief operations officer, and the technology plan is prepared by the senior officer in charge of technology spending and coauthored by positions like the CSO, CSCO, or CPO. Like those other strategic documents, the technology plan tries to draw a line between spending, broad strategies, and desired outcomes. It helps explain where the company will be investing its resources to gain capabilities. Naturally, this document has to be quite flexible. Technology changes all of the time. It's not uncommon to see the

(*Continued*)

(Continued)

technology plan undergo annual revisions. It's also a political document in that it helps explain how spending scarce resources on technology will meet the company's needs.

The Role of Certifications

Certifications, or "certs," are vendor-sponsored technical assessments that demonstrate a measurable level of competence with their products. Certified-technicians can command higher wages, qualify the professional for a position demanding particular skillsets, or justify a promotion. In addition, hiring managers can look at the curricula associated with the certification and assume that the potential job candidate does, in fact, have the technical skillsets they're claiming to have. Certifications also provide a great way to encourage employees to improve their skills with the latest technologies. Certifications also offer a degree of political clout: if an organization is able to say that it has x-number of CCNA's on staff, then it is able to argue that it has made a significant commitment to securing Cisco devices used in their operations. This fact may look potentially attractive to stakeholders who feel the execution of the business plan depends on qualified personnel.

Why are Assessments and Corrective Action Important?

Think of a company that installs a firewall. Every company that wants to interact on the Internet needs to set up filters to protect their trusted assets from the untrusted space they can't control. A firewall is a reasonable precaution. Upon configuring the firewall, several assumptions went into its configuration and placement on the network. Ports were left open and pointed to specific internal IP addresses as to allow the business to continue to conduct business activities. Passwords were set. Access controls were introduced. Now, within four short months of its installation, IP addresses may be reassigned, the organization's needs may change, new vulnerabilities may be released that exploit the ports that were opened, and a new critical software update for the firewall's IOS may have been released by the manufacturer. If the company's attention is elsewhere, then they're managing the firewall under the same assumptions they had 4 months ago — which may be entirely inaccurate. A successful audit and corrective action practice would review the assumptions behind the firewall and compare them to current requirements. Corrective action could be taken to reduce the attack surface of the firewall. Instead of managing security by assumption, we manage security by fact, and management can demonstrate a strong response to their due care obligation.

References

Anttila, J., 2006. Senior Executives Commitment to Information Security—From Motivation to Responsibility. www.qualityintegration.biz/GuangzhouC.html (accessed 27.03.10).

Cantrell, B., 2007. Due Care in the Computing Environment. www.giac.org/resources/white-paper/law/142.php (accessed 27.03.10.).

Ellison, R.J., 2006. Security and Project Management. Carnegie Mellon University, https://build-securityin.us-cert.gov/bsi/articles/best-practices/project/38-BSI.html (accessed 27.03.10.

Pastore, R., 2008. CIO: Models for Global IT Governance. www.cio.com/article/191700/Models_for_Global_IT_Governance?page=1&taxonomyId=3154 (accessed 27.03.10).

Romero, S., 2008. Transparency or Visibility: Can the Business See Through You? http://community.ca.com/blogs/theitgovernanceevangelist/archive/2008/08/26/transparency-or-visibility-can-the-business-see-through-you.aspx (accessed 27.03.10).

Further Reading

FEMA Building Design for Homeland Security. http://www.fema.gov/media-library-data/20130726-157-20490-6000/suburban_ig_combined_12_2008.txt (accessed 27.10.16).

IT Governance, http://www.itgovernanceusa.com/ (accessed 31.10.16).

CHAPTER 18

Substance Abuse

What You Will Learn

- Why employers conduct drug and alcohol testing.
- The role of the CSO in enforcing a company's drug and alcohol abuse policy.
- The mechanics of drug testing by urinalysis and of alcohol testing by blood alcohol concentration.
- Intervention by supervisors when drug and alcohol use is indicated.
- Reasonable cause for drug and alcohol testing.
- How to conduct coordinated investigations.

INTRODUCTION

Let us agree at the outset that substance abuse means the abuse of both drugs and alcohol. Let us also agree that drug abuse means the use of illicit drugs, that is, drugs that are prohibited by law to use, such as heroin and marijuana, and the use of legal drugs in a manner not prescribed by a physician or recommended by the drug manufacturer. And for the purpose of this discussion, we will agree that alcohol, which is legal to use, is abused when it is consumed in violation of the employer's work rule such as use immediately before reporting to work and use on the job.

Why is substance abuse a concern of the employer, and by extension, to the Chief Security Officer (CSO)? The reasons are many and simple. Substance abuse causes the following:

- Absenteeism, which lowers productivity and shifts the burden of work to nonabusing employees.
- Mental and physical lapses that result in poor decisions, wastage of materials, and accidents that injure and kill.
- Damage to the health of abusing employees, which drives up the employer's medical benefit costs.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00018-9

- Higher rates of employee turnover. According to the 2000 survey by the Substance Abuse and Mental Health Services Administration, substance abusers were more likely to have had three or more employers in the past year.
- Damage to the morale of the nonabusing employees and friction between the abusers and nonabusers.
- Problems in supervision that divert the attention and time of managers.
- Loss related to employees who steal to support their habits.
- Damage to the public image and reputation of the organization.

According to Ferraro (2006), once abusers of illegal drugs have exhausted their discretionary income, they buy their drugs on credit. Once credit is exhausted, they typically deal or steal. The abuser who deals is likely to sell drugs at work. The abuser who steals is likely to steal from the employer or the employer's customers and vendors.

ROLE OF THE CHIEF SECURITY OFFICER

What does all this have to do with the CSO? The connection is the role of the CSO in carrying out the employer's substance abuse policy, which typically prohibits the use, possession, and transfer of abused substances on company premises or while conducting the company's business. Enforcement of this prohibition largely falls into the security purview. Also specified in a typical policy is a requirement to investigate violations of company policy and cooperate with police and prosecutorial authorities in the investigation of drug law violations. Translated into tasks or duties, the CSO ensures the following:

- Workplace inspections are conducted.
- Abuse substances and paraphernalia prohibited by the policy are confiscated, stored, marked as potential evidence, and disposed off in the manner required by law.
- Violations are investigated, and recommendations are made for preventing the same or similar violations.

In addition, the CSO may be tasked to evaluate compliance to policy in the matter of the company's drug and alcohol-testing program. The questions that management may want the CSO to answer include the following:

- Are fairness and nondiscrimination present in the practice of selecting the employees to be tested? If random selection is specified, is the selection process truly random and free of suggestions to the contrary?

- Are the test specimens (e.g., urine for drugs and breath for alcohol) collected in a manner that provides a reasonable degree of personal privacy yet prevents contamination, switching, or mislabeling?
- Are test specimens transported tamper-free and with attention to chain of custody?
- Are test results distributed on a need-to-know basis, and are they given the same or higher level of protection given to medical information?

Even small deviations from the standards of a testing program can cause large problems, and if the CSO is charged with discovering deviations, he or she must have a grasp of testing program fundamentals. One of the recurring problems is with chain of custody, a set of procedures well known to law enforcement but not to collectors of test specimens. Chain of custody requires an identification of the specimen, the name of the person who collected it, from whom it was collected, to whom it was next given, and the date, time, and purpose of the transfer. This process of transfer continues throughout the testing process and concludes when the specimen is no longer needed, at which time it is finally destroyed. A form called the chain of custody accompanies the specimen from beginning to end and records the pertinent information. A properly conducted chain of custody will obviate a challenge as to the possibility the specimen was altered by an unknown person who came into custody of the specimen.

TESTING FOR ILLEGAL DRUGS

Drug testing seeks to identify in a person's body the evidence of illegal drug use. (Note: The meaning of the term "illegal drug use" includes the use of legal drugs that have not been prescribed or have been taken contrary to a prescription.) The most common method of drug testing is the analysis of urine. The individual to be tested is asked (not compelled) to provide a urine specimen. Fig. 18.1 depicts a job applicant submitting a urine sample for testing.

The specimen is collected in a manner that prevents cheating and error. The integrity of the specimen has to be unquestionably reliable. Any indication of contamination, switching, or mislabeling will render a test result invalid. To assure reliability, a chain of custody form is signed by every person who handles the specimen from collection until final destruction.

A specimen is carefully packaged and quickly transported to a testing lab, where it is analyzed for the presence of illegal drugs. The illegal drugs most often of concern to employers are cocaine, marijuana, opiates, amphetamines, and phencyclidine (PCP).

FIGURE 18.1
Drug testing of job applicants is a common business practice. *Burns International Security Services.*

Drugs and alcohol are tested in certified laboratories. The testing methodology for drugs is analysis of urine specimens. The methodology usually follows a two-test approach. The first test is called a screening test. If no drugs are found in the screening test, the specimen is not further tested and is declared negative. If a drug is found in the screening test, the specimen is tested a second time using a different and more sensitive technique. The second test is called a confirmatory test. If the confirmatory test fails to validate the first test, the specimen is declared negative; if the confirmatory test validates the screening test, the specimen is declared positive. Fig. 18.2 shows a technician conducting a test for illegal drugs.

In some programs, a positive report is forwarded to a physician who evaluates the report in light of information about the individual. The information may come from what the individual says and/or what a medical examination reveals. If there is any reliable indication that the positive test resulted from something other than illegal drug use, such as the proper use of a prescription drug, the test is declared negative.

Almost all testing programs provide opportunities for challenging positive test reports, including the right to obtain a retest by the same or equally competent laboratory. Some programs have treatment and return-to-duty

FIGURE 18.2
Drug testing is performed with highly reliable and accurate scientific methods. *Burns International Security Services.*

provisions, and almost all organizations that conduct drug testing assist employees by identifying treatment resources in the local community.

Denny (2008) says that his experience in filling job positions is that, all too often, candidates at every level try to beat drug tests, and when they are successful, the consequences can be devastating.

ALCOHOL TESTING

Alcohol is not an illegal substance. However, an employer has the right to exclude alcohol from the workplace and to prohibit alcohol consumption while at work. Also, the employer will usually make it a violation of policy when an employee arrives at work under the influence of alcohol. The degrees of influence are presented below.

A test for alcohol measures the concentration of alcohol in the blood. Blood–alcohol concentration (BAC) is the relative proportion of ethyl

alcohol within the blood, based on the number of grams of alcohol per milliliter of blood, expressed as a percentage. In a BAC test, blood alcohol zones are the measures of intoxication. Three zones are commonly used:

- Zone 1 includes blood alcohol values from 0.00% to 0.05% and is considered fairly good evidence that the person is sober.
- Zone 2 ranges from 0.05% to 0.15% and is inconclusive as to whether or not the person is under the influence.
- Zone 3 relates to findings above 0.15%. At this level, a person is considered to be intoxicated. Its equivalent is to drink 8 oz of whiskey or eight 12-oz bottles of beer.

Fig. 18.3 depicts an individual breathing into an alcohol testing device. The testing specimen can be breath, blood, or urine. In the breath testing technique, a sample of deep-lung breath is collected from the subject's air output and held captive in a device that measures hydrocarbons.

Hydrocarbons will be present in the deep-lung breath of a person who has recently consumed an alcoholic beverage. However, an exaggerated reading can occur if in the 15-min period immediately preceding the test, the subject consumed or regurgitated alcohol. Thus, a 15-min waiting period before testing is recommended to guard against an exaggerated reading.

A consent form signed by the individual demonstrates willingness to be tested, whether for illegal drugs or alcohol. Fig. 18.4 is a sample consent form.

FIGURE 18.3
A test of breath is usually a screening test. *iStockphotos.*

The Drug Recognition Process

Report 221 of the National Institute of Justice offers an alternative to urinalysis called the drug recognition process. It is a systematic, standardized evaluation based on a variety of observable signs and symptoms that are known to reliably indicate drug impairment. A conclusion that impairment is present must be based on the process as a whole, not on any single element. The process is considered standardized because it is conducted in the same way for every person.

The recognition techniques of the process include evaluation of specific physical and behavioral symptoms, such as eye movements and their appearance, certain body gestures, slurred speech, and poor physical coordination. The drug recognition process will indicate if a person

- Is currently under the influence of a drug or drugs.
- Has used a drug or drugs within the last 3 days.

CONSENT FOR DRUG AND ALCOHOL TESTING

Employee Name: _____ **Test Date:** _____

Social Security Number: _____ **Department:** _____

Employee Start Date: _____ **Supervisor:** _____

I understand that I am not obligated in any way to take a drug and/or alcohol test administered by my employer.
I hereby freely and voluntarily agree to take a drug and/or alcohol test administered by my employer
I also understand that the results of the drug and/or alcohol tests taken by me will me made available to my employer and others having the right by law or regulation to have access to such test results.

Signature: _____ Date: _____

FIGURE 18.4
A drug or alcohol test requires consent.

The indicators looked for in the drug recognition process are the same as those described in intervention, which appears later in this chapter.

EMPLOYEE AWARENESS AND COOPERATION

A primary component of substance abuse prevention is an awareness program designed to inform employees that substance abuse adversely affects all employees, and that acceptance of and cooperation with the program is not open to negotiation. Bomba and Deming (2005) make the point that the concept of "security awareness" is primarily a state of the mind. It is not the same as training or education but is definitely related to both.

An awareness program can include the following:

- Making employees aware of the negative consequences of abuse.
- Influencing employees to steer away from personal abuse.
- Encouraging abusers to seek treatment.
- Intervening when coworkers are observed using illegal drugs or alcohol on the job.
- Reporting violations such as coworkers performing safety-sensitive tasks while under the influence and the possession or distribution of illegal drugs or alcohol on the job.

Responsibility for administering a substance abuse awareness program is often shared by the human resources, safety, and security groups. The focal points for Human Resources (HR) include the disciplinary consequences of violations, employee assistance, rehabilitation, and return to work. The safety group has an interest in accident prevention, and the security group is concerned with keeping prohibited substances out of the workplace, detecting violations, conducting investigations, and coordinating security group efforts with local law enforcement. An effective program should be:

- A centerpiece of the organization's overall substance abuse policy. The program should be an integral standard that applies to every employee, without regard to the employee's status.
- An ongoing effort. Although the education program may be initiated with great fanfare and periodically reinvigorated, it must be a continuously operating enterprise.
- Oriented to the particular (and often changing) needs of the business. The effort should be principally dedicated for making employees aware of their individual responsibilities for maintaining a workplace free of drug and alcohol abuse.
- Innovative in awareness methods and approaches.

The CSO's contribution to the awareness program can be as follows:

- Brown-bag luncheon meetings at which employees view films, slides, PowerPoint presentations, and other audiovisuals. Having a subject matter expert on hand to supplement the presentation and answer questions adds credibility. A law enforcement officer, for example, can display paraphernalia used to administer commonly abused drugs, and a medical practitioner can explain the health consequences of abuse.
- Company-sponsored publications, such as newsletters and bulletins. Each newsletter issue, for example, can include a drug-related article. Hard-copy materials that reach the home may help promote family involvement in preventing or resolving substance abuse problems.
- Tutorials that meet special needs, for example, teaching supervisors how to look for prohibited items and how to intervene when abuse is suspected.
- Awareness materials on the company's general intranet, on the security website, on placards in public hallways, and on signage at safety-sensitive locations. Other materials might be a company-prepared handbook, posters in hallways, and fliers placed inside paycheck envelopes.
- Awareness events such as a security fair that features display booths, literature handouts, video presentations, and talks by local celebrities.

Employee awareness is an essential component of the organization's substance abuse prevention program. Other program components, such as supervisory intervention, drug testing, and employee assistance, rely on an informed workforce. Supervisors cannot step in to correct abusive situations if they have no understanding of abuse, drug testing will not be fully accepted by the workforce if the why and how of drug testing are not thoroughly explained, and employees will shy away from seeking or accepting employee assistance benefits if they are unsure of implications.

CRITICAL THINKING EXERCISE

Danny Abbott works the early evening shift as warehouse forklift operator. A few hours before he is due on the job, Danny is at a friend's home. His friend lights up a marijuana cigarette and offers to share it. Danny, who is no stranger to marijuana, hesitates for a moment.

Danny recently attended a company meeting on the subject of drug abuse. The main speaker was the company's CSO, who said that company work rules prohibited employees from being at work while under the influence or with a detectable amount of an illegal drug in the body system. The reason for the rule had to do with accident prevention and, as Danny knew, his own job as forklift operator required strict attention to safety. Danny was particularly impressed when told the company was instituting unannounced and random drug testing of employees in safety-sensitive jobs. Danny's friend takes a long drag from the marijuana cigarette and extends it to Danny.

Assume that Danny is an office clerk, and not a forklift operator. Should he be exempt from drug testing?

INTERVENTION

Supervisors are the backbone of substance abuse prevention. Active involvement of supervisors in enforcing the company's drug abuse policy and procedures is essential to maintaining a drug-free workplace.

Fig. 18.5 is an example of intervention by counseling. Intervention is actively looking for violations, and when seen, taking action. Depending on the supervisor's judgment, such as the employee's productivity and longevity, the intervention can consist of counseling, giving a verbal warning, or issuing a letter of admonishment. However, in some companies intervention along these lines is not allowed. The supervisor must refer the violator to a direct report or the HR department, where corrective measure is determined. The corrective action can be a written report placed in the violator's file, suspension, or termination.

Reasonable Cause Testing

A follow-up to supervisory intervention can be immediate testing. However, the testing must be based on reasonable cause. The word "reasonable" means that a good-faith belief the incident requires intervention. To make a test under the reasonable cause rule, the alleged violator has a right not to

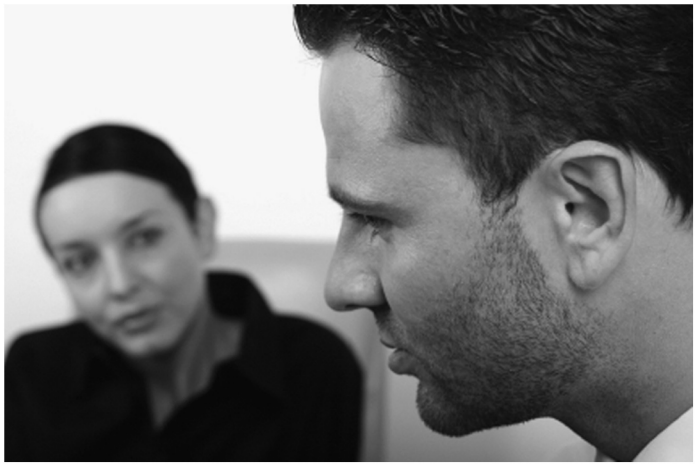


FIGURE 18.5
A supervisor counsels a violator.

consent to the test, in which case company policy can require suspending the violator and reporting the incident to a higher authority. Also under the reasonable cause rule, or at any time a violation is observed, the supervisor should complete a report of the incident in full detail. Make a note of the incident in full detail. Fig. 18.6 shows a checklist that can be used to complete the report of a Reasonable Cause Incident. A sample report of a Reasonable Cause Incident.

A reasonable cause test should be done as quickly as possible to preclude natural diminution of the drug or alcohol in the body system. The supervisor should obtain a urine sample at the scene for suspected drug abuse and capture a deep-lung breath in an alcohol testing device for suspected alcohol abuse. Some companies prefer running a swab through the alleged violator's mouth and placing the swab in a contamination-free container such as a capped medical vial.

The alleged violator's conduct leading to reasonable cause can be, and should be when possible, witnessed. If there are no witnesses, the supervisor should ask another supervisor to witness the conduct that merits reasonable cause testing.

Another step under reasonable cause testing is to search the alleged violator but again with consent, in writing, if possible with a person witnessing the signature.

The term unreasonable is applicable when there are no facts that would lead a prudent person to believe that evidence of an undue influence does not exist or when the supervisor violated the alleged violator's rights. In the latter, an example would be a nonconsented search of the employee's locker for the purpose of finding anything that could be used to incriminate the employee. This type of search is unreasonable because it is a type of fishing expedition.

The following are the questions that the supervisor must ask himself or herself:

- Are the facts reliable? The supervisor can consider the facts of a situation to be wholly reliable when they have been witnessed by him or her, a reliable employee with follow-up confirmation by the supervisor, or another supervisor.
- Are the facts explainable? A decision to conduct reasonable cause testing must be supported by specific details that can be explained. For example, it would not be sufficient to say that an employee appeared to be under the influence. An explanation would need to include details of the observed impairment such as "the employee was staggering and his speech was slurred."

REPORT OF REASONABLE CAUSE INCIDENT

Name of Individual: _____

Time and Date of Incident: _____

Place of Incident: _____

Brief Description of the Incident

_____

_____

_____

_____

_____

The Individual's Appearance Was:

[ ] Normal	[ ] Sleepy	[ ] Hyperactive	[ ] Tremors
[ ] Bloodshot Eyes	[ ] Runny Nose	[ ] Pale	[ ] Flushed
[ ] Staggering	[ ] Uncoordinated	[ ] Glazed Eyes	[ ] Dreamy
[ ] Nervous	[ ] Confused	[ ] Sweating	[ ] Unkempt

[ ] Other specific details of appearance, including odors:

_____

_____

The Individual's Conduct Was:

[ ] Normal	[ ] Loud	[ ] Abusive	[ ] Disruptive
[ ] Erratic	[ ] Violent	[ ] Giggling	[ ] Rapid Talking
[ ] Mood Swing	[ ] Wandering	[ ] Argumentative	[ ] Sleeping
[ ] Destructive	[ ] Belligerent	[ ] Irritable	[ ] Passive

[ ] Other specific details of conduct:

FIGURE 18.6
This form can be used when documenting a Reasonable Cause Incident.

What the Individual Said or Did

Overall, the Individual Seemed:

[ ] Unable To Function [ ] Unsafe To Be Around [ ] Under the Influence

Comments

Specimen Collection

After being informed that providing a specimen for laboratory analysis to determine the presence of alcohol or drugs was a voluntary act, the Individual:

[ ] Voluntarily Provided a Specimen [ ] Refused to Provide a Specimen

Name of Person/Agency That Collected the Specimen: _____

Time and Date of Specimen Collection: _____

Time and Date Specimen Was Forwarded to Lab: _____

"We, the supervisors or managers whose signatures appear below, have determined that reasonable cause exists to believe that the Individual named in this incident was impaired by or under the influence of alcohol or a drug or drugs at the time, date and place indicated, and that testing for the presence of alcohol or drugs is justified by the circumstances."

Signature _____ Time and Date _____

Signature _____ Time and Date _____

FIGURE 18.6
(Continued)

- Is the impairment present now? The supervisor has to be sure that the suspected impairment exists at the moment the decision is being made. There are two good reasons for this: first, the test will most likely be negative if the influencing substance has diminished, and second, it would be unreasonable to require a person to take a test based on suspected past impairment.

Reasonable cause testing should not be authorized unless facts clearly point to impairment resulting from the use of alcohol or drugs.

Consent to Test

Under this concept, which carries the force of law, no person may be compelled to provide specimens. An employer, however, has the right to terminate an employee who refuses to provide a specimen when requested to do so. The employer's right must be supported by prior notice to the employee that consent to test is a condition of employment. If the consent cannot be shown to exist, consent should be obtained immediately. If the employee refuses to give consent, termination may follow.

Search with Implied Consent

A search with implied consent is a search conducted as a condition of employment or as a part of an employment contract. Conditions of employment and employment contracts frequently express or imply consent to search employees and their belongings.

The rationale for implied consent searching is based on preventing an injurious outcome that can be reasonably expected to occur in the absence of a regularly conducted search program. An injurious outcome could be an explosion or fire in the workplace. The search program would be justified because of the need to ensure that ignition devices are excluded from the workplace. The same can be said for excluding impaired workers whose judgment or lack of motor skills might contribute to an explosion or fire or might detract from the proper emergency response.

An implied consent search is more like an inspection than anything else. It does not rely on reasonable belief; there need not be an accident, an incident, or a set of suspicious facts for the implied consent search.

Looking for the Indicators

Observing people at work is a natural supervisory activity. Although the act of observing is natural, so is the human tendency to not always understand what is seen. In familiar surroundings, such as where we work, we tend to

overlook the obvious. The indicators of abuse will not be seen when a supervisor does not consciously look for them. And even when there is a conscious intent, the discovery is difficult because the indicators are often carefully masked and easily mistaken for other things.

Observation works best when planned and deliberately carried out. Preparation includes determining where and when to look, knowing what to look for, and making a record of the findings. The process is enhanced when the supervisor predetermines the area to be looked at and considers the operations performed in the area selected for inspection.

Knowing where to look has to be supplemented with knowing what to look for (i.e., the evidences of use). Planning a walk-through would involve an itinerary for inspecting restrooms, employee break and changing rooms, trash receptacles, stairwells, and parking lots. These are the places where a supervisor may find discarded items such as glassine envelopes that once contained marijuana or cocaine, plastic vials that contained crack, empty adhesive tubes and paper bags that were used for glue sniffing, butt tips from marijuana cigarettes, and soiled paper towels that were used to clean residues from marijuana, hashish, and crack pipes.

Indicators of Abuse

Indicators of abuse fall into three categories: performance, behavior, and general indicators.

Performance Indicators

- Frequent no-shows and lateness. Examples include not showing up for work on Fridays and Mondays, and repeated lateness in arriving at work.
- Unexplained absences from the assigned workstation.
- Frequent and long visits to the restroom or locker room.
- Visits to the employee by strangers or other employees for matters unrelated to the job.

Behavior Indicators

- Unexplained change in disposition in a short period of time. The employee may go from being uncooperative to cooperative, from quiet to talkative, from sad to happy. The reason may be that the employee took a drug between the "down" mood and the "up" mood. If the mood swings in the opposite direction, it may indicate that a drug is wearing off.
- Weight loss and loss of appetite.

- Nervousness that might appear in the form of starting to smoke or increasing a smoking habit.
- Reluctance to show the arms or legs. If an employee is taking drugs intravenously, he or she will try to hide the injection marks by wearing long-sleeve garments and wearing slacks in place of skirts and dresses. Blood spots on pant legs and sleeves may appear.
- Withdrawal symptoms. The employee may show the physiological effects of a drug as it is wearing off. The common symptoms are runny nose, sniffling, red eyes, trembling of hands or mouth, unsteady gait, and a general tiredness.
- Active symptoms. The employee may show signs of being under the influence. Generally, a drug will either relax or excite. A person who has taken a relaxant (depressant) tends to be "mellowed out," slow moving, dreamily happy, and likely to talk with slurring of words. The person who has taken a stimulant tends to be energetic, twitchy, fast moving, and likely to talk in a rapid and nonstop manner.

General Indicators

These may include indicators characteristic of one or both of the two preceding groups.

- An admission. A drug-abusing employee may admit to use, possibly to seek help or to explain unacceptable performance.
- Possession of a drug without medical reason. Drugs can be in the form of prescription drugs or illegally manufactured drugs. They might appear as pills, tablets, capsules, powders, pastes, leafy materials, gum-like substances, and liquids.
- Concealment. A user may hide a drug on the body or in some place that is accessible only to him or her. A user will sometimes favor concealment in an area also used by other employees. If the concealed drug is found, the user can avoid being singled out.
- Paraphernalia. An employee may possess or conceal drug paraphernalia, such as a syringe, needle, cooker spoon, roach clip, or glass pipe.
- Injection marks. An employee may show needle marks, boil-like abscesses, or scabs and scars, especially on the arms, legs, and backs of the hands.
- Drowsiness. An employee may show unusual sleepiness or general lethargy. This can be indicative of a slight overdose of an opiate, especially when it is accompanied by scratching of the body.
- Changes in the size of eye pupils. The pupils will greatly constrict immediately after taking an opiate. The pupils of an amphetamine user will dilate after use.

- Erratic conduct. The opiate user may vacantly stare and be generally unaware of surroundings; the stimulant user may be excited, euphoric, and talkative; the user of marijuana, inhalants, and depressants may be sleepy or appear to be drunk; and the user of hallucinogens, such as Phencyclidine (PCP) and Lysergic acid diethylamide (LSD), may engage in bizarre and possibly violent conduct.
- Change in eating habits. The abuser of stimulants will go for long periods of time without eating. The narcotics user may have a loss of appetite or consume candy, cookies, soda pop, and sweet-tasting food items.
- Illness symptoms. Users will display a variety of illness symptoms. For example, the opiate user in withdrawal may have the sniffles, flushed skin, muscular twitching, and nausea; the user of hallucinogens may experience an increase in blood pressure, heart rate, and blood sugar, irregular breathing, sweating, trembling, dizziness, and nausea; the cocaine user may have inflamed nasal membranes.
- Drug jargon. The use of drug jargon, awareness of how drugs are administered and their effects, and an attitude that excuses or defends drug use. The possession of magazines or literature marketed for persons interested in drug abuse is another indicator.
- Drug refuse. Trash receptacles in restrooms and public areas may contain items that suggest drug use. Discarded paper, plastic bags, and aerosol cans are the refuse of sniffers. The small vial that contained crack or the glassine envelope that contained heroin might be discarded, as well as metal bottle caps, eye droppers, syringes, and burnt matches that are used for cooking heroin preparatory to injection.
- Frequent absences. Absence from the job for 15–30 min every 4 or 5 h, especially in cases where the individual isolates himself in absolute privacy, is a telltale sign. This is the time when an addict "shoots up" or "snorts."
- Nothing to show for money. An addict will experience a discrepancy between income and expenditures for necessities, spending on alcohol or drugs most of what is earned, borrowed, or stolen.
- Borrowing. A constant need for money that may appear as borrowing from fellow workers, stealing, writing bad checks, and working as a prostitute.

INVESTIGATION

The CSO and/or an investigations unit working for the CSO will investigate violations that have not already been dealt with by supervisors. Legal aspects, which the CSO should know, will influence the investigation. Three aspects

of concern are contraband, chain of custody, and coordination with law enforcement.

Contraband

In the strict legal context, contraband is any item that by itself is a crime to possess such as illegal drugs, untaxed whiskey, stolen property, lethal weapons, explosives, and counterfeit money. All of these may be prohibited from the workplace because possession of them places the possessor in violation of the law. Alcohol is legal to possess, but company policy would prohibit its possession on company premises.

Chain of Custody

This concept relates to procedures for documenting access to a specimen (e.g., a blood or urine sample) as it was taken, transported, processed, and stored. A failure to properly monitor the collection of a urine specimen can result in actions by the donor to substitute a false specimen, contaminate his or her fresh specimen, or switch specimens with another donor.

Coordination with Law Enforcement

When a substance abuse violation is a criminal offense, law enforcement must be notified. Crimes that fall into this category are possession of drugs that have been identified as illegal by the Drug Enforcement Administration (DEA); selling or distributing drugs; smuggling or trafficking, for example, by using the company's transportation modalities; laundering money, for example, by using the company's financial functions.

Confiscated drugs are shown in Fig. 18.7. Drugs that have been confiscated by the CSO or security group must be precisely inventoried, a change of custody form prepared, and the drugs delivered to law enforcement without delay.

In a coordinated investigation, the usual practice is to split the investigative tasks. The CSO handles matters internal to the organization, and law enforcement personnel handle everything outside the organization. When an investigation moves to the courtroom, the CSO is teamed with the principal police investigators and a prosecutor.

THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

The Health Insurance Portability and Accountability Act (HIPPA) has established National Drug Codes with which treatment providers and health-plan

FIGURE 18.7
This photo shows Ecstasy pills, an illegal drug. *Drug Enforcement Administration.*

administrators are required to conform to adopted code sets for procedures, diagnoses, and drugs. Companies that collect specimens, whether the employing company or a third-party company, are not affected by HIPPA because they are not medical or treatment providers or health plan administrators. However, if the specimen is transported such as from the collection point to the test laboratory, and the transporter is employed by an organization subject to HIPPA, the regulations may apply. As a side note, company's drug testing programs almost always fall into the purview of the Human Resources Department. Involvement by the CSO, if at all, is to randomly monitor the collection of samples and chain of custody requirements. The principal role of the CSO in this regard is to ensure that crosscontamination does not occur and that samples do not get mixed up.

However, the CSO is intimately involved in matters involving drug trafficking, possessing, and using illegal drugs on company premises, or anywhere an employee works such as a truck driver or a salesman making a call on a prospective buyer. When drugs are confiscated by the CSO, they must be turned over to law enforcement without delay, and the case will be taken over by them or the DEA. The CSO, however, still has a role to play because much of the information needed by the investigating agency will be in the files of the company.

If a company is subject to HIPPA, the law requires employers to have standard national numbers that identify them on standard transactions. The employer identification number issued by the Internal Revenue Service was selected as the identifier for employers.

The National Provider Identifier (NPI) is a different identifier. It is a unique number assigned to cover health-care providers. Covered health-care providers, all health plans, and health-care clearinghouses must use the NPIs in administrative and financial transactions. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about health-care providers such as the state in which they operate or their medical specialty.

The Secretary of Health and Human Services is authorized to order compliance reviews to determine if covered entities are complying with the HIPPA law. The HIPAA is a 1996 Federal law that restricts access to individuals' private medical information.

Medicare and Medicaid are not issuers of health insurance and are therefore exempt. They are plans through which individuals obtain health coverage, not treatment.

CRITICAL THINKING EXERCISE

"None of my people are into drugs," said Kurt Walling, supervisor of an oil field drilling crew. "We work hard and long, but we work safe. Our accident record proves it." The CSO, Hal Anson, listened but was not convinced. As he had explained to Kurt, information developed by a law enforcement agency indicated a sharp rise in local street sales of amphetamine. Hal did not believe the oil field was immune to uppers or any other type of drug. "Just the same, it's good to be on the lookout," Hal said before leaving.

A week later one of the laborers on Kurt's crew lost three fingers when a clamp on a drill bit crushed his hand. A blood test made at the hospital revealed a large concentration of amphetamine in the worker's body system. Hal called Kurt and asked if there was anything he could do to help. "Yes," Kurt replied, "I need you to come out and show me again how to look for that amphetamine stuff."

What next steps should the CSO take? How should he address the drilling crew with regard to drug use?

REVIEW QUESTIONS

1. Employers use drug testing as a tool for maintaining a safe workplace. Name and describe two other reasons for operating a drug testing program.
2. Describe the two-test approach of urinalysis.
3. Under what circumstance might a positive drug test be disregarded?
4. Name and describe at least three objectives of a drug abuse awareness program.
5. State why supervisors are considered the backbone of intervention.

6. Law enforcement must be notified when illegal drugs are found in the workplace. The CSO has to perform three other tasks in regard to confiscated drugs. What are they?

References

Bomba, J.R., Deming, P.S., 2005. CPP Study Guide. twelfth ed. American Society for Industrial Security International, Arlington, VA.

Denny, R.M., 2008. Selecting and hiring loss prevention personnel. In: Sennewald, C.A., Christman, J.H. (Eds.), Retail Crime, Security, and Loss Prevention. Butterworth–Heinemann, Boston, MA, p. 459.

Ferraro, E.F., 2006. Investigations in the Workplace. Auerbach Publications, Boca Raton, FL.

Further Reading

Ferraro, E.F., 2007. The drug recognition process. In: Fay, J.J. (Ed.), Encyclopedia of Security Management. Butterworth-Heinemann, Boston, MA, p. 358.

Office of National Drug Control Policy, 1988. www.whitehousedrugpolicy.gov/prevent/workplace/index.html. (accessed 08.07.10).

CHAPTER 19

Executive Protection

What You Will Learn

- Elements of an executive protection plan.
- The nature of threats faced by protected persons.
- Measures to prevent the kidnap or assassination of protected executives at home and abroad.
- Major duties of executive protection professionals.
- The concept of defense in depth.
- The proof of life code.
- Procedures following abduction of a protected executive.

INTRODUCTION

Three guiding principles stated by Oatman (2006) may help executive protection professionals (EPPs) organize their thinking and their protective efforts:

- Be systematic, not symptomatic. This principle urges EPPs to understand the complete picture of risks and protective measures, address all relevant elements of protective operations, avoid the urge to plug small holes without solving underlying problems, and apply simple, sometimes basic measures, consistently across many domains.
- Be proactive, not reactive. This encourages EPPs to look forward and outward. That means conducting threat assessments, weighing and managing risks, appropriately applying resources, and performing countersurveillance. The opposite approach—event-driven response—can result in excessive security measures, overengineering, inflated deployment of security personnel, and unnecessary inconvenience to the protected person.
- React with flight, not fight. The primary purpose of executive protection is not to capture or kill attackers but to protect the executive. Experience shows that, in this context, escaping from an

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00019-0

attack leads to better outcomes than standing one's ground and fighting back. Therefore, the EPP should develop plans that emphasize getting the protectee away from danger or else finding cover. Preparing for a safe escape requires detailed advance preparation, including site surveys and training for a near-automatic execution of the exit strategy.

THE PROTECTED PERSONS

An executive protection program is a security component in many venues: business, government, entertainment, sports, wealth, and other fields. Our principal perspective in this book is business, and for that reason, we will use the term chief executive officer (CEO) when referring to the protected person. We will also use the term program when referring to the executive protection program. Not all CEOs are protected. This is because in some organizations:

- The board of directors sees no need for it.
- The CEO refuses to accept it.
- The threat is believed not to exist or is perceived to be at such a low level a program is not merited.
- The cost of a program is not affordable.

In the business venue are questions to be asked and answered.

- Who is entitled to receive protection?
- What should the extent of protection be?
- Who will provide it?
- What are the circumstances that would merit changes as to who should be protected, the extent of protection, and the composition of the protection party?

As to the first question, the top leaders of a business enterprise, such as the board of directors, typically will stipulate protection according to rank or status. Some businesses will provide protection only for persons at the CEO level or above such as the chairman of the board of directors. At a lower level, protection might be afforded to persons of lesser rank who head up operations in areas where kidnapping and assassination are not uncommon such as in South America and the Middle East. When ransom has been paid or an assassination committed in the past, a company may mandate protection of its potentially targeted employees.

The extent of protection will vary relative to the value of the person to the organization and the person's exposure to personal danger. The

superintendent of an oil production facility in the Andes may be third or fourth from the top of the organizational chart but will be highly protected because without him or her the facility might have to be shut down and/or a hefty ransom paid. The CEO of the company, who is sitting in a high-rise office building in Houston and who has a much higher rank than the field superintendent, may be under no protection at all (except when he would travel to the production site in the Andes).

Persons providing protection in overseas areas are usually locals who come from a military, law enforcement, or security background and who have been vetted. However, the leader of the protection cadre should be an on-site employee of the company such as a member of the security department located at the company's stateside headquarters. The same applies when a senior executive travels abroad openly such as to a conference is well known to the public. In this case, however, protection tends to be made with a greater number of EPPs. Protocol and necessity require that local or federal law enforcement in the host company be participants, not as in-close protectors, but as uniformed and nonuniformed personnel assigned to the outer layers of protection and as spotters within the audience group or in locations that permit an unobstructed view, oftentimes with telescopes and video recording equipment. The recording equipment would be useful in a postincident investigation or as a procedure for identifying activists or trouble in the incipient stage.

In some cases, local security firms are brought in as supplemental elements. The choice of the security firm is made by the local police department, but the team leader of the protected executive's party should make sure the security company is reliable, has a history of successfully performing executive protection duties, and is not owned by the brother-in-law of the chief of police.

When the overseas event is attended also by a higher ranking person, such as the President of the United States, leadership of the protection program will be provided by the organization of the higher ranking person. In such an event, the protective force of the company will be subordinated to the leader of protection for the senior person.

PROGRAM SIZE, EQUIPMENT, AND OBJECTIVES

A program can be small and simple, comprehensive and complex, or somewhere in between. The nature of the threat will determine the nature of program. As the threat level rises, so must the capability of the program.

The protection elements in a small program can consist of guards at the office building and an alarm system in the home. The program enlarges as duress alarms are installed in the executive suite, a security officer is the receptionist at the suite entrance, and secretaries are trained to look for and react to danger. At the home, exterior lighting is added, and a security patrol passes by several times during hours of darkness. A comprehensive program can have all of the previous plus a driver and an automobile for local commuting. The driver will be skilled in bodyguard tactics, escape driving, use of a firearm, and administration of Cardiopulmonary resuscitation (CPR) which s a method for reviving those who are suffering from cardiac or respiratory arrest and first aid. The vehicle will be resistant to bullets and explosives and have capabilities for quick acceleration, high speed, and tight cornering. Fig. 19.1 shows the head of Homeland Security being briefed concerning the limousine assigned to her for Department of Homeland Security (DHS) business. The CEO's home will have a controlled entrance gate and one or a few security officers stationed at perimeter entrances and along the perimeter wall or fence. A communications system will allow the chauffeur/driver and other security personnel to communicate among themselves and with a security control center.

Whatever the size and complexity of the program, the Chief Security Officer (CSO) is the person in charge. When the program is large, the CSO will be assisted by a person that might hold a position titled executive protection manager (EPM). This individual supervises routine protective activities at the CEO's office and home and accompanies the CEO when he or she is traveling in high-risk areas and appearing at or attending public events.

FIGURE 19.1

A limousine is a common item of equipment used for executive protection. *U.S. Department of Homeland Security.*

PROTECTION AT THE OFFICE AND AT HOME

At the office or the home, the protective shield is a combination of physical safeguards and people. These have four main functions:

- Keep threats away.
- Give warning when a potential threat is near.
- Summon help.
- Provide protection until arrival of a larger response party.

Many physical safeguards serve purposes in addition to executive protection. For example, fences, lights, sensors, alarms, and CCTV at the office are there to protect everyone. Other safeguards serve the CEO only (e.g., duress alarms, bullet- and explosive-resistant walls, concealed room, specially equipped vehicle, and competent driver).

People who protect the CEO at the office consist mainly of security officers, and they too serve the general employees, visitors, guests, and vendors. At the CEO's home, the people component is slightly different: They are armed or unarmed and uniformed or ununiformed security officers. Members of the household staff, such as cook, housekeeper, or gardener, are taught to give warnings of danger.

THE THREAT

U.S. businesspersons, both at home and overseas, are targets for kidnapping, assassination, and other acts of violence at the hands of criminals and terrorists. The criminals' usual objective is to acquire money in exchange for their captives. When the kidnappers are also followers of an ideology, their objective may be to force changes to government policy or business practices or to obtain release from incarceration of their fellow criminals.

Kidnapping is a classic act of terrorism, according to Bomba and Deming (2005). Terrorists also use kidnapping as a means of acquiring money, but their usual objectives are to shape public opinion, overthrow a government, elevate a religion or cult, or simply annihilate people. Experience tells us that CEOs often become the targets of deranged individuals with motives as strange as the acts they commit. For example, a CEO whose decision caused an employee to be disciplined, laid off, or terminated may become the center of the employee's frustrations. The employee may believe he or she was discriminated against and as a result will attempt revenge.

ADVERSARY ATTEMPTS AT THE RESIDENCE OR OFFICE

A group intending to kidnap or harm the CEO may attempt to gain entry to the residence or office through pretext. Examples are posing as a cable repairman, slipping past a guard during shift change, and pretending to be a FedEx courier.

The group's target can be the CEO's child. If kidnapping is the objective, the method may be trickery in effecting release of the child from the custody of a babysitter, childcare center, or school. The target can be the CEO's spouse, and the capture may be attempted when he or she is away from the home such as when shopping, jogging, or socializing.

The best guidance for the protectors and the protected is to anticipate possible scenarios, take preemptive steps, look for the early warning signals, and react quickly. The CSO must evaluate the vulnerabilities of the organization with respect to the threat, the current capacity of the organization to resist, and the range of countermeasures necessary. A program has credibility when it is anchored in the authority of an unambiguous company policy, takes into account specific threats, and is active in seeking reasonable countermeasures to lower risk to an acceptable threshold.

EVENT PROTECTION IN THE UNITED STATES

Kidnapping is but one of several threats confronting a CEO. Other threats include assassination, assault, robbery, and nonattack threats such as heart attack, sudden illness, or injurious accident. In all cases, the protected executive will be in the presence of one or more persons qualified to administer CPR, defibrillation, and first aid. Such persons outside of the organization, particularly drivers, will be screened by a background investigation, know where immediate medical assistance is available, know the quickest route for getting there, and know who in the organization to call in such a situation. The CSO, who ensures the drivers' qualifications, is the person most often called.

Of all threats, assassination presents the greatest risk by far. Resistance is likely to involve use of violence to thwart the threat. On the other hand, kidnapping is usually carried out covertly, thus avoiding resistance by force.

The CEO is most vulnerable when in close proximity to the public. Potential assassins understand this. They know that the protective capability is much reduced and that with little sophistication and a simple weapon the target can be brought down. We know this from experience. Nearly all assassinations of prominent leaders have occurred in public places, the assassins were able to get close enough to act, and the weapon was concealable.

CEOs are in an exposed position when they appear at an event. Events vary, but all of them have one thing in common: The CEO is exposed to danger to some degree. Event protection is an activity separate from security provided to the CEO in the office, at home, during commuting, and routine out-of-town travel. Routine security requires a lesser number of people; event security can require numerous people, some of whom may of necessity be outside contractors.

Team Leader

The person in overall charge of event-related protection can have a number of titles (e.g., mission leader or person-in-charge). We will use team leader and mission when referring to event-related protection activities. The team leader will be the CSO or the EPM. The big-picture functions of the team leader are preparing an operational plan and supervising the mission team. The mission team for an event has four groups: advance party, residence party, baggage party, and protective party.

Advance Party

This group travels in advance to the locale of the upcoming mission and

- Conducts on-site inspections to evaluate probable risks to the CEO and proactively sets up countermeasures. Inspections take place at arrival and departure terminals, offices to be visited, conference rooms, restaurants, event venues, and other places on the CEO's travel agenda.
- Meets with and initiates working relationships with officials of participating agencies.
- Conducts reconnaissance of local travel routes and makes recommendations to local traffic control officials. Recommendations might include speed, composition, and order of a motorcade.
- Coordinates local ground transportation and arranges for the security of baggage.
- Inspects vehicles to be used for local ground transportation and briefs drivers concerning what to do if a vehicle is involved in an accident or breaks down or if the CSO is injured or becomes ill.
- Prepares sketches, maps, photographs, and written reports to fully inform the team leader and team supervisor.

Residence Party

This group provides around-the-clock protection at the CEO's places of stay during travel. Duties can include keeping a log of occurrences, screening incoming telephone calls, checking packages, controlling the access and movements of visitors, and driving the CEO from place to place.

FIGURE 19.2
Note the protective party accompanying former President Bush and his wife. *United States Secret Service.*

Baggage Party

The baggage party provides oversight protection to the CEO's baggage. The function begins at the starting point and continues during travel to the visit location. Oversight is discontinued during the time the baggage is in use by the CEO. The baggage party resumes oversight at the outset of and during the return trip and concludes when the CEO reaches home base. This group does not actually handle baggage but supervises the movement and custody of it.

Protective Party

This group conducts surveillance and provides close-in protection prior to, during, and after the event. The protective party consists entirely of or is complemented by persons from the advance, residence, and baggage parties. Fig. 19.2 shows a protective party at work.

The nuts and bolts of the mission, which are covered in the operational plan, determine the tasks of the protective party. Details of the operational plan are known only by the team leader and members of the protective party. Details can be revealed to outsiders only when knowledge of them is necessary for plan execution. For example, if the team is to be armed, this fact is made known to local law enforcement authorities.

EVENT PROTECTION OVERSEAS

The situation changes when the event is to occur overseas. For one thing, the organization sponsoring the event may have to perform administrative tasks

normally done by the advance team such as acquire maps and photographs and identify routes of travel, emergency care facilities, and private security firms. The sponsor can also introduce the advance team to local agencies involved in the event. When the CEO's organization has an office near the event site, staff from it can help as well.

Events held overseas present out-of-the-ordinary circumstances, some of which can be impediments. Impediments decrease the protective capability, which in turn increases risk to the CEO. Problems are created when assisting persons at the overseas site prove to be unreliable. Small details, such as traffic conditions and ground transportation, are certain to be different and therefore problematic. What may work nicely close to home base may not work nicely overseas. The essential tasks include the following:

- Book travel and hotel accommodations in the name of the sponsoring organization. Work through a vetted point of contact (POC). Preferably, the POC will be a senior person in a governmental police or intelligence service.
- Maintain confidentiality of details associated with the CSO's travel, accommodations, and attendance. Communicate with the POC and others on a need-to-know basis.
- Evaluate arrangements made at the location site pertaining to side trips.
- Anticipate potential disruptions, most particularly public demonstrations and actions of paparazzi.
- Acquire pertinent maps, sketches, diagrams, photographs, and so on. These will depict the layout of the event site, areas surrounding the event site, travel routes to and from the event site, and places where the CSO will be stationary. Rest rooms are included.
- When the sponsoring organization is company owned or company managed, the POC will be an employee of the sponsoring organization. Make clear to the POC that overall security is the responsibility of the sponsoring organization, subject to approval of the team leader. (Note: Bodyguard protection during the event will be provided by the team.)
- Confer with and obtain advice of local law enforcement authorities concerning potential security threats, obtain recommendations, and be cautious in allowing participation of local resources in carrying out the mission.
- Consult with other agencies of interest such as an embassy or consular office. Obtain intelligence estimates as to possible security threats.
- Avoid advance publicity.
- Schedule local ground transportation as tightly as possible. Local ground travel will be in a primary vehicle operated or occupied by a team member or a local person vetted, trained in CPR and first aid, and having knowledge of the roadways and of available emergency medical

treatment facilities. The primary vehicle and backup vehicle will be equipped with a telephone and cell phone. A primary and an alternate route will be selected and tested in advance.
- Confer with the security professionals at hotels to be used. Evaluate security normally provided to CSOs, and where necessary augment to ensure an adequate level of protection.
- Escort the CSO throughout the event and give to him or her a contact telephone number to use in the case of an emergency, an unanticipated incident, or a change in schedule.
- Employ local security officers only in exceptional circumstances. Hiring should be through a reputable security company recommended by the police. The police must be informed of any decision to use armed persons.
- Obtain the services of an antieavesdropping specialist if information security will be an issue at a closed venue.
- Advise the CSO to cancel or reschedule the event if the risk is high or local security capabilities are inadequate.

OPERATIONAL PLAN

Information acquired by the advance team is dropped into the planning pot along with information obtained from the CEO's staff. Details can include the type and theme of the event, event agenda, names of event speakers, special guests, characteristics of the audience, travel itinerary, persons traveling with the CEO, modes of travel to and from the event city, social activities, shopping and sightseeing trips, and so on. Also placed into the pot is information about potential threats, especially any threat in the form of a terrorist group. These pot ingredients are a terrorist group's proximity to the event site, its stated intentions, capabilities, resolve, preferred targets, weapons, and tactics. The team leader, along with the CSO, stirs the pot to see what type of stew has been cooked.

Based on what has been learned, the team leader begins to put together a plan. The plan will take into consideration the following:

- The attitude of the CEO regarding the protective shield.
- Political, religious, and cultural beliefs that pervade or surround the event.
- Duration of risk exposure (i.e., the length of time the CEO will be exposed to a potential threat).
- Coordination with other agencies, particularly law enforcement.
- Ability of the protective force to deflect an attack and react effectively.

- Laws that apply such as laws dealing with possession of weapons and the application of deadly force.
- Means of communication.
- Terrain and geography.
- Modes of transportation, both routine and emergency.
- Availability of emergency medical treatment.
- Selection and training of security personnel.
- News media presence and their expected activities.

Murphy's Law applies. Even when a plan addresses every possible glitch, the unexpected will happen. It is for this reason that planning has to include a strong flavoring of flexibility.

ANTIKIDNAP PLAN

A first step in a company's defense against executive kidnapping is to develop a policy and obtain approval of an antikidnap plan. Approval in most cases will be made by the board of directors and will involve consideration of kidnap insurance, ransom payments, and a crisis management team (CMT). The policy provides direction and authority for the antikidnap plan.

Kidnap Insurance

If kidnap insurance is purchased, the carrier will require absolute secrecy with respect to any premeditation concerning intent to pay ransom. The carrier may also dictate who is to do the negotiating of ransom payments, require that the organization's response be conducted in accordance with applicable laws of the United States and other nations, and that prompt and full notification be given to law enforcement. A failure by the organization to meet the carrier's requirements can render the coverage null and void or reduce the carrier's obligations to pay.

Although the organization's plan for dealing with kidnapping is a highly sensitive matter, it cannot be developed with such great secrecy that it will reflect the thinking of one or a few individuals who may not have all the right answers. An initial planning group consisting of in-house and outside experts can be helpful in touching all the bases. In addition to the CSO, who has a key role to play within the group, other members can include the following:

- Agents of the Federal Bureau of Investigation (FBI).
- A counterterrorism expert.
- A person familiar with the national government of the place where the kidnapping occurred or where the kidnapped person is being held captive.

- A kidnap insurance specialist.
- A professional hostage negotiator.
- A public affairs specialist.
- An electronics communication technician.
- A human resources specialist.

US law requires notification to the FBI when a kidnapping is confirmed. Leadership transfers to the FBI, which may or may not choose to utilize the services of the company's CMT.

Kidnap Survey

A survey of the CEO's home can uncover weaknesses correctible with simple safeguards such as keeping shrubs trimmed, adding outside lights, and installing an alarm system inside the home. In high-risk circumstances, it may become necessary to add watch dogs and security officers and an alarm system that begins at the perimeter of the property in addition to the home alarm system. Fig. 19.3 provides kidnap prevention tips.

Thought in the survey is given to the time needed to execute an effective, timely response to a threat made at the CEOs home. When such a response is uncertain, protection can be supplemented by creating in the home a concealed room. A concealed room typically features a highly resistive door, a panic button, and a telephone. A weapon inside the room is an option.

A survey might call for screening and equipping protective staff. Screening can go beyond routine background checking. Equipping can include defensive items such as bullet-resistant vests, firearms, cell phones, and walkie-talkies.

Kidnap Prevention Tips

Instruct family and business associates not to provide information concerning you or your family to strangers.

Avoid giving unnecessary personal details in response to inquiries from information collectors that would be used in such publications as business directories, social registers, or community directories.

Review your organization's security plans to determine their effectiveness. Make certain employees are aware of these plans. Establish simple, effective signal systems which, when activated, will alert your business associates or family members that you are in danger.

Be alert to strangers who are on business property for no apparent reason.

Vary your daily routines to avoid the habitual patterns that kidnappers look for. Fluctuate your travel as to times and routes and travel to and from the office.

Refuse to meet with strangers at secluded or unknown locations.

Inform a business associate or family member of your destination when leavingthe office or home and what time you intend to return.

Lock all doors and roll up windows of your automobile while traveling to and from work.

FIGURE 19.3

Anti-kidnapping tips. These tips can be helpful in establishing an anti-kidnapping program.

ABDUCTION

The value of planning and preparation is immediately evident in the aftermath of abduction. Preparation should be made to receive contact from the kidnappers and to respond in a manner that will not place the CEO's life at greater risk.

Contact

The kidnappers will likely make contact by telephone, although it could be made by letter or through another party such as a newspaper or radio station. If contact is by telephone, certain protocols are in order to:

- Express a willingness to cooperate.
- Ask to speak to the CEO.
- Ask for the proof of life code.
- Record the call.

If contact is in writing, the document and its envelope or outside container are carefully protected in order not to adversely affect forensic analyses such as examinations for fingerprints and saliva on the envelope flap. An attempt to handle the situation without recourse to law enforcement is likely to fail.

By the time the kidnappers have made contact, the FBI will have been notified and the CMT activated. The CMT leader, to whom considerable decision-making authority has been delegated by the board of directors, is the key person in coordinating major issues with the FBI and law enforcement and other parties of interest. Fig. 19.4 is a list of tasks that can be of use after a kidnapping occurs. The CMT members perform their preplanned tasks (e.g., notifying next of kin, dealing with the news media, setting up a

If Kidnapping Occurs…

Call the Federal Bureau of Investigation. The telephone number of the nearest FBI office is listed in the front of the telephone directory. The reporting person should be prepared to furnish in an orderly fashion all facts relating to the disappearance of the victim.

Maintain absolute secrecy and do not permit any of the facts regarding the kidnapping or demands for ransom to be known outside the immediate family and the investigating officers.

Do not handle letters or written communications demanding the payment of ransom. Turn these over to the investigating officers as soon as possible.

Do not touch or disturb anything at the scene of the abduction. Minute particles of evidence not visible to the naked eye could be destroyed.

Be calm and try to maintain a normal routine.

Place full confidence in the investigating officers. Help the investigators by providing photographs, a full description of the victim, and all facts relating to the personal habits, characteristics, and peculiarities of the victim.

FIGURE 19.4

Tasks to be used after kidnapping has occurred and tips to be discussed with protected persons. This tip sheet or one similar to it can be given to the protected person for reference if he or she is kidnapped.

command center, establishing a rumor control center, and coordinating with the kidnap insurance carrier). Communication technicians, communication equipment, and overall direction are provided by the FBI.

Ransom

Kidnappers often demand an immediate and large payment but do not expect the demand to be met quickly and entirely. They realize that even if an immediate payment can be effected, it is not likely to be as large as a payment arranged with deliberate speed. Kidnappers focus on "making a big score" and want to believe that the ransom payer has not contacted law enforcement authorities. An expectation of success suppresses their fear of getting caught.

PROOF OF LIFE

The proof of life code is one or many bits of information that would be known only to the CEO. Examples include the name of the CEO's first grade teacher, the name of the CEO's first dog, or the family nickname of an eccentric aunt. In discussions with kidnappers, proof of life information can be used to verify that the CEO is alive. Other examples of proof of life information are details such as photographs of the CEO, tattoos, moles, hair pieces, prosthetic devices, scars, birth marks, jewelry worn, and visible disfigurements. Dental and medical records and eye glasses and contact lenses' records can also serve as proof of life information when facts of this nature are communicated back to the FBI.

Executive File

An executive file is created by the CSO. It contains the proof of life code in addition to many of the items mentioned above. To the greatest extent possible, the CSO should obtain photographs, maps, sketches, and the like of the location where the kidnapping is believed to have occurred. Information of this type can be extremely helpful in determining where the person is being held captive.

Training

The CSO, his or her immediate family, and protective staff are at the top of the list for training in advance of kidnap or attempted kidnap. Below them are house servants and office workers with frequent access to the CEO. The training topics address how to avoid attracting attention, the tactics of kidnappers, the early warning signals of a kidnapping attempt, how to respond, and, if abducted, how to survive. Survival can be assisted by the following:

- Portraying symptoms of the Stockholm Syndrome.
- Asking for the Bible or Koran or other religious item of reverence held by the captors.
- Following a routine that consumes time and diverts worry from the situation.
- Treating the matter as a common, usual business deal that is certain to be consummated.
- Avoiding direct confrontation such as staring at the captors or their apparent leader.
- Soliciting understanding and sympathy with the apparent leader or someone close to him.

Buy-in to protection is demonstrated by the protected executive's commitment to and active involvement in protective arrangements. Involvement has three dimensions:

- Training.
- Genuine interest in the program.
- Cooperation during training and with the program.

The first of the three is problematic. According to Muuss and Rabern (2006), CEOs are often busy and do not assign a high priority to training. The CSO has to find a way to get past the reluctance. In this case, patience is a virtue; persuasion is a must. Horror stories and cajolery, while not always a good tactic, may help. In the context of orienting a new executive, Sennewald (1998) recommends asking the new CEO to compare the new company's executive protection program over what he or she was accustomed to in the previous job. By pointing out the merits and virtues of the new program, the CSO may be able to overcome the new CEO's reluctance to receive training.

Fortunately for the busy CEO (and all are), the key points of training are knowledge-based (i.e., the CEO can learn without actually getting up from a desk). The exceptions would be firearms and self-defense training. For many companies and many CEOs, the use of firearms is not seen as helpful, and for some CEOs, self-defense is not practical for reasons of age or inclination.

Training of the CEO should emphasize:

- Activities of the protection team.
- Listening to and carefully evaluating the team leader's advice.
- Obeying protection team's directions during an attack.
- Knowing how to keep from being kidnapped or assassinated.
- Knowing how to respond if taken hostage.

The CEO learns to closely control information that an adversary would need to be successful, avoid predictable behavior, and stay within the shell

maintained by the protective party at public events. As to response, the CEO learns the early warning signals and how to recognize them, actions to take and not take, and most importantly, how to survive if taken hostage.

Training is a serious and difficult endeavor. It is serious because death or injury can result if the CEO makes an incorrect response. It is difficult when the CEO has little or no familiarity with violence, and without training stands little chance of surviving. Can such things be learned easily? The answer is no. Is this something that has to be learned? The answer is yes.

Avoid Attracting Attention

Kidnappers are assisted when they possess details of the CEO's appearance at social activities, local movement, and out-of-town travel. Care has to be taken when talking on the telephone, in restaurants, and in other places where conversations can be overheard. Written information personal to the CEO deserves protection and should be shredded when no longer needed.

Routes to and from work and the vehicles used should be frequently and randomly changed; the times, dates, and places of out-of-office business meetings should not follow a discernible pattern; and family and social routines should be varied.

CRITICAL THINKING EXERCISE

Exxon executive Sidney J. Reso disappeared from his home in Morris Township, New Jersey, on the morning of April 19, 1992. Reso's wife discovered his car at the end of the driveway—empty but with the engine running. After calling his office and finding he had not arrived, she called the police.

At first, the Morris County authorities handled it as a missing person case. The next day, however, a caller to the Exxon switchboard claimed to have information about Reso and said that a letter could be found at a nearby shopping mall. Convinced then that a kidnapping had occurred, the Morris County Prosecutor's Office (MCPO) called the FBI.

Within 4 h, the Reso home became an FBI command post complete with trap, trace, and recording devices on phone lines. The neighborhood and surrounding wooded areas were thoroughly searched, and 24-h surveillance and security was set up at the Reso home and at the homes of four children in Texas, Missouri, California, and Washington, DC.

A ransom demand letter was picked up at the mall. The kidnappers instructed that a cell phone be obtained for future calls and that the phone number be published in a classified ad in the Newark Star Ledger. The letter also contained a demand for $18.5 million in hundred-dollar bills.

Exxon provided the ransom money and the FBI packaged it. A cell phone was obtained and the waiting for a call began. Specialist teams were gathered and made ready to move on an instant's notice. As they waited, the teams practiced skills that ranged from communication intercepts, to sniper firing, and to SWAT exercises.

The kidnappers made eight calls and sent 14 letters before attempting to collect the ransom. The attempt occurred on May 3 but went awry when the kidnappers made a mistake in following their own instructions. More calls, letters, and advertisements followed.

On June 16, the kidnappers seemed ready once again to act. They instructed Reso's wife, daughter, and an Exxon executive to deliver the ransom and to take the cell phone with them so they could receive instructions along the way. Two FBI agents posing as Reso's wife and daughter accompanied the Exxon executive. The kidnappers' instructions took them on a rambling journey. Meanwhile, FBI agents in many separate locations watched out of sight. A break came when an agent observed a heavy-set white man with blonde hair wearing gloves making a phone call at a shopping mall. The agent also observed this same man remove the gloves when he got into a red Cutlass Ciera, which was traced to a rental car company. Shortly after that, one of the kidnappers' calls was traced to a pay phone in an area where a surveillance team was in place. The team observed a woman calling from a pay phone, and the time of the call matched the time of one of the kidnappers' calls.

Agents went to the rental car company and waited. Arthur Seale returned the Ciera. His wife Jackie arrived to pick him up. Jackie Seale turned out to be the same woman who had been seen earlier making a call from a pay phone. The Seales were arrested.

Arthur Seale had previously worked as a police officer and a security official at Exxon. He and his wife decided to kidnap and ransom Sidney Reso in order to get out of serious financial difficulty. They began by watching the Reso house and learning Mr. Reso's morning routine. When they felt prepared to act, they went to the house and moved the morning newspaper from one side of the driveway to the other. They knew that he always picked up the newspaper and took it to work with him. To pick up the newspaper where Seale had placed it, Reso would have to get out of his car and walk around it. When Reso did exactly that, Arthur Seale approached him quickly and at gunpoint forced him into a rental van driven by Jackie Seale. The gun went off, and Reso was shot in the arm. The Seales drove him to a storage facility where, after treating his gunshot wound, they blindfolded him, handcuffed him, gagged him, and placed him in a coffin-like wooden box.

One week after the Seales were arrested, Jackie began cooperating. She said that Reso had died on May 3, just four days after his kidnapping. She and Arthur Seale removed the body from the box at the storage facility and buried it at another location.

The Seales were charged with multiple federal and state offenses. He pled guilty to seven federal counts, including extortion, use of a weapon in the commission of a crime, and a state charge of murder. He was sentenced to 95 years in federal prison to be followed by 70 years' state imprisonment. She was sentenced to 20 years in federal prison for the two counts of extortion.

Considering the antikidnap procedure already mentioned, what protective steps could have been taken to prevent the kidnap of Mr. Reso?

COUNTERMEASURES

In-depth, defense is a tactic used in almost every mission. It consists of one or more rings of protection that an attacker has to penetrate in order to reach the target. For a high-risk mission, the number of rings is numerous. For example, in a situation where the CEO moves through a dense crowd, a tight ring of one to four persons move in unison with him or her, a loose ring of

trouble spotters operate 15–25 m away, and spotters at an elevated location communicate with those down below. In a low-risk situation, the CEO may be accompanied by one or two persons and no spotters. Shown in Fig. 19.5 is a rooftop spotter.

In-depth, defense can be likened to an onion. As each layer of the onion is peeled back, another layer is beneath it, and each layer is increasingly difficult to peel.

The main concept of a layered defense is to delay the aggressor and to force a change in the aggressor's tactics or plan. Forcing the aggressor to defeat layer after layer gives to the protection team more time to obtain vital information, such as learning if the aggressor possesses a weapon, the type of weapon, and whether there is more than one aggressor. Just as important, if not more, is the time it gives the protection team to determine the best direction of flight and move the protected person to safety. In the case of an outside event, a safe haven might be a vehicle nearby with a driver behind the wheel and engine running or a nearby building with a guard or guards at the entrance. At in indoor event, the safe haven might be a guarded room, inside of which is an escape door.

In-depth defense is mobile. As it moves, the CEO remains at the center and moves with it.

FIGURE 19.5
Members of the protective party look for the early signs of an attack from an elevated location. *iStockphotos.*

After-Action Report

A written report is made for the record at the conclusion of a mission. It is written in narrative style, with emphasis on problems encountered and steps taken to resolve them. The report contains recommendations for improvement of performance in future missions.

Problems described in the after-action report give proof of a fact: It is not possible to give absolute personal protection. The best that can be expected is to reduce the risks as much as possible. Persons assigned to CEO protection duties have to understand this basic premise. They also have to know and accept the legal and sociological constraints that are present in every mission.

CONCLUSIONS

There can no protective program without the CEO's buy-in. A CEO understands risk as a management concept but may not be ready to acknowledge risk in personal terms. CSOs have been known to respond with denial, not unlike alcoholics refusing to look at the evidence of addiction. A program will not work until risk is acknowledged and training provided.

REVIEW QUESTIONS

1. Name the usual motives of terrorist kidnappers.
2. How does event protection change for overseas events?
3. Name three duties of the advance party.
4. What is the defense-in-depth concept?
5. In one sentence, describe the proof of life code.
6. What is the single greatest factor likely to impede the training of a protected person?

References

Bomba, J.R., Deming, P.S., 2005. CPP Study Guide. ASIS International, Arlington, VA.

Muuss, J.P., Rabern, D., 2006. The Complete Guide for CPP Examination Preparation. Auerbach Publications, New York.

Oatman, R.R., 2006. Executive Protection: New Solutions for a New Era. Noble House, New York.

Sennewald, C.A., 1998. Effective Security Management. Third ed. Butterworth-Heinemann, Boston, MA.

CHAPTER 20

Workplace Violence

What You Will Learn

- The elements of a workplace violence prevention policy and plan.
- The characteristics of workplace violence.
- The composition and functions of a violence response team.
- The role of the supervisor in dealing with workplace violence.
- Potential legal barriers to firing a violent employee.
- Liability issues related to workplace violence.

INTRODUCTION

Violence in the workplace has always been a top concern for the chief security officer (CSO). Although on-the-job violence is not new under the sun, the most extreme form of it, homicide, has occurred with increased frequency in recent years. Studies made of workplace violence reveal the following:

- It appears in a variety of shapes and forms.
- There is no absolute, sure-fire method for preventing it in every situation.
- A small amount of preparation can go a long way in reducing injuries and saving lives.
- Prevention and mitigation cannot be achieved through the efforts of the CSO alone.
- Effective management of workplace violence depends on joint efforts of specialists in several disciplines.

POLICY

A policy on workplace violence is developed at senior management level. It is a broad-brush statement that serves as a template for development of a

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00020-7

plan that will make the policy functional. At a minimum, a workplace violence policy should:

- State the organization's right and obligation to ensure a workplace free of violent behavior.
- Use examples to show what is meant by violent behavior.
- Define terms to avoid misinterpretation and create escape holes that could defeat intent or precipitate litigation.
- Demonstrate an organizational commitment to deny employment to applicants with a history of violence and to weed out employees who engage in violent behavior. The policy can, for example, require background inquiries of job applicants and automatic dismissal of employees who commit serious acts of violence.
- Require and encourage policy compliance by all employees.

CRITICAL THINKING EXERCISE

Muriel, 62-years old and a 15-year employee with a convenience store chain, knew by name all of the regular customers at her corner store. She was attentive to her job and took pride in holding shoplifting losses to a minimum and maintaining an accurate till. During an audit by a security department investigator, she boasted that she had only once been short in the till and that to keep her good record intact she had made up the shortage out of her own pocket.

Muriel explained a man she did not know entered her store just before closing time. After ensuring that he was the only customer, the man produced a gun and forced Muriel to give him the content of the till, amounting to slightly more than $50. Later, when talking to the company's security investigator, Muriel said she was going to buy a gun and keep it under the counter. "Ain't nobody gonna rob me no more," she said. The security investigator informed her that company policy prohibited guns on store premises and that the proper response to a robber's demand was to cooperate and surrender whatever the robber wanted. Muriel replied that she understood the policy but "damn sure didn't like it."

A week later, right at closing time, the same robber returned and demanded she hand over the money. Muriel reached into the till, removed a handful of bills, and threw them in the robber's face. When the robber bent down to pick up the money, Muriel lifted a heavy bottle of dill pickles from the counter in front of her. She crashed the bottle on the back of the robber's head. He stood up, shot her in the neck, and cleaned out the rest of the till before fleeing.

Muriel recovered but the company did not allow her to return as a store employee. After two months as a file clerk in the company's accounts payable department, Muriel quit and applied for social security benefits.

Did the security investigator act appropriately? Was there anything else the investigator could have done? Was Muriel correct in attempting to thwart the robbery?

Every policy must have a plan. The purpose of a plan is to execute policy. Whereas a policy is broad, a plan is detailed. Persons assigned to develop the plan usually work as a team, and a member of the team is certain to be the CSO. The main elements of a plan should be to:

- Describe how the organization will monitor and enforce compliance. An important element here is to ban lethal weapons at work and to express management's right to look for weapons at entry points and on the premises.
- Assign specific responsibilities to key persons such as the CSO, head of human resources, and chief safety coordinator.
- Assign general responsibilities such as requiring employees to report indicators or incidents of violent behavior.
- Name consequences for noncompliance (e.g., suspension or termination).
- Report violations. However, avoid a zero-tolerance position because every case will have its own unique set of circumstances. Also, zero tolerance can discourage employees from reporting violent behavior. An employee's desire may be to get a coworker's behavior stopped, but not get the coworker disciplined or fired. As a result of the failure to report a violation and set off the intervention that follows, a major incident can cause innocent persons to be injured or killed.
- Identify training and the people to be trained.
- Name employee assistance benefits such as services available to victims of violence and psychiatric counseling of violators.

A plan will place everyone on notice that violence is not acceptable and will be dealt with in every case. This simple message can be conveyed in a variety of formats such as memoranda, bulletin board and electronic messages, employee handbooks, and as an agenda item at employee meetings.

The wide variation in violent behaviors does not allow definitive predictions of likely incidents. The best that can be done is to identify broad scenarios, e.g., incidents involving actual death or injury, incidents involving lethal weapons, arguments, threats, intimidation, verbal assaults, and bullying. Alternatively, a single scenario could be developed to deal with all incidents. Fig. 20.1 is a checklist for developing a generic plan.

Primary among the objectives of a plan is to develop a simple system for ensuring that all incidents of violence, whether large or small, are reported and documented. Capozzoli and McVey (1996) say that it doesn't matter if an incident is actual or threatened, it must be fully documented.

The reporting channels can include hotlines, supervisors, human resource specialists, and a conspicuously posted phone number that connects to the security desk.

Checklist for a Generic Plan

Develop a plan that will

prohibit threats, intimidation, harassment, unwanted physical conduct, and any form of violent behavior at work,
prohibit the possession, distribution, or use of alcohol and illegal drug use at work,
prohibit lethal weapons at work,
apply the plan to all employees at all levels,
educate employees concerning the unacceptability of violence and the consequences of policy violations,
train supervisors to recognize the early warning signs of violent behavior and to intervene to prevent violence before it can occur, assign clear responsibility for compliance and enforcement.

Screen job applicants for

any history of violent behavior,
current abuse of violence-inducing substances such as alcohol and illegal drugs.

Investigate

every threat or suspected threat of violence,
every complaint of violence,
with investigators specifically trained in the dynamics of violent behavior.

Take immediate corrective action to

terminate any employee who seriously violates the policy, e.g., commits a physical assault upon another,
suspend any employee who commits a minor policy violation,
refer to an approved rehabilitation program any employee who commits a minor policy violation and who shows promise of rehabilitation, assist through an employee assistance program any employee who has been subjected to violence.

Follow-up to

ensure that every incident has been thoroughly investigated and documented,
ensure that employees who have returned to work following rehabilitation are not at risk of relapse,
ensure that victims of violence have been properly assisted,
ensure that any needed changes to security measures, such as access control, have been made.

FIGURE 20.1

Action items such as these can be useful in developing a single-scenario plan.

The credibility of the reporting system rests on its record, i.e., employees will make reports when they believe that reports will be handled quickly and effectively. The reporting system breaks down when reports have no follow through, are handled improperly, and when the promise of confidentiality is breached. Also, important to the success of any reporting system is management's encouragement to report incidents and not reveal the identity of persons making reports.

Procedures

The elements of a plan are spelled out in even greater detail by procedures. A procedure is a task or a combination of tasks. If the plan says that security officers must receive training in violence prevention, a set of procedures will specify the training topics, when and where the training will be held, who will conduct the training, who will attend the training, methods of training, testing, and so forth.

Procedures for dealing with workplace violence are very much like procedures for dealing with other emergencies such as fire, explosion, hurricanes, and so on.

The main indicators of violence are the following:

- Potential violence:
  - Showing approval of the use of violence to resolve problems.
  - Talking about guns and bringing gun literature to work.
  - Showing hatred for another or others.
  - Blaming others for imagined actions.
  - Talking about revenge.
- Violence during an early stage:
  - Bringing to or brandishing at work a lethal weapon.
  - Arguing out of the norm with coworkers and supervisors.
  - Bullying, intimidating, threatening, and harassing.
  - Making direct or veiled threats of harm.
  - Identifying with perpetrators of violence, particularly homicide.
  - Showing desperation over family, financial, and other personal problems.
  - Talking about suicide.
  - Abusing drugs or alcohol.
  - Exhibiting extreme changes in mood and behavior.
  - Acting in confrontational ways.
  - Sending notes or e-mails containing actual or implied threats.
  - Picking fights.
- Violence in progress:
  - Hitting, kicking, or throwing objects while angry.
  - Striking another or others.
  - Threatening another or others with visible possession of a weapon.
  - Screaming, yelling, and cursing in an irrational way.
  - Harming others in any way.

All of the above call for action; the actions will vary and be executed by different persons or groups. For example, a report of potential violence might call for supervisory intervention followed by counseling. Violence in progress will have a different set of actions: notifying key persons and groups, calling for law enforcement assistance, evacuating the danger area, dispatching security officers, setting up a first-aid station, calling to obtain the assistance of a medical treatment provider, and calling professionals skilled at defusing violent situations. Depending on circumstances, the fire department and a bomb squad or ordnance unit might be called.

FIGURE 20.2
A final step in ending a very serious situation can be intervention by a SWAT team. *U.S. Customs Bureau.*

The nature of a violent event will determine the nature of response. A key responder will always be the CSO because he or she leads the security group's response, is familiar with the nature of violence and the deadly force law, and is the company's liaison with law enforcement.

When the aggressor possesses or produces a lethal weapon, the rule of thumb is for all company responders to withdraw and turn the situation over to law enforcement. Fig. 20.2 depicts a special weapons and tactics team responding to an incident of workplace violence involving a lethal weapon.

Procedures acknowledge in their content the reality that violence is often unpredictable in timing and intensity but that injurious consequences can be lessened by being prepared to act swiftly and decisively. Preparation involves having needed equipment and supplies in ready condition, designating alternate responders, training responders, and conducting practical exercises. Where glitches occur during an exercise, procedures must be adjusted accordingly.

CHARACTERISTICS OF WORKPLACE VIOLENCE

Workplace violence does not "just happen." In fact, it can be anticipated. According to Heskett (1996), a workplace rife with stress and marked by antipathy between management and labor is like a powder keg waiting for a spark. Employee grievances are symptoms of trouble on the horizon. Some

forms of low stress are natural, even healthy, but high stress can be counterproductive and conducive to violence. High stress combined with a heavy-handed management and a workforce culture unable to assuage bitterness and resentment are the ingredients of volatility.

A method for determining the company's ability to prevent and respond to violence is to examine previous incidents. Questions that can be asked when looking into the past are the following:

- What was the nature of the incident and why did it happen?
- Could it have been prevented?
- Did any signals precede the incident?
- How effective was the company's response?
- Have steps been taken to prevent recurrence and to respond more capably?
- What can be learned from the past and put to good use in the future?

Of particular interest when examining the company's history of workplace violence is to identify patterns of risk and possible prevention strategies. The records may reflect, e.g., that a particular work group has had a greater number of violent incidents than other groups or that one group appears prone to committing serious acts of violence. Why is this the case?

Kelleher (1997) says not all characteristics of violence are likely to be apparent in security group records, such as obsessing over another individual, blaming others for personal shortcomings, vocalizing or rehearsing violent intentions, and exhibiting behavior that is strange to the extent it discomforts coworkers.

If too much work is assigned to one individual or if the conditions of work are harsh, violence is likely. When the workforce is too busy or uncaring about the activities of coworkers, the early indications of violent behavior will be missed. In some industries, culture has little significance, such as when employees work in many different locations, but a culture is certain to exist when many employees work at one location. If workers and management view violence as unimportant or in the nature of the work, the culture will follow suit.

Culture is strongly influenced by the way employees are treated. Are employees regarded as tools and is productivity the key driver? Predictors of trouble lie ahead when there is evidence of an "us versus them" attitude, specifically between labor and management, between subordinates and supervisors, and between workers generally.

At first, violence may be so minor as to escape notice, but when it reaches full bloom, it can be extremely harmful, both to the affected employees and the company at large.

Factors that mitigate violence and its consequences include the following:

- Employment of in-house specialists such as skilled practitioners in employee assistance, counseling, mediation, conflict resolution, health, safety, and threat assessment.
- Availability of specialists in the community such as psychologists, psychiatrists, therapists, and law enforcement officers.
- Management's determination and actions to prevent violent incidents.

It is wrong to think of workplace violence as "worker-against-worker" violence only. In the matter of homicide, which is the most serious of violent incidents, the norm is "outsider-against-worker" violence. Heskett (1996) reports that robberies result in the highest percentage of occupational fatalities in the United States. Convenience stores, liquor stores, hotels, and motels are a few of the businesses most susceptible to robbery.

The characteristics of most robberies are the following:

- Low risk for the robber.
- Use of a weapon, usually a handgun.
- A public facility that affords ease of access.
- For convenience stores, poor security such as no outside security lighting, no Closed Circuit Television (CCTV) camera, and windows covered with advertisements that block visibility from the outside.
- Location in a high-crime area.
- A history of prior robberies.
- General knowledge that the management of the target has a policy of "no resistance" to robbers that require cooperation by the employee and surrender of the assets desired.
- Use of a vehicle and easy accessibility to an escape route.
- Certainty of obtaining what is wanted, which might be cash, cigarettes, liquor, and so on.
- The target has a single attendant and few or no customers.
- Intimidation of the attendant and customers.
- Little or no planning.
- Spur-of-the-moment decision by the robber.
- Young age (the typical robber is 25 years of age or under).

Fig. 20.3 provides simple ideas for deterring late-night robbery.

Checklist for Deterring Robbery (Late-Night Retail Business)

If your business

requires employees to exchange money with the public, or
is open during the evening or late hours, or
is in a high-crime area, or has experienced a robbery, a violent incident,threats, harassment or other abusive conduct in the past 3 years.

Do these things

keep more than one employee at the business site during operating hours,
provide employees with an emergency signaling system, e.g., a robbery or duress alarm, and at a minimum, an outside telephone line,
post emergency telephone numbers adjacent to the phone,
ensure that the entrance to the business is easily seen from the street,
ensure bright lighting around the entrance, adjacent areas, and parking lot,
ensure that indoor lights work properly and are on,
ensure that views from the outside are clear of obstructions,
place the cash register in plain view,
install a drop safe or time-access safe,
enforce strict cash control rules, e.g., when and how to store cash in the safe,
install security cameras,
install a bullet-resistant enclosure for employees if thebusiness has a history of robberies and assaults,
develop proactive and reactive procedures, e.g., how to spot the early indicators of a robbery attempt and how to report a serious incident. Keep the procedures on hand and train employees to follow them,
train employees in conflict resolution and how to respond to violent behavior, post anticrime signage, e.g., signs declaring that only a small amount of cash is kept in the register and that security cameras are operating, enforce strict procedures for opening and closing the business.

FIGURE 20.3

Retail businesses operating late at night have a higher than average rate of robbery, and the violence that accompanies the crime.

CRITICAL THINKING EXERCISE

A convenience store clerk was shot and killed in a daytime robbery. The deceased clerk's wife sued the convenience store, alleging inadequate security. The defendant argued that it owed no duty to the clerk because there had been no prior similar crimes on the premises, therefore making the robbery and murder unforeseeable.

After hearing the testimony of an expert witness, the court disagreed with the defendant. The expert witness had described the "inherent risk of robbery and violent crime in the convenience store business" and also pointed out several security inadequacies at the store such as poor visibility from the outside, poor lighting, no security alarm, no video camera, and no training of employees on security measures. The court ordered the convenience store owner to pay the dead clerk's wife $1.8 million, an award later upheld on appeal.

Is this case an incident of workplace violence? Whether you say yes or no, defend your decision.

ASSESSMENT

An analogy is appropriate. A policy tells us the destination, a plan tells us the route, and procedures tell us how to get there. An assessment evaluates the plan and its procedures (key tasks). Essentially, the merger of a plan and its procedures is a program. In this case, we have an antiviolence program. The program should identify the following:

- Strengths and weaknesses. Assessment by a third party is a good choice because it can eliminate the bias and blindness that tend to creep into a program developed in-house.
- Key tasks of preventing and responding to violent incidents.
- Equipment, supplies, and other resources that must be on hand to properly perform the key tasks.
- Individual positions and groups inside and outside the organization that perform the tasks in partnership.
- Interactions among and between the partners.
- Training that is needed to ensure effective performance.
- Jurisdictional issues such as police authority versus the company's authority.
- Security force interactions such as the working relationships between guards and console operators and between supervisors and subordinates such as that depicted in Fig. 20.4.

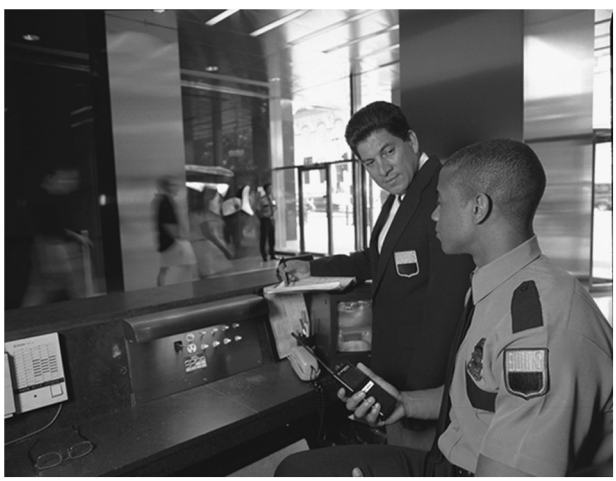


FIGURE 20.4
A professional security presence is a deterrent to crime, including violence. *Burns International Security Services.*

When the assessment focuses on the security group, much light is cast upon the readiness of other groups. Simply stated, the security group cannot perform its assigned tasks when other groups fail to perform their tasks.

Task performance is enhanced when the antiviolence program is supported by persons in positions of authority. These are typically persons holding management positions and possessing the authority to assign responsibilities, dedicate in-house resources, purchase needed equipment, negotiate agreements with outside agencies, order training to be done and exercises conducted, evaluate results of exercises, and correct noted weaknesses in program execution.

The assessment ends when all facts have been gathered and analyzed. Analysis should be able to answer a few basic questions, as follows:

- What types of violent acts can be expected?
- What can be done to prevent or reduce the negative effects of anticipated violence?
- What does the organization have and not have in the way of pertinent expertise and material resources?
- What can be done to close gaps in the ability to prevent and respond?

READINESS

Readiness is demonstrated when the assessment exercise reveals the absence of flaws. However, readiness is a condition subject to change, both anticipated and unanticipated. Examples of change are new threats, responders leaving the company, loss or deterioration of equipment and supplies (such as personal defense equipment for security officers and first-aid supplies), and refresher training not conducted with sufficient frequency.

Change must be addressed. The CSO is in a good position to detect change and take corrective action within the security group and to recommend corrective action by other groups.

Readiness also incorporates mitigation. Certainty that prevention will always work denotes poor planning. Procedures must be in place to deal with the aftereffects of violence. At a minimum, mitigation is having a capability to administer first aid, rapidly acquire medical treatment, either on scene or by transport to a medical facility, evacuating potential victims to safe locations, informing the general population of the workforce that a violent incident is occurring and that predesignated safety measures must be taken.

Training

Instruction in how to respond to workplace violence is needed more by the security group than by any other organizational unit. The knowledge and skills imparted to security group members through training are mirrored by tasks specified in the antiviolence program. If the program requires security officers to use calmative techniques when first confronting a violent employee, the officers must be taught the calmative techniques. If the program requires security officers to summon the police at a certain point in an escalating situation, the officers must be taught to recognize the certain point when it occurs.

Ranking tasks by criticality is central to effective training. Tasks with life safety implications deserve highest training emphasis. They must be taught, they must be learned, and they must be practiced.

The CSO, in addition to ensuring competence through training of security group employees, is often called upon to help train employees outside the security group. Three employee categories stand out: the general employee population, managers and supervisors, and a small group of specialists comprising the violence response team (VRT). It is interesting to note that the CSO can be a trainee and a trainer in all three categories.

A key objective in training employees is to ensure understanding of and support for the company's antiviolence policy. Topics can include the nature and consequences of workplace violence, policy enforcement, and the responsibility of every employee to abide by the policy such as not engage in aggressive behavior and report those who do.

Another objective is to make employees aware of actions they may be required to take during a violent incident in progress, such as move to safe places, lock doors, or leave the premises.

Being members of the total work population, managers and supervisors should receive training as described above. In addition, they should receive instruction in the following:

- Their individual obligations to support the organization's workplace violence policy generally and their specific, procedural duties as expressed in the antiviolence program.
- How to look for and recognize the early warning signals of violence.
- How to intervene, document, and report incidents of violence.
- Evaluating the effectiveness of the antiviolence program and making recommendations for improvement.

The members of the VRT are expected to be competent in their own disciplines prior to being trained in the specifics of the antiviolence program. Persons on the team who are designated to mediate in crises are expected to possess mediation skills by virtue of prior education and experience. The same expectation applies to other members of the team, such as the CSO. He or she is expected to have skill in leading and directing the activities of security officers during a crisis situation, knowing the particular capabilities of particular weapons, knowing the law in respect to the use of force, and understanding the dimensions of antisocial behavior.

The principal objectives in training the VRT are to know the following:

- The name and authority of the person in charge.
- The team's chain of command.
- The composition of the team according to members' names and professional credentials.
- Personal duties/tasks and the duties/tasks of comembers.
- Methods of communication.
- Interactions within the team.
- A range of intervention tactics.
- Call-out and deployment of the team.

A supplemental benefit of VRT training is the positive effect of merging separate disciplines to accomplish a common goal.

RESPONSE

Companies that have developed antiviolence programs say that managers and supervisors supported by knowledgeable and skilled individuals have a greater chance to prevent and bring to a successful conclusion situations involving disruptive and intimidating employee behavior. These knowledgeable and skilled individuals are members of the VRT. A team approach enhances greater odds of success because it offers the promise of creative solutions that might otherwise not be considered.

To ignore behavior that forecasts, the possibility of violence is to ask for trouble—trouble that can be enormous in consequences: they include injury, death, damage to or loss of critical assets, disruption of business operations, loss of productivity, reduced employee morale, key employees leaving the company, lost business opportunity, loss of public confidence, reputation damage, loss of customers, and the risk of criminal and civil liability. The cost of investing in a proactive antiviolence program is miniscule in comparison to potential losses.

CRITICAL THINKING EXERCISE

The walls of Frank's cubicle were covered with photos and military citations going back to when he served in the U.S. Army. Frank, an outgoing person, often spoke to coworkers about his fine collection of guns and his membership in the National Rifle Association. A bumper sticker on Frank's automobile bore the words "... when they pry my cold dead fingers ..." Frank displayed no emotion when informed by his boss that he was one of several hundred employees to be let go in a restructuring of the company. He politely declined the company's offer of counseling to help him find work elsewhere and was uncharacteristically silent while being out-processed by a human resources specialist.

A week later, Frank returned to the job site. The lobby receptionist called Frank's former boss to obtain authority to issue Frank a visitor's pass. After shaking hands with his former boss, Frank calmly removed a 45-caliber pistol from a shoulder holster under his jacket. He shot his former boss in the chest, killing him instantly. Frank put the pistol back in the holster and sat down in a chair to wait for the arrival of the police.

Is this an incident that could have been anticipated, and if so, what actions should have been taken before it happened? If you believe the incident could not have been anticipated, explain your reasoning.

Dealing effectively with hostile and intimidating situations creates a safe and productive environment, which happens to be an obligation of management. Prompt and decisive intervention has a deterrent effect on employees contemplating violence. The frequency and severity of physical violence can be reduced when violence-prone employees clearly understand that such behavior will not be tolerated and that discipline of one kind or another will be applied in every case.

In addition to the CSO, the members of the VRT typically include representatives from human resources, organizational health, safety, public affairs, building management, legal affairs, and unions when applicable. Although many disciplines may be represented on the team and are essential to success, only a few members will be involved in directly responding to violent incidents. The primary responders come from the security and human resources groups. Nonengagement members of the team assist in a variety of ways, e.g., rendering medical aid, negotiating release of hostages, dealing with the media, coordinating evacuation if needed, notifying and assisting law enforcement if needed, and partnering with union representatives if applicable.

A multidisciplined composition of the VRT helps it:

- identify the resources and expertise needed to capably prevent and respond to violent situations,

- carefully and honestly evaluate the organization's current prevention and response capabilities,
- identify and compensate for weak or missing human competence,
- anticipate situational changes and be prepared to change with them, and
- provide insight and input to VRT operations with respect to understanding the psychological dynamics of violence in progress.

INTERVENTION

Intervention is not always a function of the VRT. The most desirable form of intervention is one that defuses violent behavior before it occurs, as would be the case when a supervisor intervenes when he or she spots or is informed of a subordinate displaying the early signs of aggressive behavior. Intervention in this sense is not physical restraint: It is using calmative language and gestures, encouraging the aggressor to vent frustration through dialog, demonstrating sympathy, and, on some points, agreeing with the aggressor. Sympathy and agreement may be not entirely genuine but are forgivable when they are the supervisor's one and only recourse.

A supervisory tactic that nearly always fails and in many cases triggers escalation is confrontation. While the common understanding of intervention is to confront, the nature of the confrontation should not be adversarial. A Clint Eastwood approach is taboo.

An important element in intervention is to determine if the aggressor possesses a means to inflict injury or death or has a capability to damage the employer's assets. In use of the word "means," we are talking about lethal weapons such as firearm, knife, bludgeon, or bomb. In use of the word "means" in respect to the employer's assets, examples include a heavy wrench to damage equipment or a blow torch to start a fire. Damage to company assets often include destroying paper and data files, planting a virus or a Trojan horse in the computer system, and providing sensitive data to competitors.

A second matter to be considered is the capability of the aggressor to act. If the weapon is a knife with ruler, capability in the sense used here does not exist or is severely limited.

Third is the perceived intent of the aggressor. Statements like, "I hate all of you," and "I'm going to get even if it is the last thing I ever do" are not revealing of intent because they are statements commonly made during temporary anger. On the other hand, intent is revealed when the aggressor points a pistol at a person and says, "Prepare to die."

Finally is the matter of immediacy. Is the aggressive action occurring right now? A supervisor who arrives at the scene after being told of the situation might find that the incident has come to a close. However, if the incident has a possibility of immediate repetition, calling out the VRT may be appropriate. It would be the supervisor's call to make, and that is what a supervisor is expected to do: make difficult decisions. To summarize, the supervisor should determine if the aggressor:

- Has the means to commit violence. Brandishing a 12-in ruler is not a means for inflicting serious injury or death.
- Has the intent to act. Intent is not present when the aggressor is not specific in stating an intended action, does not go beyond making a warning, and calms down and returns to work.
- Is in the threatening mode at that very moment. The need to intervene with physical restraint is not appropriate when the incident has ended or appears to be in the process of ending.

Irrespective of the situation is a requirement to document the incident and make a report up the chain of command. These supervisory duties should be done without the knowledge of the offender, except when the incident is minor and intervention consists of counseling. The decision to refer the offender to a medical treatment provider is best handled by the human resources group.

PSYCHOLOGICAL PROFILING

The term *psychological profiling* tends to conjure up a mental picture of a massive police hunt for a diabolical killer too clever to be caught by standard police techniques. In a sense, it's unfortunate that profiling is so widely misunderstood. First, the technique is not restricted to serial murders and is not practiced solely by Federal Bureau of Investigation agents. Next, it is not a scientific procedure in the same way that fingerprints and DNA tests conclusively identify individuals. Both in art and science, psychological profiling is performed by highly trained and educated behavioral scientists with long experience in the field.

Psychological profiling can be effectively used in the business setting. The uses may be to link a particular employee to an anonymous threat, evaluate the possibility that an employee will harm herself or others, or determine if an employee's on-the-job behavior suggests a potential for violence. Profiling has proven itself in a wide variety of corporate-related crimes such as product tampering, sabotage, extortion, and kidnapping.

A single written communication, such as a threatening letter to a chief executive officer, can provide clues to the author: age, sex, marital status, intelligence level, life style, work habits, motive, and emotional stability. These characterizing details can be applied to a population of suspects for the purpose of ruling some in and some out.

When an individual's identity is known, profiling can be used as a predictor of behavior. If a corporation, e.g., has an employee who has a history of borderline behavior, a profile can be helpful in assessing future behavior so that an intelligent decision can be made as to whether or not the employee should be reassigned, counseled, treated, or terminated.

CRITICAL THINKING EXERCISE

Jake, a machinist in an aircraft manufacturing plant, angrily confronted a quality control specialist named Anna. He accused her of unfairly rejecting his work output. When she tried to explain that all work output had to meet precise technical specifications, he told her she was like all women who tried to do a man's job. "You can't handle the stress so you take it out on the men." Before storming away, Jake called Anna a whore and told her he would "punch out her lights" if she didn't stop picking on him.

Anna reported the incident to her supervisor, Harkins. "I don't want to get him in trouble," she said. "But I do want him to stay away from me." Harkins took no notes. A week later, Jake once again confronted Anna. This time he called her a bitch and said he would "punch her silly if she didn't get off his ass." Anna did not report this second incident with Jake. She did, however, continue to reject his unacceptable output, as she did the unacceptable output of other machinists.

In the middle of a workday, shortly after the machine shop had completed a rush project, Jake went to Anna's workstation and pointed a finger in her face. He told her she was "dead meat." Again, Anna did not make a report.

At 5 P.M., as Anna walked to her car in the company's parking lot, Jake stepped from behind a van and blocked her path. He punched her in the face, knocking her to the ground. Other employees on their way to their cars rushed to Anna's aid but were too late to prevent Jake from kicking her twice in the head and once in the abdomen. Jake fled.

A plant security officer drove Anna to a local hospital where she received 16 stitches to close a facial laceration. A nurse called the police and Anna filed a complaint.

Jake was fired. He pled no contest to a criminal charge of aggravated assault and was placed on probation. Anna left the aircraft plant for a quality control job elsewhere. Within six months, she filed a civil suit alleging negligence by her former employer and Harkins.

Was this a preventable incident? Explain your answer. If you believe the incident was not preventable, explain your reasoning.

LIABILITY

The Americans with Disabilities Act (ADA) is widely regarded as the most sweeping nondiscrimination legislation since the Civil Rights Act of 1964. The Act provides broad nondiscrimination protection in employment, public services, public accommodation, and services operated by private entities, transportation, and telecommunications for individuals with disabilities.

In the context of the ADA, Jones (2006) defines the term "disability" with respect to an individual as (1) having a physical or mental impairment that substantially limits one or more of the individual's major life activities, (2) having a record of such an impairment, or (3) being regarded as having such an impairment.

Relevance of the ADA to workplace violence is mainly connected to hiring and firing of persons who claim to be disabled as per the ADA definition. Hiring a physically impaired person poses a relatively minor risk compared to hiring a mentally impaired person whose impairment involves previous violent conduct. Firing an employee for committing an act of violence, whether impaired or not, is a different story because ADA protection does not apply. However, if the company did not have a policy prohibiting the act of violence committed, the terminated employee might be successful in a civil suit alleging wrongful termination. An antiviolence policy that does not exist or is poorly crafted can help the offender escape the company's sanction and, in addition, receive a monetary award at the company's expense.

Along a similar line, the Equal Employment Opportunity Commission (EEOC) might view the termination as discriminatory if the company failed to terminate other employees for the same or similar offense.

Inbau et al. (1996) state that employers who are covered by the Federal Rehabilitation Act and the ADA, which prohibit discrimination against "otherwise qualified" disabled individuals, or by one of the many state laws similarly prohibiting disability discrimination may find that their possible range of sanctions immediately following a positive (drug or alcohol) test is limited by a duty to "reasonably accommodate" an employee who claims disability on the basis of drug or alcohol addiction.

Allegations of wrongful conduct seem to pop up with regularity. One of them relies on the concept of *respondeat superior*, which holds that "the master is responsible for the acts of his servants." The common defense, which most often is successful, is to demonstrate that the duties of the offending employee did not include performance of the violent act committed.

Negligent Hiring

Negligent hiring can be alleged when a person is injured by an employee. (Note that the definition of injury in civil procedure is physical or mental injury or damage to property of another.) The essence of the allegation is that the employer hired the offender with knowledge that the offender had committed similar crimes in the past. A defense might be that the employer was required to hire the offender as per ADA or EEOC rules or the employer had informed the offender's coworkers of the prior offenses, the assumption being that they will be cautious in their dealings with the offender.

Wrongful Termination

Wrongful termination can be alleged when the offender was treated more harshly than employees who had committed identical or similar offenses. Unfair treatment could be suspension without rehabilitation that had been afforded to others but not to the offender. Other wrongful termination suits can allege racial, gender, age, religious, and political discrimination.

Nondisclosure of Problematic Performance

An employer can face liability for nondisclosure of problematic employee performance, for example, when representing a former employee's performance was favorable when in fact it was marked by violent behavior. A foreseeable risk of harm to others is created when a violence-prone individual is hired by another company that relies on a former employer's statement.

Inadequate Security

Inadequate security is a claim that the plaintiff was the victim of violence that would not have occurred if the employer had provided adequate security. To prove the case, the plaintiff might present evidence that the employer knew of the inadequacy of the security that made it possible for the offender to act and the employer did nothing beforehand to offset it. The offered evidence might be previous incidents of violence on or near the employer's premises, location of the premises in a high-crime area, and not providing security officers.

Avoiding Liability

Liability can be avoided by a proactive approach to violent behavior. The most obvious and most effective element of the approach would be to screen job applicants thoroughly, being careful meanwhile to avoid discrimination on any grounds. Charges of unfairness in hiring can be resisted by clearly stating up front that persons with a history of violent behavior will not be

considered for employment and by placing into job descriptions a standard that requires the incumbent to possess positive interpersonal skills. It is simply good practice to turn down job applicants who are found through the preemployment screening process to be lacking in a skill related to the job. However, caution and commonsense apply. If the job does not involve interacting with other people, a job standard that requires interpersonal skills is susceptible to challenge. On the other hand is the comfort that nearly every job will require interaction with humans in one manner or another.

Next would be to expressly state in writing and through other forms of communication that employees are prohibited from engaging in any form of on-the-job behavior that constitutes violence, no matter how minor, or that suggests possible future violence, and to act immediately and decisively when the prohibition is not observed.

Caution

Action taken against an offending employee must not be punitive or appear to be punitive. Also, the action should be commensurate to the violation. For example, verbal epithets directed at a coworker may signal future violence but are not inherently violent. For a management to say that violent behavior in the workplace will not be tolerated is not the same as saying that all forms of violent behavior will result in termination. Because there are degrees of aggressive behavior, there should be degrees of corrective action. It should also be recognized that an employee may commit a minor violation over and over again, with each separate violation being corrected with a separate admonishment. Has the corrective action worked in this case? No, it has not. Should a more serious corrective action be taken? Perhaps.

Think also of progression: an employee commits a minor violation and is admonished; soon after, he commits a moderately serious violation and is sent home from work; next, he commits a more serious violation and is suspended. Should management terminate him at that point or wait until he commits an even more serious violation that calls for termination? Stated another way, should management wait until the employee hurts someone before excluding him from the workplace?

CRITICAL THINKING EXERCISE

Several warehouse workers have complained to their boss, Robert, that a coworker, Karl, has a bad temper. Among other disruptive acts, Karl has cursed loudly, made threats, and shook his fist at coworkers. After he shoved a female coworker and told her he would kill her, Karl was called into Robert's office. While Robert was explaining the unacceptability of Karl's behavior, Karl ran his hand across his throat to symbolize decapitation. Robert sent Karl home and suspended him for 3 days. A memo from Robert to the human resources group documented the offense and HR added it to Karl's documented prior offenses.

A month later, Karl got into a dispute with Luke, a fellow warehouseman, and slashed his throat with a razor-like tool used to open cartons. Luke died at the scene. Luke's wife had a friend in the human resources group. The friend gave her a copy of the file that described all of Karl's offenses. Shortly following Karl's conviction in criminal court, Luke's wife filed a civil suit against the company and Robert.

What do you think the outcome of the civil suit will be? What allegations can be made against the company? Against Robert?

CONCLUSION

The CSO's obligations in the matter of workplace violence include a critical examination of the working environment, including parking lots, entryways, and public areas such as reception areas and an entry lobby.

Many people who become violent communicate their intentions in advance. Threats from anyone should be reported, analyzed, and acted upon. A proven way to prevent violence is to foster a day-to-day attitude of respect and consideration among the workforce.

The practice of not allowing weapons, such as firearms, swords, spears, and other lethal items, is a sensible practice, and compliance of the practice should be monitored by the CSO.

Very important to detecting the early signs of violent behavior are coworkers willing to report the early signs of violence and supervisors capable of dealing with them. Also very important to defusing a violent action is a competent VRT whose members are able to work together.

An antiviolence program should be built on a plan and a set of procedures that are well understood through training and practiced in hands-on exercises.

REVIEW QUESTIONS

1. What is the major difference between a policy and a plan?
2. Name and describe five main elements of a workplace violence prevention plan.
3. Name eight indicators of workplace violence in the making.
4. The major cause of workplace violence can be summarized in a single word. What is that word?
5. Give an example of intervention.
6. Give one example each of negligent hiring, wrongful termination, and inadequate security.

References

Capozzoli, T., McVey, R.S., 1996. Managing Violence in the Workplace. St. Lucie Press, Delray Beach, FL.

Heskett, S.L., 1996. Workplace Violence: Before, During, and After. Butterworth-Heinemann, Boston, MA.

Inbau, F.E., Farber, B.J., Arnold, D.W., 1996. Protective Security Law. second ed Butterworth-Heinemann, Boston, MA.

Jones, N.L., 2006. The Americans with Disabilities Act (ADA): The Definition of Disability. University of North Texas, Denton, TX.

Kelleher, M.D., 1997. Profiling the Lethal Employee. Praeger Publishing, Westport, CT.

CHAPTER 21

Employee Awareness Program

What You Will Learn

- The goals and nature of an employee awareness program.
- The supervisor's role in ensuring compliance with an employee awareness program.
- The modes of educating employees concerning employee awareness program.
- The role of the Chief Security Officer in developing and operating the employee awareness program.
- The workplace culture and how it affects security compliance.

INTRODUCTION

The security of an organization rests squarely on the practices of employees. The Chief Security Officer (CSO) can design the finest protective programs, obtain the full support of the management team, secure generous funding, form a competent security group, and acquire a complete assortment of equipment. None of these components will matter, however, if employees fail to meet their individual security responsibilities. A security agenda, no matter how perfectly conceived and generously supported, is incapable of rising above poor security practices by employees. Like the analogy of the weak link in the chain, an organization's security cannot be stronger than the weakest day-to-day behaviors of its employees.

GOALS

The subject of employee behaviors leads to a question: How does the CSO influence employee behaviors? The answer is: CSO influences employee behaviors by making employees aware of security. In this sense, awareness has three goals: help employees understand their individual security responsibilities, help them meet those responsibilities, and help them engage the first two goals willingly. The first two goals require the employee to gain

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00021-9

knowledge and help them through encouragement. The third goal is distinctly different and almost always difficult to attain because it calls for an attitudinal shift. To illustrate the point, imagine that Bill Smith, a clerk in the accounts payable office, is ready to go home. He knows the rule that requires him to lock away check stock and he knows how to operate the combination dial on the check stock safe.

But Bill is tired, quitting time has come and gone, and Bill is eager to leave. Will he take the time needed to lock the check stock in the safe? His willingness will be the determining factor. Bill knows the rule and has locked and unlocked the safe hundreds of times. But will he do so now? Much depends on Bill's attitude, and the reality is that Bill's attitude, and that of every other employee, is difficult to shape. The CSO can teach "the why and the how" of the rule but cannot easily teach the attitude that influences compliance.

Yes, the CSO may be positioned to trigger punishment of Bill if he fails to lock the safe, thereby administering a valuable lesson to Bill (or so we would hope). One method for "attitude adjustment" is through individual employee counseling sessions that emphasize the importance of following security protocol. However, influencing attitude is easily attempted but never easily accomplished.

Awareness is an Ongoing Process

An employee awareness program is routine and ongoing. It is not a one-time effort or an effort that clicks on in response to loss events and clicks off again when things settle down. Although a program may be initiated with great fanfare and periodically reinvigorated, it must operate continuously.

Awareness is Local

Employee awareness is a local affair that serves the unique needs of the business unit. Although security topics may be suggested from outside of the business unit, the program is principally dedicated to raising awareness of internal security issues.

Squarebriggs (1999) points out that when the content of the awareness program aligns with the experiences of employees, a psychological agreement is reached. The content of an awareness program conducted elsewhere will seem alien to the local audience. This principle applies as well to the content of awareness programs purchased off the shelf.

Organizations that are regulated in some way, such as by the Environmental Protection Agency (EPA), may find an employee awareness program essential to meeting EPA requirements. A single security error can cause serious

problems. For example, EPA regulates drinking water systems. If an employee allowed an unauthorized person into the control center of a water system and the system was compromised, either deliberately or by mistake, the company would want to know: "Was the employee aware that the control center was off limits to outsiders?" If the employee can show he or she was not aware that visitors were forbidden to enter the control center, the CSO might be asked to explain why the employee awareness program failed in this important respect.

AWARENESS PROGRAM

Every forum that can possibly influence the security behaviors of employees is up for grabs in an energetic awareness program. Fig. 21.1 is an example of a security group employee promoting employee awareness in a casual conversation over coffee. Security fairs, slogan contests, posters, awards, and all things imaginable should be considered, and brainstorming can be the vehicle for surfacing unique ideas.

Tyson (2002) says that if one accepts the premise that security is a weak-link discipline, then no organization can truly approach being "secure" unless it considers all its risks when crafting overall security strategy and formulating risk mitigation decisions. Reading between the lines of Tyson's statement is the need for management to strengthen the security discipline in order to attain security objectives. A tried and true method for strengthening security

FIGURE 21.1
The opportunities for spreading the security message are boundless.

is education of people responsible for improved security. The people we are talking about comprise the entire workforce.

Message style and mode of delivery should vary according to the audience. Although a message might remain constant, style and delivery should vary at different levels of the organization. For senior management, a higher level of language is appropriate and a visit by a person of standing, such as the FBI agent in charge of public affairs or the chief of the local police department, can serve the education program, as well as promote cooperation with the two important agencies. For supervisors and their subordinates, the venue can be departmental conferences, brown-bag lunches, and floor warden training sessions.

Apathy

Apathy arises when the awareness program suffers from vagueness and imprecision. Employees are like moviegoers: if bad writing and bad acting make a movie a clunker, some of the audience will fall asleep, others will get up and leave, and some will inwardly curse for having wasted the price of a ticket. Apathy can arise quickly and exert a devastating effect. The worst thing that the CSO can do is to surrender to it. Doctrine of The National Crime Prevention Institute holds it is true that some individuals may be apathetic on principle to the whole notion of employee awareness; it is also true that employee apathy is often offered up as an excuse for program ineffectiveness.

THE MESSAGE

When selecting a topic, it is helpful to ask: Is the topic important enough to address? If the answer is "yes," then ask: Is the content of the topic doctrinally correct? Is content consistent with company policies and practices?

A topic that is long or complicated can be broken down into comprehensible parts. The parts can be arranged in a logical series, with each part building on the other. Packaging the topic imaginatively is also important. Going outside the box of traditional techniques grabs attention. Even a small dose of innovation can turn ho-hums into a buzz of excitement, and there is nothing wrong with emulating the techniques of professional idea marketers or borrowing from the successful techniques used in employee awareness programs of other organizations.

The avenues for raising employee awareness include presentations at employee meetings and bringing in outside experts to address topics of concern such as having a bomb-threat specialist teach mailroom employees how to spot parcel bombs. Fig. 21.2 presents tips on developing a presentation. Conducting tutorials that meet special needs can be effective, such as

Tips on Developing a Presentation

Research the topic. Gather all the information you can.
Organize the gathered information.
Prepare to write.
- Know your purposes.
- Identify main ideas.
- Prepare an outline.

Write a draft.
- Avoid big words and jargon.
- Use active (as opposed to passive) verbs.
- Avoid adjectives that suggest opinion. A presentation should be factual.
- Avoid crutch terms and deadheads, such as "in light of" and "in compliance with."
- Keep sentences short and punchy.
- Support the main ideas with examples, facts, and reasons.

Read your draft and revise it twice.
Have your draft critiqued by one or two persons whose judgment you trust.
Revise one last time.
Choose the appropriate methods for supplementing lecture, e.g., slides, transparencies, films, videos, handouts, chalkboard, and block paper on an easel.

FIGURE 21.2
Developing a presentation is more important than delivering it.

showing secretaries how to mark envelopes that contain sensitive documents about to be mailed, and teaching new hires the fundamentals of the fire alarm system.

Awareness messages can be placed on static and electronic bulletin boards, on the security website of the company's intranet, on placards in public hallways, and on signage in high-risk locations. Helping employees protect themselves from crime can be a facet of the employee awareness program. Activities along this line can include directing employees to community-operated anticrime programs that deal with burglary, assault, and other crimes. Employees can be assisted with advice about

- Installation of home alarm systems.
- What to do when the employee's automobile breaks down on a highway.
- Procurement of a cell phone.
- Joining or starting a neighborhood watch program.
- Being watchful in mall parking lots.
- What to do when the employee is put in fear of assault or robbery.

The Spotlight

The CSO can be writer, director, producer, and actor. He or she can ideate the story line (program objectives), write the dialogue and action scenes

(program content), select the actors (program presenters), direct the program, obtain the funding, and bring all the parts together into a meaningful production.

WORKFORCE CULTURE

The first that can be said about a company's workforce culture is that there are many and varied cultures; each department within the company, from mailroom to executive suite, has its own culture set. The set is driven by the nature of the work within the department. It can also be driven by the nature of work outside the department such as a rivalry between two or more departments in productive output. For example, workers on a production line might compete with or even disagree with workers charged with enforcing quality control standards, with workers introducing raw materials to the beginning of the line, or workers moving the finished product from the end of the line. Cultural difference can exist within departments as well. It is no secret that salespersons compete with one another, not necessarily on the grounds of income but on the pride that accompanies "outselling" a coworker. Also, the sales department, which might market several products, will have cultural differences between persons selling different products, usually in different venues, and using different techniques.

Complicating the mix of cultures are social, ethnic, and economic differences between employees. Further still, and more importantly, is the influence of what each employee expects to personally get out of his or her job. Some employees simply like the work, others like the socialization that accompanies the work, and still others strive for advancement, and if they cannot find their goal or see it on the horizon, they jump to a company with better possibilities. Finally, there are employees who do not like the work, complain about it, and look for opportunities to avoid work. These many differences face the CSO when he or she tries to sell an overall package of security that embraces all workers. There is also a cultural drive to be better than the other company, such as a competitor, or exceed the best practices of the industry.

Like other departments, security employees have their own set of cultural values. Usually, there is a firm belief that every security employee, irrespective of cultural beliefs, has an obligation to practice good security habits to be an example for the entire workforce. Do all employees accept the obligation? Do all employees care if the entire workplace benefits from good security practices? The answer is "no," and herein lies the CSO's challenge.

The second that can be said about a company's culture is the influence upon it by senior managers and supervisors. Workers at lower levels are always on

the lookout for superiors who arrive late, go home early, do not visit their departments, do not give "atta boys" when merited, are only interested in containing costs and increasing productivity, and are quick to pull the trigger on terminations.

Purpura (2002) says that a supervisor can be perceived as *an agent of socialization* . . .. In a business organization, a supervisor becomes an agent of socialization after establishing a working relationship with a new employee. Socialization according to Purpura means bringing a subordinate into the working group, guiding the subordinate in the performance of tasks, and, in terms of security education, ensuring compliance with the company's security program.

The persons closest to workers are their supervisors. It has been said before, and it is important to say again, that nothing works when supervisors are not cooperative. The CSO should recognize this cold hard fact and give strong emphasis to educating supervisors, and when education does not seem to be working for some supervisors, go the extra mile such as one-on-one meetings, or being in the coffee room where a supervisor is known to be at a particular time, or taking a seat alongside a supervisor in the cafeteria at lunchtime. Another effective method is to get people working under a recalcitrant supervisor to change his or her mind. Least desirable is to go over the supervisor's head. If this action is necessary, the CSO must have indisputable facts that omission of employee awareness by the supervisor has led to security breaches, especially those forbidden by security policy.

Employee awareness can be seen in the individual actions of employees. Awareness can be manifested in actions such as cooperating with the security guard force; stopping strangers on the premises to determine if they are there with permission; keeping hallways (escape routes) free of obstacles; locking desks, containers, and offices; shutting off coffee machines at the end of the day; and reporting unusual incidents.

Separate cultures often revolve around activities enjoyable to employees such as playing on a company softball or bowling team, attending the same church, and holding common views. Informal groups often have a member with connections to persons of higher authority. Because they are liked or can influence other employees, management will listen to what they say, which often moves along the company's grapevine.

A workplace culture, although disparate in many ways, can be educated in a single theme: employee awareness. The trick behind accomplishment of the goal is to have management communicate its belief in the program, garner support of supervisors, and gain cooperation of all workers, from top to bottom.

CONCLUSION

Without the willing cooperation of employees and complete support of supervisors and upper management, the awareness program cannot succeed.

Effectiveness of the employee awareness program is a CSO's responsibility. This is more than just assuring presentation of a meaningful and interesting program; it requires involvement of the CSO in convincing supervisors and management to be supportive, gaining the confidence of employees, and ensuring they understand their personal responsibilities.

An awareness program that has no relevancy to the particular security needs of the organization will be a waste of time. For example, if the organization is a storage and beer distribution company, employees working in a warehouse or driving trucks do not need to be taught how to protect sensitive data.

The beliefs and values of employees, both individually and collectively, should be respected. An absolutely incorrect approach is to force employees to abide by security rules. They must be convinced that security has a value to them and to the company.

REVIEW QUESTIONS

1. What is the primary goal of security awareness?
2. Name and describe at least three methods for "selling" the security awareness program.
3. What is the role of the CSO in developing a security awareness program?
4. What is meant by the term workplace culture?

References

Purpura, P., 2002. Security and Loss Prevention. fourth ed Butterworth—Heinemann, Boston, MA.

Squarebriggs, R., 1999. Coach is better than security supervisor. In: Robert, R.R. (Ed.), Issues in Security Management: Thinking Critically about Security. Butterworth—Heinemann, Boston, MA, p. 25.

Tyson, D., 2002. Security Convergence: Managing Enterprise Security Risk. Butterworth—Heinemann, Boston, MA.

CHAPTER 22

Vulnerability Assessment

What You Will Learn

- The purpose of a vulnerability assessment (VA).
- Steps in conducting a VA.
- The major difference between VA and security inspections/reviews.
- The meaning of "single point of failure."
- Three judgments that must be made in assigning criticality to an asset.
- The purpose of an exit briefing.

INTRODUCTION

Vulnerability assessment (VA) is a methodology for determining the vulnerability of an asset or assets at risk of being lost, taken, damaged, or destroyed. As such, the VA can be used as a tool for managing threats, or if you prefer, managing the risk that accompanies threats. Threats come in a wide variety. First are threats of nature such as flooding, hurricanes, earthquakes, etc. Second are accidents such as fire, breakdown of equipment, and collapse of a structure. The third category poses the greatest threat, what are called man-made threats such as crime, sabotage, and terrorism.

When the Chief Security Officer (CSO) thinks of terrorism, he or she must not ignore the possibilities of terrorism committed by homegrown individuals, such as Timothy McVeigh and Eric Rudolph, and domestic groups such as the Aryan Nation and the so-called Skinheads.

In this chapter, the word "vulnerability" means weakness in security, and when reference is made to a "target," think of a physical entity or process important to the operation of a business. A target can be one or more critical assets within a business facility, or the facility and all the critical assets within it, or a combination of several facilities and their critical assets. A critical asset is synonymous with the term target, that is to say, a physical entity or process

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00022-0

essential to the operation or even survival of a business. Making an asset difficult to compromise is known as "target hardening."

Although you will find in this chapter an occasional reference to nonbusiness targets, such as symbolic monuments and government buildings, keep in mind that the main thrust of the chapter is a VA methodology for finding and correcting weaknesses in privately owned businesses.

THE PROCESS

The VA process consists of step-by-step actions, which are as follows:

- Determine authority, scope, and leadership.
- Form a multidisciplinary team.
- Characterize the facility.
- Identify meaningful assets.
- From meaningful assets, identify critical assets.
- Characterize the potential threats.
- Identify current capabilities to counter the threats.
- Identify the missing capabilities (i.e., vulnerability).
- Identify and recommend countermeasures.
- Implement the countermeasures.

Technically, the last step is not a part of the VA. The implementation of countermeasures is "doing" actions such as acquiring and installing physical safeguards, hiring and training security officers, and revising plans and procedures. The VA is an analytical process—not an action process. Fig. 22.1 is a checklist of steps in the VA process.

Determine Authority, Scope, and Leadership

Authority usually refers to the person at the top, such as the CEO of the company or facility, or an organization above the Chief Executive Officer (CEO), such as a company's board of directors, or a regulatory agency such as the Occupational Safety and Health Administration, Environmental Protection Agency, Department of Homeland Security (DHS), or an organization that regulates the company's activities.

Scope

Scope is the extent of the VA and is either set by the company or the agency that authorized or commanded the VA. The assessment can focus on a single asset, a group of assets, the facility holding the assets, facilities at various locations, essential processes, etc. The chemical plant shown in Fig. 22.2 is

Steps in the VA Process

Determine authority, scope, and leadership.
Form a multidisciplinary team.
Characterize the target site.
- In advance, obtain a full set of documents
- Apportion documents according to disciplines on the team

From all assets, identify the meaningful assets.
From the meaningful assets, identify the critical assets.
- Impact on life
- Impact on dollars
- Impact on operations

Characterize the potential terrorist group, i.e., the threat.
- Existence
- History
- Intentions
- Capability
- Targeting
- Security Environment

Identify the site's current capabilities to counter the threat.
Identify the missing capabilities, i.e., the vulnerabilities.
Identify and recommend measures that eliminate/reduce vulnerabilities.
Implement the measures.
Test and revise as needed.

FIGURE 22.1
This checklist can be used as a tool when preparing to conduct a VA.

an example of a facility likely to contain several critical assets having public health implications.

Scope also means the depth of the assessment—how penetrating it will be. Assume an asset is a piece of essential equipment. The penetration, or "drilling down," might consist of determining the expected life of the asset, its current condition, if a replacement is on site, and if not, the availability of on-site repair, time required to get the equipment, other dependent equipment, and availability of the equipment elsewhere, its cost, delivery time, and installation time.

"Drilling down" is done in a variety of ways. A way that can be especially revealing is to interview knowledgeable employees. Relevant information is often held by employees working in the trenches far below actual protection of the asset. An example of knowledgeable persons might be a janitorial staff that works during evening hours and sees weaknesses such as geoscientists leaving sensitive maps atop their desks or tacked to the wall, or executive secretaries hiding container keys or safe combinations inside the pages of desk calendars. Relevant information might be found beyond

FIGURE 22.2
Criticality is high when a plant, such as the chemical plant depicted here, manufactures products of a toxic or lethal nature. *iStockphotos.*

the company's boundaries such as printer repairmen, soft drink and water bottle delivery persons, couriers, and other vendors who have free access to the facility.

When the facility poses a potential health and safety risk that extends beyond the perimeter of the facility, the surrounding community should be included in the VA. Agencies to be contacted include fire and police departments, public health offices, medical treatment facilities, emergency communication centers, and companies that provide off-site facilities for continued business operations during and immediately following an emergency that would make the facility unsuitable until repairs can be made.

As mentioned in the chapter on emergency management, the CSO should have entered into mutual assistance agreements with local emergency response agencies. Just as the company will have an emergency response plan, so will the partners to the agreement. The trick, of course, is to integrate all of the separate plans into an overarching plan that follows guidance contained in the National Incident Management System and Incident Control System. The background of mutual assistance is a matter to be investigated during the VA, and where gaps or other problems are discovered, they should be reported as vulnerability.

Leadership

The VA team leader is typically a third party, such as a person from a similar or identical company external to the company or a consultant with expertise related to the protected asset(s). The team leader may not be expert in a scientific discipline but will possess leadership and organizational skills.

A preliminary task of the team leader is to form a multidisciplinary team composed of professionals whose collective expertise correspond to the nature of the facility. If the critical asset is an atom-smashing cyclotron, one or more members of the team will be physicists, radiological specialists, engineers, and the like. If the critical asset is a process that uses ordinary equipment to produce a mineral ore, expect the team to have geologists and metallurgists. Nonscientific members of the team will usually be the CSO, safety coordinators, HazMat technicians, health professionals, a draftsman for preparing sketches, a photographer, and a person to transcribe notes and write progress reports.

Roper (1997) is supportive by making the point that persons who conduct VAs should meet all the requirements necessary (to the tasks) and have the appropriate managerial support and equipment available.

Well in advance of the scheduled assessment, the team leader will request facility management designate a key supervisor to act as the VA team's point of contact (POC). The POC's functions are fourfold: (1) in advance of the assessment, send to the team leader documents pertinent to the facility, its business processes, and security program; (2) remove obstacles and "open doors" during the assessment; (3) schedule employees to be interviewed; and (4) serve as a guide generally.

Documents of interest to the VA team to be sent by the POC in advance include the following:

- Mutual agreements for assistance from outside agencies.
- As-built plans (a running record of how the facility or any part of it was constructed and renovated).
- Contingency plans and procedures.
- Characteristics of the guard force, e.g., number of officers, deployment, equipment, and training.
- Physical security safeguards such as perimeter fencing, gates, security lighting, and sensors.
- The security control center.
- Security systems such as access control, intrusion detection, and data protection.

FIGURE 22.3
More than one VA team member might be assigned to analyze a single area. *iStockphotos.*

- Layouts of buildings within the facility and building floor layouts, wiring circuitry, plumbing lines, heating, ventilating and air conditioning (HVAC) system locations and ductwork, and sources of power.
- Firefighting equipment such as hand-held extinguishers, their placement, and frequency of inspections; emergency fire pump and standpipes; back-up power; ventilation louvers; valves; fire stairwells; locations of community fire departments and their response times; and a floor warden program, if any.
- Safety rules, including placement and storage of hazardous materials.
- The organizational chart.
- Photographs of the facility during the day, at night, and on weekends and holidays.
- Photographs of assets believed by management to be critical.
- Preemployment screening, including drug and other tests.

Documents pertaining to the above are apportioned to VA team members according to their professional discipline; for example, security-related documents go to the CSO, firefighting equipment and safety rules go to the safety and HazMat professionals, and as-built plans and diagrams go to the engineer. The purpose of acquiring knowledge in advance will shorten the time period of the assessment and allow team members to have an idea of what to expect when the VA begins. Fig. 22.3 shows VA team members comparing notes.

Characterize the Facility

Here are examples of site characteristics. Not all will apply, and other characteristics not mentioned here might be relevant.

- Nature of operations at the facility.
- Where the facility is located.
- Roadways leading to and from the facility.
- Structures and their contents within the facility and where situated.
- Size and composition of structures.
- Internal building features such as utilities, back-up power, sewage disposal, elevators, number of floors, windows, and doors.
- The surrounding community.
- Physical safeguards such as fences, lights, sensors, and closed circuit television (CCTV).
- Terrain features and soil composition.
- Flora and fauna.
- Climate and weather.
- Nearby roadways.
- Proximity to major external facilities that could interfere with sensors.
- The facility's primary services or outputs.
- Critical activities that take place at the facility.
- Professionals working at the facility.
- Materials from external organizations required for the facility's operations.
- The number and type of organizations in and around the facility that might cause collateral damage.

These characteristics help describe the physical makeup of the facility and help determine the probable effect of an adverse event affecting physical and human assets.

Identify Meaningful Assets

Think of assets in three categories: (1) assets that seemingly require no protection such as office supplies and furniture, (2) assets that require protection of equipment and buildings, and (3) assets that require a high degree of protection such as people and assets which if lost, damaged, or destroyed would cripple the company or put it out of business. Critical assets will be found in the meaningful assets category.

Identify Critical Assets

In every case, the critical asset of a facility is people. In the case of people, criticality relates to replacement of employees who are essential to operations, costs of preventing and mitigating injury and death, costs of long-term treatment, money settlements to family members, legal costs, loss of employee morale, loss of public confidence, and legal liability if inadequate safety or security is proven.

The people asset, although high on the protection list, tends to sustain damage that is collateral to the attack. (Attack here means direct action against the facility.)

Next on the criticality list are physical assets that are essential to business operations. For example, a piece of equipment called the catalytic processor is essential to the operation of a petroleum refinery, and as such, is a critical asset. Again, e.g., a specially constructed feeder that inserts gunpowder into artillery shells is a critical asset because it is essential to the production of artillery rounds. The petroleum refinery will shut down until the processor is repaired or replaced, and production of ammunition will stop until a new feeder is repaired or replaced.

Care must be taken not to misidentify or fail to recognize critical assets. In documents provided in advance of or during the VA, management's judgment should be apparent as to which assets are critical. However, management's judgment may not be accurate. If the team assumes that management is entirely correct, it may ignore an asset that is in fact critical but unknown as such.

A similar problem in identifying a critical asset is called the "single point of failure." To illustrate, an assembly line that produces an electronic circuit board is essential to the flying of a helicopter. Imagine the circuit board shown in Fig. 22.4 was not properly assembled and as a result was not able to perform its intended function. Without the board, the helicopter cannot fly. At the beginning of the assembly line is a blank circuit board, and coming off the other end of the line is a complete circuit board. Now imagine near the center of the assembly line is a small, inexpensive piece of equipment called the "master chip inserter." The function of the inserter is to

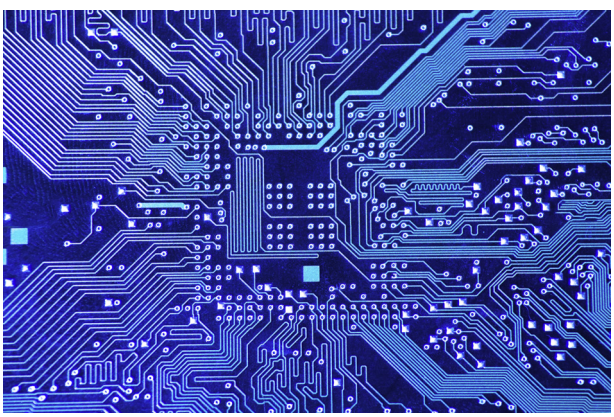


FIGURE 22.4

A chip missing from a circuit board can shut down an entire process. *iStockphotos.*

attach an extremely small chip on the circuit board before the board moves on to the next assembly line station. The inserter in this scenario happens to be brand new. It was a backup taken out of storage when the previous inserter broke down the previous week. At the present time, there is no other back-up inserter, and repair of inserters is not possible. The manager of the assembly line is not aware that a backup is not on hand. He also doesn't know the company that manufactures the inserter has gone out of business. If the one and only inserter breaks down, the assembly line will stop and remain stopped until a replacement is found, which may be months down the road or never. This small, inexpensive, and seemingly unimportant piece of equipment is a single point of failure—a failure that could turn out to be a national defense problem.

Judgment as to criticality can be aided by evaluating an asset in three dimensions.

- Impact on life.
- Impact on operations.
- Impact on dollars.

The measurement of impact on life is answered by the question "How many people will perish or be injured if the facility is attacked?" The answer depends on the mode of attack, weapons used, and intent of the attackers.

Operational impact is evaluated by the probable effect on the organization's core functions and processes. The estimate of operational impact (probable effect) can run the gamut from mildly damaging to catastrophic. The risk management department calculates, as best it can, the probable effect and assigns a criticality rating based on the costs of returning the operation to its normal function. It may be possible for an emergency-prepared facility to continue functioning after sustaining severe damage. At a lesser prepared facility, complete shutdown could be inevitable.

Also considered should be loss of function outside the facility. Imagine for example that the facility cannot function without electrical power. Loss of power also will bring external business operations to a halt and disrupt critical community facilities such as hospitals, police and fire stations, subways, water supply and sewage disposal systems, and the normal daily activities of people.

The impact on dollars can be relative, that is, dollar value at one facility may be significantly higher or lower than at another facility, even when both facilities are comparable in size, function, and output. A facility owned by a financially secure organization may be able to absorb a high dollar loss, whereas a facility that operates on the edge of bankruptcy may have no financial cushion at all and be forced to cease operations.

It is possible to estimate in dollars the impact on people and operations, although not with perfect accuracy. The third impact, which is entirely computed in dollars, means that all three impacts can have dollars as a common denominator. Resulting losses expressed in dollars is of considerable assistance to those charged with risk management duties.

Characterize the Potential Threat

In this rendition of VA, the potential threat is a terrorist group. Remember that other threats exist such as Acts of God, accidents, and plain old crime.

A terrorist threat is an indication, circumstance, event, or adversary with the potential to cause loss of or damage to an asset. Specific naming and characterization of potential terrorist groups relies almost entirely on information provided by the DHS, Federal Bureau of Investigation, other law enforcement and intelligence agencies, and the Department of State for overseas operations. DHS uses six factors to evaluate a potential terrorist group.

- Existence. This factor addresses the questions: What terrorist groups are hostile to the facility? Are they in striking distance? If in striking distance, are they identifiable?
- History. The questions to be answered here are: What has the potential threat group done in the past? Where and how many times? How recently? When was the most recent incident and where, and against what target?
- Capability asks: What weapons do the terrorist groups possess? What weapons have they used in past attacks? Can such weapons be acquired or constructed in the area proximal to the facility? What tactics were used and to what degree of success? What is their manpower? Are they skilled and trained? What resources do they command? Do they have outside support?
- Intention addresses the questions: What would a potential threat group hope to achieve by attacking? Has a threat group stated an intention to attack? Is the facility similar to facilities already attacked?
- Targeting. This factor asks: Is the facility being watched? Have any attempts been made to acquire information about the facility, particularly security-related information? Have there been any innocuous-appearing attempts to gain entry to the facility? Has security of the facility been tested such as by causing an intrusion detection sensor to activate?

Security environment: Indicates if and how the political and security posture of the threatened jurisdiction affects the capability of terrorist elements to

carry out their intentions. Addresses whether the jurisdiction is concerned with terrorism and whether it has taken strong proactive countermeasures to deal with such a threat.

Identify the Site's Current Capabilities

With an understanding of the facility as a potential target, it is possible to conceptualize a security system resistant to attack. A preliminary step, however, is necessary: the capabilities of the present system must be ascertained. The assumption here is that the facility has a security program already in place.

Identify the Missing Capabilities (Vulnerability)

The VA team's next step is to evaluate the resistance of the site to attack. For example, assume a potential threat is known to be targeting the facility, and the threat group has a history of attacking with vehicle bombs. The essential question to be asked is, "Does the facility currently have a capability to resist this form of attack?" If the answer is no, the VA team has identified a missing capability.

A missing capability is vulnerability, and vulnerability is a weakness that can be exploited by an adversary. A simple way of identifying missing capabilities is to compare current capabilities against required capabilities. Examples might be the following: compare the number of security officers on hand and the number needed, compare the capabilities of the current CCTV system against capabilities of an intruder to reach the target through circumvention, and compare the absence of an access control system against a needed access control system.

Identify and Recommend Measures that Eliminate or Reduce Vulnerability

Capabilities are established with countermeasures. In the vehicle bomb attack scenario, a number of countermeasures are indicated: channel entrances and roadways away from key buildings; require vehicles to be parked at a safe distance away from key buildings; install bollards or similar devices at places that would prevent ramming a building; and place bomb-resistant film on glass surfaces.

Implement Countermeasures

Now comes the time to produce a set of action steps to implement the identified countermeasures. Because many of the action steps relate directly to

the facility's security system, the CSO has an important part to play. The CSOs input to the action steps can address the following:

- Use of force.
- Competency of the security guard force.
- Legal restrictions and liability.
- Technical capabilities of physical safeguards.
- Cost and availability of security-related equipment and services.
- Security manpower issues.

A schedule for working through the action steps is also developed. Like the construction of a house, certain steps must be done before others, and each will have its own schedule for completion.

EXIT BRIEFING

Not mentioned earlier, but important nonetheless, are three meetings held between facility management and the VA team. The most important of these is the exit briefing. But first, let us discuss the two previous meetings.

Roper (1997) provides a checklist for the first meeting:

- The VA team leader makes introductions.
- The purpose and objectives of the inspection are stated.
- Management views and comments are solicited.
- Support is requested.
- The thrust of the assessment is highlighted.
- The benefits accruing from the assessment are discussed.
- Potential threats are characterized.
- VA team activities are outlined.
- Management is thanked in advance for the cooperation requested.

A second meeting takes place at about the midpoint of the VA. The team leader reports on preliminary findings, obstacles encountered, and work remaining to be done. If a particular weakness has been identified and is correctable before the VA has been completed, the team leader will encourage management to correct the weakness, which if done immediately, will reflect favorably on management's cooperation and may not find its way into the VA final report.

The third meeting, or exit briefing, covers all weaknesses discovered and recommends measures for correcting them. The team leader acknowledges that management will want to consider the recommendations in terms of cost and possible impact on productivity. Still, the team leader will encourage action be taken as quickly as possible.

FINAL REPORT

A fairly complex VA will be finalized with a fairly comprehensive written report that may take as long as a month to complete. The team leader may prepare a "laundry list" of actions that need to be taken in advance of the final report.

Garcia (2006) makes excellent points when referring to reporting the results of the VA. She says that after analysis of facility data is complete, the VA team reports the results in a manner that is useful to the managers at the facility. The goal of the report is to provide accurate, unbiased information that clearly defines the current effectiveness of the physical protection system (PPS), along with potential solutions if the current system is not effective. The VA (report) informs facility management of the state of the PPS and supports upgrade decisions.

Garcia (2006) goes on to say that reporting can be formal or informal, verbal or written, and may take the form of a short overview, or a longer, more detailed approach. Regardless of how reporting is presented and documented, certain content must be included to make the report understandable and useful to the facility. By its very nature, a VA report is a powerful document and should not be shared indiscriminately.

The team leader walks on shaky ground when meeting with management, particularly during the final meeting. Tact is necessary because logically every weakness is a management failure. The weaknesses should have been avoided in the first place, discovered at some point, and corrected without delay. Management will not be deliriously happy to know its failures have been uncovered and soon are to be made known to a higher organization.

MANAGEMENT ACTIONS

Actions taken by management to correct deficiencies identified in a VA will not likely correspond perfectly to the measures recommended by the VA team. Before deciding on what actions to take, management might very well pose a number of questions:

- Can we afford the costs of implementing the recommended measures?
- Are the recommended measures cost effective?
- Would implementation of the measures interfere with site operations?
- Are we willing to accept some of the risk by not fully implementing the recommended measures?

The VA methodology has variants, and properly so, but in the final analysis, they all work the same, i.e., they move along a similar pathway. The

methodology, regardless of name, is directed at evaluating a particular facility, determining threats, identifying critical assets, assessing current and missing protective capabilities, and recommending countermeasures. Why will VAs vary? The answer is that facilities vary widely, and each has its own set of unique characteristics that mandate evaluation methods that correspond to those characteristics. A dam, an electrical grid, and a chemical plant are distinctly different in so many ways. Each will have its own VA methodology. Some states, in their concern for protection of state-owned assets, have VA models. The federal government has a generic VA model, and some agencies within the government have specific models. As an example, the Environmental Protection Agency (EPA) uses a six-step approach for assessing water systems. The steps for that model are as follows:

- Evaluate the situation.
- Identify threats.
- Consider the consequences.
- Assess the likelihood.
- Evaluate measures.
- Plan the protective actions.

Take note in Step 2, the threats that can impact drinking water, a critical asset, are much different than threats facing passenger airlines. The methods of identifying threats against water systems include monitoring the quality of water, and among the methods of identifying threats against passenger airlines are baggage inspections and searches of passengers and their carry-on property. Because threats and critical assets vary, the techniques of assessment will vary accordingly, yet the VA methodology remains constant.

Tucker (2006) writes of an interesting twist to the basic VA methodology. The twist is a tool called the vulnerability self-assessment tool (VSAT). The hands-on work of VA team members is massaged by software to produce standardized reports and display detected weaknesses in a color-coded threat matrix. The software also prioritizes countermeasures based on the anticipated reduction in risk per dollar spent.

Tucker (2006) posits 11 steps in the VSAT process:

1. Identify assets.
2. Identify threats.
3. Determine criticality.
4. Identify existing countermeasures.
5. Determine risk level.
6. Determine the probability of failure.
7. Identify vulnerability.
8. Determine whether risk is acceptable.

9. Develop new countermeasures.
10. Perform risk-cost analysis.
11. Develop a business continuity plan.

Steps 8 and 10 are dollar-driven, which adds an extra dimension to the fundamental VA methodology. Properly so, VSAT does not directly address implementation of countermeasures, nor does it bother with testing implemented countermeasures and revising them as needed, at least until the next VSAT is conducted. Because VSAT goes into detail with respect to the use of information technology to maintain business continuity, it can be particularly useful when the critical asset is an information technology asset.

CRITICAL THINKING EXERCISE

(Note: In this exercise, we have used a home instead of a business facility. But it doesn't matter because the VA is amenable.) Grace and Walter Nystrom own and operate a convenience store, which takes them away from their home for most of everyday. For the past 30 years, they have lived in the same house, a one-story ranch house in a neighborhood that is transitioning down. In the past 3 months, six burglaries have occurred at houses nearby.

Over the years, the Nystroms have acquired and kept in their home personal assets such as jewelry Grace purchased or inherited from her mother and grandmother. The jewelry is kept in an 18-inch by 18-inch safe in the master bedroom closet. Also inside the safe is a pair of valuable dueling pistols. In the living room are a Sony HDTV and an Onkyo sound system. On top of the dining room chiffonnier is a tea set, champagne bucket, and small items, all made of sterling silver. In the den, where Walter keeps work-related records, are two desktop PCs, two printers and copiers, a scanner, and a fax machine. On a book shelf are an iPod and Kindle.

When Grace and Walter return home in the evening, they park their car in the driveway because there is no garage. The car is a new, top-of-the-line Lexus.

The Nystroms are worried a burglary will occur at their home, yet they have little knowledge of how to keep a burglary from occurring. Walter called the local police department for advice. The police department sent a crime prevention officer to the Nystrom home to conduct a crime prevention inspection. The officer spent a full day evaluating the home. That evening, he briefed the Nystroms on his findings. He told them, "Place deadbolts on the front and back doors. Now, because on both sides of the front door are narrow, stained-glass windows, a burglar could break the glass, reach inside and turn the dead bolt's thumb latch. To overcome the problem, place foil tape on the glass so that if the glass breaks, an alarm will sound. You'll experience the replacement cost of the decorative window, but you've frightened the burglar away."

Walter answered, "But I don't know anything about foil tape."

> *"Before leaving I'll give you the name and phone number of a company that can do it for you. Now let me talk about the windows. You should install a special window latch—one that will be in addition to the standard latch now in place. This special latch can be unlocked from the inside but not the outside. Below each window, you should plant holly bushes or another kind of plant that causes pain to anyone trying to pass through it."*
>
> *"I can take care of that myself," Grace said. "I need the exercise."*

The police officer continued: "The jewelry and dueling pistols are at very great risk."

Before the officer could continue, Walter interjected, "But they're in a safe!"

> *"Let me show you what I mean," the officer said, leading the Nystroms into the master bedroom closet. The officer bent over, and flexing his knees, lifted the safe one foot off the floor. "If I can do that, two young men can carry it out the door, or easier still, place it on a dolly and wheel it away." The officer brushed his hands against the side of his pants, and added, "At each corner of this safe are heavy duty brackets that are meant to be bolted to the floor. There are no bolts."*

Walter pleaded, "I didn't want to put holes in the floor." Grace stared accusingly at Walter as the officer moved ahead of them into the center of the house.

The officer pointed to the dining room and the open den. "If someone gets in the house you can kiss most of these valuables good-bye—the TV, stereo system, silver set, and so forth. The answer is to keep the burglars out."

"You mean an alarm system?" Walter asked.

> *"Yes, but it does not have to be elaborate. Instead of putting a sensor on every door and window, install one or two motion detectors. If a sensor detects movement, inside the den for example, an alarm will sound right here at the house and at a central station where an operator will call the police."*

Grace and Walter looked at each other. The police officer was sure they'd talk about his recommendations before making any kind of decision.

"One last thing," the officer said. "Make sure the anti-theft alarm system is active when you leave the Lexus in the driveway. And if it were me, I'd buy a locking bar for the wheel."

Using the VA methodology as a guide, identify the scope, the threat, the assets, the countermeasures, and management. Before the officer arrived, management was operating under a false premise. What was it?

National Implications

The DHS has developed the National Infrastructure Protection Plan, which specifically addresses security of the nation's Critical Infrastructure and Key Resources (CIKRs) such as energy, finance, transportation, etc. Each CIKR is assigned a sector-specific agency (SPA) that prepares a plan for its sector. Because the majority of CIKRs are privately owned, considerable input to protection planning must come from businesses. Input of a security nature is determined by the CSO of the business. In a very important sense, CSOs have something to contribute to an SPA's plan to protect the sector within which the company operates. DHS has called for a partnership between the federal government and businesses. For the arrangement to work, both partners must assure each other that appropriate security measures are in place.

CONCLUSIONS

The VA methodology is an analytical process for identifying a site's critical assets, evaluating the protective shield that surrounds the assets, determining resistance to a threat, and recommending physical and procedural measures to improve resistance. VA models can vary according to assets and process at the assessed site. Still, the basic methodology remains the same.

REVIEW QUESTIONS

1. Name the steps in the VA process.
2. What is "target hardening?"
3. List six examples of a site characteristic.
4. What is meant by the term "scope?"
5. Name the three judgments necessary in determining criticality.
6. What is accomplished during an exit briefing?
7. Name and describe the function of risk management when conducting a VA.

References

Garcia, M.L., 2006. Vulnerability Assessment of Physical Protection Systems. Butterworth-Heinemann, Boston, MA.

Roper, C.A., 1997. Physical Security and the Inspection Process. Butterworth-Heinemann, Boston, MA.

Tucker, E., 2006. Business impact analysis, Risk Analysis and the Security Survey, third ed. Butterworth-Heinemann, Boston, MA, p. 40.

Further Reading

Environmental Protection Agency, 2005. Drinking Water Security for Small Systems Serving 3,300 or Fewer Persons. U.S. Government Printing Office, Washington, DC.

CHAPTER 23

Security Program Design

What You Will Learn

- The three pillars of a security program.
- The distinction between plans and policies.
- Varying levels of training for security program participants.
- Testing to ensure efficacy of design.
- Which outside agencies to involve in a full-scale drill.
- Revising a security program to improve design.

INTRODUCTION

Many references are made in this book to a security program. In the previous chapter, the point was made that a vulnerability assessment is a tool for constructing a security program. This is true because a vulnerability assessment (VA) will examine a facility in terms of a security program's three main parts: people, process, and physical security. Each of the three could be perfect in all respects, but when they cannot function together, the VA team will conclude that the facility has a major weakness. The point can be made by thinking of a ballpoint pen. The pen has three parts: the ballpoint, ink, and a chassis that contains the ink. If the ballpoint is jammed or if the ink is dry or if the chassis is cracked, the pen will not function as it was designed to do. The pen may not work at all or it may still write but not in the way it is supposed to write. The same logic applies with respect to a security program. If the program does not have enough security officers or the process is poorly understood or the physical security features are outmoded, the program will not work or will work inefficiently. A VA can surface the inadequacies, which then makes it possible to reconsider, with solid facts, a new security program design.

Implementation of the recommendations made in a VA report, even when followed to the *n*th degree, will not guarantee the security program will rise to perfection. The only way to discover if the security program will work in an emergency is to put it to the test. Results of the test may lead management

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00023-2

to think: we need more here, need less there, do it this way, not that way, and so forth. Management is in the first step of security program design.

THREE PILLARS

It will help to establish definitions right from the start. A security program is a bundle made of three major parts: people, process, and physical security. Fig. 23.1 is a chart depicting the parts of a security program.

The parts are sometimes called the "pillars of security," and rightly so. When the parts work together, they are said to be in harmony with one another. When any one of the pillars tumbles, the program becomes entirely dysfunctional. If a pillar cracks or leans to one side, the program may continue to function but not as it should. In other words, the program can collapse, or in other cases give the appearance of functionality when such is not the case.

People

The people part consists of the Chief Security Officer (CSO) and security personnel whose duties are various and numerous. Fig. 23.2 shows a security officer placing an electronic wand close to a receiver. The receiver makes a record that the officer on patrol checked the surrounding area. This task is one of many that are relatively unknown outside of the security group.

Other persons comprising the people component of a security program include medical, safety and Hazmat professionals, members of the emergency

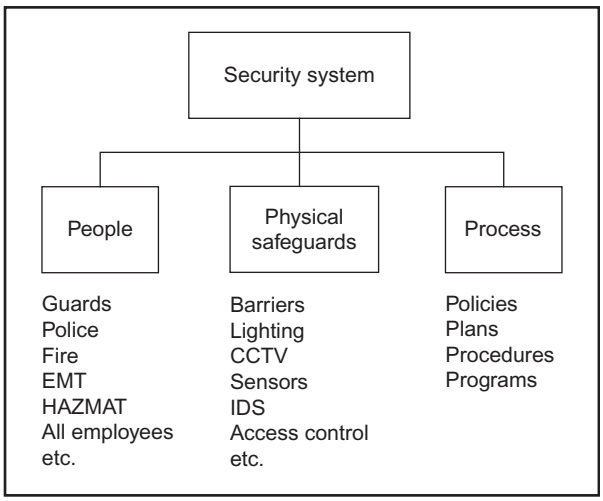


FIGURE 23.1
The three pillars of a security program.

FIGURE 23.2
Security officers perform tasks that are sometimes not recognized or understood by company employees. *iStockphotos.*

management team, floor or fire wardens, and others who have a direct part to play in the functioning of the security program under emergency conditions. It can be said, with genuine emphasis, that the entire human population of a company is an element of the security program, the rationale being that every employee has security responsibilities.

Process

Process constitutes the second part of the program. Process includes responding to emergencies according to policy, plans, and procedures. These written documents spell out security tasks to be performed by people. For the security group, process gives directional guidance as to the tasks to be performed, how they are to be performed, and collaboration with other responders. The directional guidance of process can consist of post orders, temporary memoranda, special orders, access control lists, equipment operation, notification lists, etc.

Procedures in the building management department might be acquiring first-aid supplies, setting up a triage area and medical emergency tents, evacuating employees, shutting down and turning on certain equipment, and many other tasks.

The information technology (IT) department might follow procedures for shielding equipment, protecting data, and moving IT operations to an off-site location.

All departments in a business will be responsible for following security procedures whether routinely or during a major emergency. Process documents

represent a logical set of actions that can be used as job aids, albeit long and numerous. Although nothing more than words on paper, they prescribe certain essential actions to be taken in certain serious situations.

Bottom line, the source of procedures is plans, and the source of plans is policies. Policies state what the security program is expected to do; plans designate who is to do what; and procedures state how to do it.

Physical Security

The third part of the program is physical security safeguards, which can be neatly characterized as a combination of systems: access control, intrusion detection, closed circuit television (CCTV), fire detection and control, fencing, lighting, sensors, and other systems dictated by need. Understanding the workings of a security program may be helped with an analogy: A carpenter (a person) knows the steps (procedures) for using an electric saw (a physical tool). When the three steps are performed properly, a table is made, which can be likened to a security program.

Following are major headings of physical safeguards. Not shown, but within each heading, are safeguards by type, e.g., barriers can include chain-link fences, masonry walls, concertina wire, and bollards:

- Barriers.
- Portals.
- Lights.
- CCTV.
- Intrusion detectors.
- Access controls.
- Communications.
- Fire detectors.
- Guard enclosures.
- Vehicles.

Fig. 23.3 is a photo of a mounted CCTV camera. The chief characteristics of a high-quality CCTV system are color imaging, high-resolution images, long-distance viewing, wide-area coverage, zooming and panning, operation in daylight and sunlight, durability, and a signal that movement has been detected in the field of view.

TRAINING

Training is the means for ensuring that every employee knows his or her part in making the security program work, and each department head is responsible for making it happen. The modes of training can vary, provided they

FIGURE 23.3
A CCTV system is very common to a security program. *iStockphotos.*

address the procedures. The person in charge of the floor warden program might attend an out-of-house workshop, while floor wardens might attend in-house training conducted by a fire inspector from the local community. Training of this type is called "enrichment" training because it does not directly focus on the nitty–gritty of the procedures. The most effective form of training is actual performance of tasks mandated by the procedures. For example, the floor wardens might conduct an evacuation drill with a fire marshal acting as the evaluator.

In the security group, training for the CSO and the CSO's staff might be obtained at security seminars, while security officers might receive training given by shift supervisors and experienced coworkers. Firearms practice is shown in Fig. 23.4. (Note: Some companies, usually companies having low-value assets or a management that fears liability resulting from improper use of a firearm, will not allow officers to carry firearms.)

Security officer training has two stages: entry level and upper level. Entry level covers basic principles and response procedures for serious incidents; upper level includes refresher training, advanced training, and training in how to deal with complex situations. Entry level is more important than upper level because topics are foundational and capped with knowledge related to likely serious events. A negative in the upper-level training program for security officers is the rate of turnover in the security industry. It is so high that only a small percentage of officers ever reach a point where they qualify for upper-level training, which, as you can imagine, causes the security program to be less than fully effective.

FIGURE 23.4
A security officer practicing shooting skills at a firing range. *iStockphotos.*

At the entry level, a security officer is taught basic principles first and response procedures next. According to a guideline published by the American Society for Industrial Security International (ASIS), entry-level training should begin on the day of hire and extend for about 100 days. Training combines lecture and demonstration, films and videos, and on-the-job practice and tutorials. Online training is gaining favor because it can be conducted anywhere, anytime, and is economical compared to other methods of instruction.

According to ASIS, the basic topics needed to be taught at the entry level are as follows:

- Employer orientation and policies.
- Job assignment and post orders.
- Use and operation of equipment.
- Nature of security operations.
- Legal aspects.
- Conduct and ethics.
- Observation and incident reporting.
- Patrol techniques.
- Interpersonal communications.
- Principles of access control.
- Loss-prevention principles.

Complexity of subject matter at the upper level requires considerably more effort in teaching and learning. The time needed to teach just one of the upper-level topics can be as long as the time needed to teach five of the lower-level topics. The first eight of the topics listed below are essential. The remainder will be pertinent to some companies but not to others.

- Fire emergencies.
- Bomb incidents.
- Workplace violence.
- Premises evacuation.
- Hazardous materials incidents.
- Emergency notifications.
- Use of deadly force.
- First aid, cardiopulmonary resuscitation, and defibrillation.
- Executive protection.
- Duress alarms.
- Special escorts.
- Crowd control.

Training is essential because the most frequent failure in the operation of a security program is human error, and human error is most often the result of poor training or training not conducted. Training is a matter that cries out for management attention. Nearly all training deficiencies result from a failure of management to require that it be done, and the reasons behind the failure are apathy and the never-ending urge to contain costs.

TESTING THE DESIGN

The final design or configuration of a security program cannot be accepted as the "right" design without first making sure it meets the objectives of the security program. If a program objective is to respond in 5 min to a confirmed report of intrusion, then the only way to make sure the objective is being met is to simulate a report of intrusion and time the response.

People Testing

This list pertains to security officers only. Employees in other departments may or may not be tested at all, and if they are, the tests will be unlike tests administered to security officers.

- Tests that assess general knowledge, aptitude, intelligence, achievement, interests, personality, honesty, integrity, drug abuse, and probability of violent behavior.
- Tests conducted as part of a training program.

- Cognitive tests that evaluate a security officer's knowledge of the job, post orders, special operating procedures, and incident plan procedures.
- Psychomotor tests that evaluate a security officer's capacity to perform tasks that depend on body coordination such as firing a weapon; body strength such as carrying an injured person; and stamina such as working long hours.
- Skill tests that evaluate a security officer's ability to perform tasks of an abstract nature such as comprehending and analyzing information.

Process Testing

- Desktop exercises can be conducted by site management to evaluate the general readiness of the security program. A scenario is presented, often by the emergency management team (the team of managers that perform command and control functions in an emergency operating center). A desktop exercise can call for a system-wide response to a specific incident. Working from their desks (or other nonscene locations), the responders simulate actions called for by the incident plan and procedures. An after-action assessment by management and the participants decides the workability of the plan and procedural changes that may be required to improve the response.
- War games evaluate the efficiency of plans and procedures in a "conflict" situation. The situation is hypothetical and typically involves a terrorist attack such as a bombing, stand-off attack, or direct assault. Following the initial attack, the terrorist group changes its tactics or reacts in some way that requires the responders to change tactics. The war game is similar to the desktop exercise because with few exceptions the responders carry out procedures from their workstations. The war game can be unannounced, administered by an outside group, the scenario "intense" and evolving, and responses monitored and graded.

Physical Security Testing

Garcia (2001) recommends evaluation of physical security safeguards in the following ways:

- Operability tests conducted daily by security group employees to evaluate operation of security program equipment.
- Equipment performance tests conducted periodically (usually monthly) by security group employees and others to assess operability and sensitivity of security program equipment such as fire detectors, fire extinguishers, intrusion sensors, CCTV cameras, defibrillators, oxygen administering devices, and backup generators.

- Postmaintenance tests conducted when security program equipment has been returned to use after maintenance or repair.
- Limited scope tests conducted to evaluate all of the equipment comprising an entire system or one or a few major pieces of equipment.
- Whole-system tests conducted to ensure the design of the physical security pillar is working as planned.

Broder (2006) recommends five basic methods for evaluating physical security:

1. Functional testing to determine whether hardware, such as a closed-circuit television camera or access control system, will do what it was designed to do.
2. Safety testing to determine whether an object or a procedure can be used without causing injury, loss, or harm.
3. Performance testing is normally concerned with conformance to timing, resource usage, or environmental constraints (an example is an anti-intrusion alarm).
4. Stress testing checks an object's tolerance due to abuse or misuse under deliberately introduced techniques.
5. Regression testing usually applies to an object, system, or procedure that has been altered to perform a new function and must still perform some of the functions for which it was originally designed.

FULL-PROGRAM TESTING

Individual testing of the three parts of a security program can improve the performance of those parts as single entities, but what is really needed is a test of all three parts working together. Logically and with a sense of reality, there are two methods of verification: an actual attack or simulated practice.

A full-scale drill is intended to verify if the new design will in fact elevate the overall security program to a degree sufficient to meet an attack or prevent injury, loss, or damage. Every activity in a full-scale drill is done "live." For example, if a terrorist attack involves the use of a bomb, an explosion is simulated (perhaps using a smoke grenade to simulate the bomb). Mock fire-fighting commences and employees evacuate the site. Injuries are simulated, first aid is applied, and a triage center is set up. Police arrive and cordon off the area, HazMat specialists look for chemical agents, and public health officials look for biological and other agents. To avoid injuries to participants, the drill particulars should be made known in advance; neighbors should be alerted to avoid panic; and local participating agencies should be informed to help them prepare. The full-scale drill is a coordinated response that

involves people using physical safeguards according to the design of the security program.

A full-scale drill cannot be realistic without involvement of outside agencies:

- Law enforcement.
- Firefighting.
- Emergency medical services.
- Public safety communications.
- Healthcare.
- Public health.
- Public emergency management.
- Public works.
- Local civil defense agencies.
- Federal Emergency Management Agency.
- Federal investigative agencies.
- Governmental administrative agencies.

REVISING

The purpose behind testing all three parts together is to discover weaknesses and opportunities for improvement. Weaknesses can be seen in many forms: inadequate training, slow response time, poor or nonexisting equipment, not enough security officers, responders not going where they are supposed to go, employees not fully committed to evacuation, failure of external agencies (perhaps due to insufficient liaison), communications that do not work or interfere with one another, and the granddaddy of all—disagreement as to who is in charge. Is it the top man in the company's emergency management team? Is it the sheriff or chief of police; or is it the senior firefighter? All of these failures represent poor design, as well as failed opportunities at collaboration.

A separate method for improving design is called environmental review. McNaughton (1999) makes the point that threats, especially crime threats, can be prevented by deflecting unauthorized persons at the facility's portals, discouraging terrorists and criminal offenders by a display of security prowess and attentiveness, reducing the reward should a terrorist or criminal succeed in the attack or committing the crime, and increasing the chances of being thwarted.

The design of a security program is a logical follow-up to a vulnerability assessment. Designing is more than setting lines to paper; it is melding parts and parts of parts to create or strengthen a function. For example, the function of detecting intrusion is not entirely improved by simply installing a

CCTV system. Adjustments of a physical/technical nature will be required to take full advantage of the system such as assigning a person to watch the CCTV monitor, training console operators, modifying procedures, and acquiring missing supplies and equipment.

Persons charged with redesign will most probably see the truth to the adage that closing a door in one place opens a door in another place. Every add-on and change to a security program, whether at the micro or macro level, will impact the functions of people, process, and physical security.

SECURITY PROGRAM DESIGN AND THE EXTERNAL ENVIRONMENT

A business does not operate in a vacuum, neither does the security program that supports the business. Program design has to take into account constraints placed upon protection. A common constraint is noise and lighting that disturbs the quality of life in the areas surrounding the facility. The CSO might like to have sirens for alert purposes or security lights to detect intruders but are unacceptable to persons in the external environment. Even esthetics can come into play. The appearance of the security fence and an entry gate that operates 24 h a day may disturb the neighbors. A fence that affects wildlife is likely to be a problem. The local police may object to security officers directing traffic to facilitate the movement of employees in and out of the facility at rush hours. If the nature of the business is objectionable to an interest group, the CSO should expect problems.

Next are the political constraints. The underlying causes may be community demands that the company pay the costs to fund replacement or relocating of telephone poles, modification of streets, hiring of extra policemen and fire fighters, etc. Also, there may be resentment of local politicians who objected to construct the facility in the first place.

The external environment will affect the security program's configuration and methods of operation. In some cases the affect will be negative and in other cases positive. In the latter regard is the external support a business will need during a major emergency.

CRITICAL THINKING EXERCISE

Tony Abruzzo is the CSO of a company that manufactures expensive computer chips. Finished chips waiting delivery to customers are placed in a warehouse. An increase in demand requires additional storage space. The executive team decides to construct a new warehouse and destroy the older, much smaller warehouse. The new warehouse will extend beyond the boundaries of the facility (but still within the company's owned property).

Using the three pillars concept, in what ways will Tony have to modify the design of the existing security program?

CONCLUSION

The design of a security program will take into account a variety of elements such as employee awareness, intrusion detection, access control, fire response, plans, procedures, training, and so forth. Yet every element will fall into one of three major categories we can call the Three Pillars. The term is quite appropriate because if one of the pillars weakens, the entire structure of the security program will eventually collapse.

Not all security programs are alike and for good reasons. Some may have no need for security lighting, CCTV monitoring, and guard patrols while other facilities will have all of these elements and more. The nature of the facility, its location and environment, and above all, the critical assets within the facility will determine security design. However, no matter how one looks at a security program, it will always have three pillars. The pillars may be different but they will be there.

Security design, then, is planning and structuring a security program that effectively protects assets through a combination of people, process, and physical security. If there is inappropriately more of one and less of another, the program is doomed to fail.

The CSOs job is to recognize when a program is dysfunctional and make adjustments to get the program back on track.

REVIEW QUESTIONS

1. Name and describe the three pillars of a security program.
2. Briefly describe the relationship between a vulnerability assessment and the design of a security program.
3. What are physical safeguards? List four examples.
4. Name at least one method for revising each pillar, and describe how the revisions will affect the overall security program.
5. Name the greatest problem likely to be encountered in an actual attack or simulated drill.
6. What is the purpose of testing a security program?

References

Broder, J.F., 2006. Risk Analysis and the Security Survey, third ed. Butterworth-Henemann, Boston, MA.

Garcia, M.L., 2001. Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann, Boston, MA.

McNaughton, D., 1999. Designing protection systems. In: Robinson, R.R. (Ed.), Issues in Security Management: Thinking Critically about Security. Butterworth-Heinemann, Boston, MA, p. 56.

CHAPTER 24

The Importance of Policies and Procedures

What You Will Learn

- Understand why employees represent a risk to your organization.
- Name some of the problems employees cause for an organization.
- Understand the factors that affect an employee's behavior.
- How to define policies, standards, and procedures.
- Define some of the benefits of a strong security program.
- Define the security hierarchy.
- Understand the three recommended classifications of security documentation.
- Be able to describe what elements are essential to the structure of documentation.
- Recommendations for maintaining the awareness of security.
- Learn ways of maintaining consistency to the security awareness program.
- Purpose of why teamwork is vital to a successful security program.
- The challenges for the security organization today.

INTRODUCTION

In today's high-tech and multicultural world, threats exist from both employees of the enterprise as well as from external sources such as criminals, activists, terrorists, and natural disasters. Surveys indicate that threats that concern security managers the most are related to their employees from such crimes as violence, fraud, theft of intellectual property and company assets, unethical conduct, and problems in the workplace such as drugs nd alcohol. Organizations need a robust security program with strong policies and procedures to channel employee behavior, create an honest employee culture, and to help provide the legal structure. The absence of clear policies and procedures or the lack of proper implementation and enforcement can generate situations that undermine organizational authority, jeopardize organizational efficiency, and give rise to lawsuits due to premises liability, negligence, foreseeability, etc.

Contemporary Security Management. DOI: http://dx.doi.org/10.1016/B978-0-12-809278-1.00024-4

In addition, every organization needs many policies and procedures to provide a functional guide for training new and existing employees and preventing difficulties in performing duties due to lack of understanding or inconsistent approaches from personnel changes. The policies and procedures that companies implement should cover relevant physical security issues such as hiring guidelines, employee screening, ethics, conduct, termination, and monitoring of employees' use of company resources such as computers, email, telephones, etc. These elements are essential to maintaining an honest and dedicated workforce. Having the policies and procedures documented does not alleviate the problem as policies and procedures must be consistently enforced. By implementing and enforcing security policies and procedures, corporations can minimize their risks and show due diligence to their employees, customers, and shareholders.

This chapter provides organizations with suggestions for security program documentation that is minimally required for a well-run physical security program. This chapter will provide a high level overview of the process of developing and maintaining program documentation and the important elements to include. In addition, this chapter will cover recommendations to ensure consistency in application and conformance.

STATEMENT OF THE PROBLEM

Many studies have been done to document the fact that employees are an organization's greatest asset while also the source of their greatest problems. One survey that pinpointed the concern was the American Society for Industrial Security International 2009 survey "Impacts of Current Economic Environment on Security."

1. General Increases in Crime and Theft
2. Employee Layoffs and Furloughs
3. Increases in Theft of Physical Property
4. Increases in Workforce Violence
5. Increases in Theft of Intellectual Property
6. Fraud—Embezzlement or Misuse of Funds
7. Increases in General Employee Dissatisfaction
8. Damage to Organization Physical Property.

Of the top eight threats, more than half can be traced back to employees; yet many organizations fail to recognize that employees are a major problem and fail to take a proactive approach to the problem. Most organizations just live with the problem and react when an incident occurs. The

reasons for this vary, but in many cases organizations feel these are isolated incidents caused by a few problem employees, or they believe there is no perceived benefit to the organization in pursuing the perpetrators. Many organizations try to avoid hiring potential problem employees and detect and investigate employee losses on their own. As long as they catch (and fire) the thief and get some restitution such as recovering what the employee stole or have insurance cover the loss, organizations feel they have done all they can. One of the major reasons organizations do not prosecute problem employees is the fear of negative publicity, although this aspect is slowly changing as employers are starting to realize that there are benefits in letting other employees in the organization know that *these types of crimes will be detected and will not be tolerated*.

To illustrate the severity of the problem, we will cite a few examples:

1. Survey participants in the annual study done by the Association of Certified Fraud Examiners estimated that the typical organization loses 5% of its revenues to fraud each year. Applied to the estimated 2011 Gross World Product, this figure translates to a potential projected global fraud loss of more than $3.5 trillion.
2. The median loss caused by the occupational fraud cases in the study was $140,000. More than one-fifth of these cases caused losses of at least $1 million (ACFE, 2012).
3. Theft occurs in 95% of American companies (Christopher, 2003).
4. Coffin (2003) documented that up to three quarters of all employees (AEs) steal from their workplace at least once.
5. 40% to 70% of applicants lie on their applications for employment (Marett, 2004).
6. Game playing on office computers actually costs businesses about $50 billion a year and middle managers are the biggest perpetrators (Keng Siau, 2002).
7. Homicide is currently the fourth-leading cause of fatal occupational injuries in the United States. According to the Bureau of Labor Statistics Census of Fatal Occupational Injuries, of the 4547 fatal workplace injuries that occurred in the United States in 2010, 506 were workplace homicides. Homicide is the leading cause of death for women in the workplace.
8. If you ignore problem employees or handle workplace problems ineffectively, you will soon have an employee turnover problem as your other good employees will go elsewhere (Delpo and Guerin, 2007).
9. Negligence can apply to the hiring, supervision, and retention of an individual employee if a violent act by that person is foreseeable (Dana Loomis, 2008).

FACTORS CONTRIBUTING TO EMPLOYEE BEHAVIOR

Watson (2000) documented in his doctoral thesis that the four factors that most influence employee behaviors in the workplace are

- The individual's culture
- The corporate culture
- Corporate policies & procedures
- Other employee attitudes

Looking at these factors, which ones can we influence to reduce the employee problems in our organization? We can easily see that an individual's culture plays an important part in forming an employee's behavior in the organization, but this is not something we can control. However, the other three factors can very much be influenced by what we do as an organization and are directly related to policies, standards, procedures, and training.

The objectives we hope to achieve with policies and procedures are to get our employees to believe that having an ethical corporate culture is good for the organization and is good for the employees. The organization's security function can best accomplish these objectives by:

- Developing a robust ethical corporate culture by getting complete buy-in from top management.
- Implementing sound corporate policies and procedures that support the corporate culture and provide the basis for a secure work environment.
- Implementing an effective communications and training program to train employees on policies and procedures so they understand them and abide by them. In this step, we must essentially retrain the employees to embrace the organization's culture despite their individual cultural background.
- Consistently enforcing our policies and procedures by rewarding those who abide by them and punishing those who do not.

Without proper program documentation, training, exercises, and enforcement, employees can become confused and overreact; lawsuits may result from inconsistent application, security officers may not know how to respond, valuable time may be wasted, and problems often occur. A review of lawsuits showed several cases where firms were sued for millions of dollars for a variety of issues such as failure to provide proper training for monitoring security systems, failure to have enough security officers on duty at a site, failure to have adequate security patrols during certain hours, failure to conduct preemployment screening to weed out employees with violent

backgrounds, improperly retaining employees who have violated standards of conduct, and other issues that could be traced to lack of or enforcement of policies and procedures (Sorensen, 2008). Regulatory authorities have taken action against companies who violate various acts such as the Financial Services and Markets Act of 2000. One organization was fined over $10 million for not taking reasonable care to establish and maintain effective systems and controls for countering the risks of bribery and corruption associated with making payments to nonauthorized overseas third parties who assisted the organization in winning business from overseas clients (Amos, 2009).

The remainder of this chapter will be devoted to recommendations on how to develop meaningful Policies, Standards, and Procedures and to gain buy-in from your employees to create an ethical corporate culture and deal with employee problems legally and effectively.

DEFINITIONS

Employment-at-Will

"Employment-at-will" means that an employer can change the terms of the employment relationship with no notice and no consequences. For example, an employer can alter wages, terminate benefits, or reduce paid time off. In its unadulterated form, the at-will rule leaves employees vulnerable to arbitrary and sudden dismissal, a limited or on-call work schedule depending on the employer's needs, and unannounced cuts in pay and benefits.

Employment relationships are presumed to be "at-will" in all US states except Montana; however, the United States is one of a handful of countries where employment is predominantly at-will. At-will means that an employer can terminate an employee at any time for any reason, except an illegal one, or for no reason without incurring legal liability. Likewise, an employee is free to leave a job at any time for any or no reason with no adverse legal consequences. Most countries throughout the world allow employers to dismiss employees only for cause. As a result, from the point of view of US headquartered multinationals, firing employees gets stricter, more complex, and more expensive outside the United States. Outside the United States, laws regulate how, when, and why an employer can end an employment relationship. Many foreign employment termination laws impose lengthy notice periods, large severance pay, and cumbersome prefiring procedural steps. There can be heavy monetary penalties if these transactions are handled improperly. Settlements are usually calculated as a multiple of annual earnings. In the European Union particularly, termination settlements can amount from 2 to 3 years of earnings or more.

Security Governance

Security governance is the set of responsibilities and practices exercised by executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly. Our research has shown that through their emerging capabilities in the area of security governance and risk management, many organizations are taking proactive steps to ensure that their investments in security controls directly support their objectives for the business. A consistent, organization-wide view of security risks integrating both physical security and IT security is an essential element of this strategy. By combining superior security governance and risk management with an integrated approach to logical and physical security, organizations gain an advantage for competing in the global economy with a distinct advantage through an optimized IT infrastructure and better protection for their digital, physical, and human assets.

Security Program

A security program is a system of individuals, processes, policies, standards, and procedures developed to protect its assets and ensure that the organization adheres to all applicable federal and state laws, industry regulations, and private contracts governing the actions of the organization. A security program is not merely a piece of paper or a binder on a shelf; it is not a quick fix to the latest hot problem; it is not a collection of hollow words. An effective security program must be a living, ongoing process that is part of the fabric of the organization. A security program must be a commitment to an ethical way of conducting business and a system for helping employees to do the right thing. On a very basic level, a security program is about education, definition, prevention, detection, collaboration, and enforcement.

Physical Protection Systems

A Physical Protection System (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks. The functions of PPS are detection, delay, and response (Garcia, 2001).

Security Policy

A security policy is a general statement of management's intent regarding how the organization manages and protects assets. A policy is a guiding principle or rule used to set direction and guide decisions to achieve rational

outcomes in an organization. It is used as a guide to decision-making within the framework of objectives, goals, and management philosophies as determined by senior management. Policies exist to make sure that decisions fall within certain boundaries, leading to a consistent and fair approach. Policies are compulsory and supported by standards and procedures.

Security policies are office rules used to support management philosophies and set the tone for a security-minded culture. Security policies are also used to set a standard for projecting your organization image or to communicate regulations that apply to all personnel. Policies are most effective when they are issued and supported by top management as a result of interpreting the organization's mission and vision statements, and regulations. Policies are used to implement laws, industry standards, and common practices.

Security Standard

A policy is more effective when standards are also developed. Standards address what must be accomplished in specific terms, containing the means by which to implement one or more security policies. Standards are compulsory and supported by procedures.

Security Procedure

A security procedure is a set sequence of necessary activities that performs a specific security task or function. Procedures are normally designed as a series of steps to be followed as a consistent and repetitive approach or cycle to accomplish an end result. Once implemented, security procedures provide a set of established actions for conducting the security affairs of the organization, which will facilitate training, process auditing, and process improvement. Procedures provide a starting point for implementing the consistency needed to decrease variation in security processes, which increases control of security within the organization. Decreasing variation is also a good way to eliminate waste, improve quality, and increase performance within the security department.

The Difference between Policies and Procedures

A policy is a guiding principle used to set direction in an organization. A procedure is a series of steps to be followed as a consistent and repetitive approach to accomplish an end result. Together, policies and procedures are used to empower an organization with the direction and consistency necessary for successful implementation of security processes.

IMPORTANCE OF SECURITY DOCUMENTATION

Security policies, standards, and procedures are used to translate the organization's business philosophies into action by utilizing sound security principles. Well-designed security documentation for businesses is an invaluable communication tool for efficiently running operations within the security department and bridging the gap between interrelated departments in the organization. Policies, standards, and procedures improve decision-making by having an authoritative source for guidance and for answering questions. Well developed and documented security policies and procedures ensure compliance with national and local laws, regulatory agencies affecting business, government contracting authorities, independent certification organizations, and organization standards of conduct to ensure compliance with employee terminations and other administrative actions. Policies, standards, and procedures serve as a quality control mechanism for the security organization. This helps ensure optimum operations and consistent delivery of the finest security services. This program documentation provides the leadership, organizational structure, and processes that ensure the following for the organization:

- Strategic security direction is clear
- Security risks are managed appropriately
- Business objectives are balanced with security risks and are ultimately achieved
- Organizational security resources are used responsibly and effectively
- Security program effectiveness is measured.

Benefits Derived from a Strong Security Program

There are many benefits to an organization when they implement an effective security program. The following benefits are some of the most important:

- *Implementing a strong security program demonstrates to other organizations that your organization has a strong commitment to integrity*. One of an organization's greatest assets is its reputation; it is very problematic to repair once it is damaged. An effective security program can help preserve and enhance an organization's reputation by preventing fraud and abuse. If policies are issued from executive levels, policies help to convince employees and customers that the organization is committed to security. Increasingly as a result of business continuity planning, organizations are requesting proof of sufficient levels of security from other organizations they partner with in doing business.
- *Security documentation reinforces employees' support of the corporate culture*. Many employees have an inherent sense of honesty and welcome a means to report improper conduct without reprisal. A call to an

anonymous hotline addresses this need and may identify issues that raise both ethical and legal concerns. When employees see an affirmative response to reports of wrongdoing, strengthen the relationship of trust with their loyal employees, and deter future illegal activity.

- *Implementation of a comprehensive security program improves employee's security awareness regarding fraud, unethical behavior, and misuse of organization assets*. An effective program provides ongoing training of employees, monitors their understanding of policies and procedures, and implements the measures to discipline those personnel who violate the organization's code of conduct or other security rules.
- *Product and service quality is enhanced by an effective security program*. The organization's mission sets forth the vision of providing products and/or services of value. Security policies and procedures, continuous security awareness training of employees, thorough investigations, and timely response to violations and deficiencies enhances the organization's ability to deliver products or services of the highest quality which in turn leads to higher profits.
- *An effective security program reduces an organization's exposure to civil damages and penalties as well as criminal and administrative sanctions*. An effective security program implements procedures for promptly and efficiently responding to problems as they arise. Through early detection and reporting, an organization can minimize the losses from false claims, penalties, and sanctions imposed by regulatory bodies, fines, and repercussions for violating contracts, and losses and expenses due to lawsuits.
- *An effective security program may mitigate sanctions imposed by the government when violations do occur*. Even though organizations have implemented security programs, some employees may engage in conduct that violates applicable statues and regulations. The Organizational Sentencing Guidelines of the United States Sentencing Commission provide for a reduction in criminal fines in cases where an organization has implemented an effective program to prevent and detect violations of the law. Government agents place substantial weight on the existence of an effective security program that predates an incident and resulting investigation.
- *An effective corporate security program may protect corporate directors from personal liability*. The fiduciary duties of corporate directors require that they keep themselves adequately informed concerning the operations and finances of the organization. An effective security program designed to assure compliance with applicable legal requirements has been recognized as meeting this duty of care. Avoidance of penalties

and fines should be a major incentive for organizations to implement a security program. If a government entity finds an organization guilty of fraud and abuse, the penalties can be severe, and loss of business and damage to reputation will most assuredly result.

- *Security documentation improves communications*. Security program documentation serves to translate the organization's business philosophies and desires into action. Well-designed policies and procedures are an invaluable communication tool for efficiently running operations within departments and gaining cooperation between departments.
- *Policies and procedures improve consistency and reduce training time*. Policies and procedures will be a functional guide for training new and existing employees and will help prevent difficulties in performing duties due to lack of understanding or inconsistent approaches from personnel changes.
- *Program documentation improves productivity*. Policies and procedures speed up decision-making by managers by having a handy, authoritative source for answering questions.
- *Well-written policies and procedures support internal audits*. Internal audits are useful tools for pinpointing problem areas and uncovering criminal conduct by employees. These audits should be conducted soon after the program is fully implemented to ensure that the processes put in place are serving their purposes and functioning correctly; and also that changes can be made before the undesirable practices become a habit and difficult to change. Furthermore, audits may uncover security documentation that needs to be modified or changed completely because it is not serving the intended purposes.
- *Documentation provides historical records*. Security documentation prepared and updated as recommended will serve as a historical record of what practices were in place in an organization during a specified time period. This may be very important in a litigation case where an organization is being sued for wrongdoing. Evidence that an organization had certain policies and procedures and training in place at a particular time may help avoid negligence charges.

The Security Solution Hierarchy

Many organizations believe that the solution to their security problems is through technology and manpower, but in reality, management should implement low-cost solutions which support behavior modification such as implementing policies and procedures, training managers and employees on

security matters, and developing frequent security awareness communications programs with their employees. Higher cost solutions should be applied, only after less costly solutions have been exhausted, and significant risk remains. This is illustrated on the Security Source Online website as shown in the figure on the left (Nesbitt, 2007).While it is imperative that the organization have policies and procedures, it cannot be emphasized enough that *the only thing worse than not having a policy is having a policy and not enforcing it*. Another axiom is—*don't enforce policies you do not have*. In other words, if you do not have a policy regarding use of the organization telephones, don't try to take action against an employee for improper use of the telephone.

APPROACHES TO PREPARING SECURITY PROGRAM DOCUMENTATION

Many organizational policies originate with the chief executive officer and his/her executive team. These upper level policies are typically visionary and spawn operational policies. For example, if the chief executive officer says it is the policy of the company to maintain an active loss prevention program, the chief security officer will create a security policy that addresses loss prevention. He will then prepare detailed procedures to guide security department employees and others as to how losses are to be prevented.

Organizations must make decisions about how they will assign the security-related work to be done in an organization such as vetting and terminating employees, procuring space and equipment, protecting information assets, protecting physical assets, and business continuity. They then need to decide who prepares security documentation and how the documentation will get completed.

Centralized Approach

Some organizations have centralized their security operations under a Chief Security Officer and in so doing they prepare, issue, and control all policies, standards, and procedures. The advantages of a centralized approach are

- Consistent and more effective delivery of security requirements
- Consistent standardized format of security documentation
- Reduced redundancy
- One location for all documentation
- Better control of documentation
- Clarity of roles and responsibilities

- More efficient process to create and maintain documentation
- Facilitates enforcement efforts
- Optimizes allocation of limited security resources.

Decentralized Approach

In most organizations, security functions are not centralized into one body. Most organization's security functions are fragmented across several departments. For example, Human Resources (HR) takes care of vetting employees, the Facilities Department manages the access control system, and a third department such as Information Technology handles data security and business continuity. In the decentralized case, in order to develop the policies and procedures, the company should select a group of personnel and subject matter experts based on the following criteria:

- Personnel who will be responsible for maintaining the policy, standard, or procedure
- Personnel who perform work associated with the documentation
- Personnel who perform maintenance on associated equipment
- Engineers who design the associated systems
- Technical writers
- Safety & security personnel involved
- Environmental personnel
- Equipment manufacturers.

CONTENT OF DOCUMENTATION

No security documentation should be implemented until you have done a complete threat and risk assessment of your organization. A qualified and objective professional should conduct security assessments. Often, the use of a qualified security consultant achieves the best result because of his or her independent perspective. One of the biggest advantages of using a qualified security consultant is objectivity. If you decide to contract with a security consultant, be sure the consultant has no ties to the security product industry, including contract guard services and security equipment manufacturers.

Once you have assessed the threats and vulnerabilities your organization faces, you consider what steps can be taken to improve your physical security. You then create security policies by putting these steps in writing. The resulting documentation will serve as a basis for the security program. All managers and key employees involved with security should be required to review, improve, and implement these security program documents. Security

plan documentation is aimed at reducing your overall risk. It will, therefore, have at least four objectives, based on your risk assessment:

- Reducing the level of threats you are experiencing.
- Reducing your vulnerabilities.
- Improving your employee preparedness for threats.
- Maximizing your response to incidents.

Standards of Conduct

The standards of conduct, first and foremost, demonstrate the organization's ethical attitude and its emphasis on compliance with all applicable laws and regulations. The code of conduct is meant for AEs and contractors of the organization. This includes management, vendors, suppliers, and independent contractors. From the board of directors to volunteers, everyone must receive, read, understand, and agree to abide by standards of the code of conduct. The code of conduct provides a process for proper decision-making, for doing the right thing. It elevates corporate performance in basic business relationships and confirms that the organization upholds and supports proper conduct. Managers should be encouraged to refer to the code of conduct whenever possible, even incorporating elements into performance reviews, and compliance with standards of conduct must be enforced through appropriate discipline when necessary. Disciplinary procedures should be stated in the standards, and the penalty—up to and including dismissal—for serious violations must be mentioned to emphasize the organization's commitment. AEs must receive, read, and understand the standards and attest in writing that they have done this.

Recommended Security Policies, Standards, and Procedures for Best Practices

In addition to the standards of conduct, three types of security policies, standards, and procedures should be developed by every organization:

1. framework,
2. all employee, and
3. security specific.

All three types of policies, standards, and procedures are essential to a security program so that rules to which employees will be held accountable, and the method for enforcing rules are clearly documented.

Framework Policies, Standards, and Procedures

The framework documentation creates the structure of how the security organization is staffed and how the security program operates. Also, framework policies also provide other business practices like the employee selection process,

background-screening requirements for new employees, the organization's workplace violence policy, and the business continuity plan. Appendix 1 shows examples of Framework Policies, Standards, and Procedures.

All Employee Policies, Standards, and Procedures

These documents define the applicable laws, security regulations, and rules that apply to AEs and how to operate compliantly within those rules. They also indicate the applicable risk areas to an organization and describe appropriate and inappropriate behaviors about those risk areas. These documents should cover such subjects as the use of organization computers, telephones, and other organization assets and how the organization monitors employees' actions. These documents set the tone for the corporate culture and should be *strict but flexible, designed to meet the employer's needs, restrict employee actions, diminish the employee's expectation of privacy, and consistently be enforced*. These documents are the most important ones for building a strong corporate culture.

While most common laws may recognize the right of an individual to take legal action for an offense generally known as "invasion of privacy," such actions historically have not provided employees with additional protections. Courts have found that employers' monitoring of their employees' electronic transmissions involving email, the Internet, and computer file usage on organization-owned equipment is not an invasion of privacy. Invasion of privacy claims against an employer generally requires employees to demonstrate, among other things, that they had a "reasonable expectation of privacy" in their communications. Courts have consistently held, however, that privacy rights in such communications do not extend to employees using organization-owned computer systems, even in situations where employees have password-protected accounts (Harada, 2002). Appendix 2 shows examples of all employee policies, standards, and procedures.

Security-specific Policies, Standards, and Procedures

These documents provide detailed instructions to security employees and others for accomplishing specific security duties. These are extremely important as security system installation, operation, and monitoring is integral to the security program. Security systems such as electronic access control, intrusion alarm, closed circuit TV (CCTV), and monitoring systems are designed to detect events that are not expected in a facility, provide alarms to alert personnel monitoring security systems, assist them in determining the cause of the alarm, and then provide the ability to dispatch an appropriate security response. Access control systems should alarm if an unauthorized person tailgates behind an authorized person through a door or turnstile into a facility.

Intrusion detection systems should alarm if an intruder opens a door or window at the wrong time or without presenting a valid ID card or code. For each alarm point, security personnel assigned to monitor alarms should have detailed operating procedures describing what actions to take to assess the alarms. Organizations are expected to exercise reasonable care in training and supervising their employees in design, installation, operation, and monitoring of security. There are numerous lawsuits concerning poor security personnel practices, negligent training, and negligent supervision (Nemeth, 2005).

Appendix 3 shows examples of security specific (SS) policies, standards, and procedures.

THE PROCESS OF PREPARING AND MAINTAINING SECURITY DOCUMENTATION

The normal process followed in preparing security documentation consists of the following steps:

- Identification of the issue requiring action
- Issue analysis and discussion
- Consultation with subject matter experts
- Coordination with stakeholders
- Policy development
- Decisions on revisions
- Implementation
- Evaluation, testing, and feedback.

Structure of Documentation

Organizations should establish a consistent structure and format for all policies, standards, and procedures. Organizations should also establish a configuration management system to ensure that all documentation is in the same format, is updated at least annually, and is located on the organization's intranet where AEs can find it and read it. Some organizations have achieved good results using social media constructs such as blogs, wikis, and Microsoft Office SharePoint Server (MOSS). A wiki is a website that allows the easy creation and editing of any number of interlinked web pages. They are particularly efficient as a central repository for organization's policies and procedures. Everything can be kept in the wiki, making it easy for employees to revise documents, and eliminating the need for emails to circulate these materials. MOSS is also a robust collaboration tool, accessible organization-wide allowing users to view all files and emails that pertain to specific policies and procedures.

Format

Each document should have the following sections:

- Name—The name of the document
- Number—Numbers assigned by category and chronological order (e.g., framework, AE, SS)
- Classification (depends on organization document classification scheme)
- Version number and date—Current version number and release date
- Reason for issuance (initial release of reason for revision)
- Type—policy, standard, or procedure
- Purpose—The purpose or intent of the specific document
- Scope—What personnel or what processes the document applies to statement—policy, standard, or procedure statements and main instructions
- Compliance—Who is responsible for complying with the document and the consequences for noncompliance
- Enforcement—Date when the policy, standard, or procedure went into effect and how it will be tested
- Page numbers—All pages should be numbered. If only a page or section is changed, a new revision should be issued for the entire document reflecting the date of the change—Don't replace only changed pages.
- Issuing authority—Executive level signature.

The security manager should maintain a log showing the name, number, creation date, and revision dates of all documents. In case of litigation, it is important that all versions of the documents are retained in the files and logs so the security manager can easily demonstrate what business practices were in effect at the time of any claims or incidents.

Security program documentation must be living documents, not just a binder on a shelf. They must become integral to the day-to-day operation of the organization. That is what a judge will look for in a litigation case. How are the policies and procedures applied throughout the year? Are they incorporated into employee performance reviews? Are they reviewed and updated according to a schedule and on time? Are employees trained on them?

SECURITY AWARENESS EDUCATION

Security awareness education and training go hand in hand with your policies and procedures and strengthen your organization's security program by

demonstrating to employees that management supports the program enough to provide training. We suggest three types of training:

1. A general session on security awareness for all new employees—These training sessions are meant to heighten awareness among AEs and communicate and emphasize the organization's commitment to ethical business behavior, which affects AEs. A minimum of 1 to 3 h for basic training in security awareness should be provided for AEs. All new employees should receive a copy of the standards of conduct. The employees should also be trained on how to find the organization's security policies and procedures. Many organizations now include all the policies and procedures on the organization's intranet where AEs can view them. At the end of general training, every regular, temporary, and contracted employee should be required to sign and date a statement that confirms his or her knowledge of and commitment to the standards of conduct and the organization's security rules. This signed statement should be retained in the employee's personnel files. Organizations that require their employees to read and sign a statement every year are most successful in gaining compliance.
2. Refresher training periodically for employees in areas of high risk where problems have happened in the past, explaining how crimes have been committed, what signs to watch for, and methods for reporting employee dishonesty.
3. Special initial and refresher training for security organization employees regarding their duties. Refresher training should particularly address changes to policies and procedures. Provide longer, more intensive training sessions to employees in certain areas of responsibility such as those operating security systems.

MONITORING SECURITY AWARENESS AND MAINTAINING CONSISTENCY

Your employees are an excellent source of knowledge about what is really going on in the organization. Approached in the right way, they will help identify problem employees, weaknesses in controls, and suggestions for improvement. If management responds to their feedback by changing procedures and rewarding them accordingly, employees will recognize their benefit for participating in the process of improving their organization and will continue to find ways to contribute even more. Periodically send out questionnaires to a sampling of employees for feedback on your program, and conduct focus group interviews. Ask them openly about risks they see to the

organization, about their daily activities, the policies and procedures, and whether they observe areas for improvement. Ask employees to be truthful about whether AEs actually follow the policies and procedures or if they find ways to ignore them. Our research concludes that the best method to catch fraud and other crimes committed by organization employees is through tips received by other employees. One of the keys is to make sure employees that support you with suggestions are rewarded.

Data collection and tracking the performance of your security program are very important because they provide you with the ability to accomplish trend analysis and measure the progress of the security organization in achieving its goals. Consider the following techniques:

- Analyze security incident reports for trends that show improvements or deterioration of security organization's performance over a given period.
- Review of internal and external complaints filed against the firm or against the security organization.
- Pose security-related questions to departing employees in exit interviews to identify problems with peer employees or managers.

Enforcement and Discipline

Employees will be much more supportive of the organization terminating an employee for a violation of organization's policy, than merely because the organization decided to let them go for no reason. The place to start with enforcement is back at the beginning with the standards of conduct and the policies and procedures. One of the framework documents should set forth the degrees of disciplinary actions that may be imposed upon corporate officers, managers, and employees for failing to comply with the organization's security program documentation and applicable statues and regulations. That policy should include five main points:

1. Noncompliance will be punished
2. Failure to report noncompliance will be punished
3. An outline of disciplinary procedures from reprimand to dismissal
4. The parties responsible for actions at each level
5. Assurance that discipline will be fair and consistent.

Failure to detect or report an offense is a serious act of noncompliance and equally as deserving of discipline as the actual misconduct. Compliance with policies, standards, and procedures is an active, ongoing process that is everyone's responsibility. Security managers should consult closely with their HR and legal departments. There are no doubt existing disciplinary policies and procedures already in place which can serve as a guide in developing new

ones that will be consistent. The HR and legal colleagues should advise that you should not discipline employees without having properly informed them of the rules. The first step toward enforcement is distributing standards of conduct and other policies, standards and procedures, and educating employees about them. The training should include the consequences of noncompliance. Punishment for noncompliance can range from oral warnings, written warnings, suspension, privilege revocation, termination, or financial penalties as appropriate. Many organizations use this type of progressive discipline. The first step in this process should be a supervisor's conference. The purpose of the supervisor's conference is to make sure the employee understands the problem and is committed to correcting the inappropriate behavior. Depending on the situation, the next step might be a conference with a higher level of management, or it could be a written warning. The written warning is the more severe next step, and it emphasizes the seriousness of the situation and stresses the urgency of modified behavior. It should also state that the employee will face further disciplinary action, up to, and including termination if the problem behavior continues. Subsequent steps might include suspension without pay or infliction of a probationary period where the employee is advised to correct the behavior within a certain time period, e.g., 30 days, or face termination. The final step is termination once all other options have been exhausted. The severity of the infraction will determine the steps. Certainly, any step beyond the basic supervisor's conference should involve the HR and legal departments and the workplace violence team including a security representative (if one has been established). Proper and thorough documentation will be essential.

Typical disciplinary action chain (steps may be repeated more than once or skipped depending on the level and severity of the offense):

- Verbal warning
- Written warning
- Suspension
- Fine(s)
- Termination.

Punishment should be commensurate with the offense. There are offenses, such as blatant acts of fraud, that warrant immediate termination, but most infractions will likely be relatively minor and most likely unintentional. These may best be handled with education or additional training. Education should never be labeled as punishment. When put in a positive and supportive context, it can efficiently correct noncompliant behavior. Be sure your policies and procedures include remedial steps such as additional training. Discipline is only a part of the enforcement equation. Objectives and plans for individuals and departments should include security initiatives.

Achievement of those plans, especially when rewarded, is a positive reinforcement that encourages support for and enforcement of the security program. Performance appraisals should include security elements and allow supervisors to recognize favorable or improved security performance. Your security program will be better enforced if you also find ways to reinforce through positive means and not just disciplinary measures.

REVIEW QUESTIONS

1. Define Policy?
2. Define Standard?
3. Define Procedure?
4. Name the three types of Policies, Standards, and Procedures and give an example of each.
5. List three benefits from security documentation.

References

ACFE, 2012. 2012 ACFE Report to the Nation on Occupational Fraud. Association of Certified Fraud Examiners, Austin.

Amos, W., 2009. Final Notice of Requirement to Pay Penalty. Financial Services Authority, London.

Christopher, D.A., 2003. Small business pilfering: the trusted employee(s). Bus. Ethics 12, 284–297.

Coffin, B. (2003, September). Breaking the silence on white collar crime. Risk Management Magazine.

Dana Loomis, P., 2008. Preventing Gun Violence in the Workplace. ASIS, Alexandria.

Delpo, A., Guerin, L., 2007. Dealing with Problem Employees: A Legal Guide. Delta Printing Solutions, Inc, Berkeley.

Mary Lynn Garcia, 2001, The Design and Evaluation of Physical Protection Systems, Butterworth Heiman.

Harada, D.D., 2002. EMPLOYEE PRIVACY—Computer-Use Monitoring Practices and Policies of Selected Companies (GAO-02-717). General Accounting Office, Washington.

Keng Siau, F.F.-H., January 2002. Acceptable Internet Use Policy. Communications of the ACM, New York, pp. 75–77.

Marett, J.G. (2004, May). The truth about lies: reminding interviewers that applicants lie may help screen out fabrications and exaggerations. HR Magazine.

Nemeth, C., 2005. Private Security and the Law. Elsevier Butterworth-Heinemann, Burlington.

Nesbitt, W.H. (2007, February 3). The SSO Security Solution Hierarchy. Retrieved August 27, 2009, from Security Source: http://www.securitysourceonline.com.

Sorensen, S., 2008. Physical Security Practice and Premises Liability. Physical Security Council's Managing Your Physical Security Program. ASIS International, Sante Fe.

Watson, D., 2000. Ethics and corporate investigations. ACFE Fraud Symposium. Saudi Aramco, Dhahran.

Further Reading

Arthur Gross-Schaefer, J.T.-S., 2000. Ethics education in the workplace: an effective tool to combat employee theft. J. Bus. Ethics, 26, 89–100.

Board Briefing on IT Governance, 2nd Edition. (2003). Retrieved October 5, 2009, from IT Governance Institute: http://www.itgi.org.

Daniel Roach, R.J., 2004. The Complete Compliance and Ethics Manual, Society of Corporate Compliance and Ethics. United States of America, Minneapolis, MN.

Davis, G. (2009, September 17). Workplace Violence Costs Companies Mondy, Women Their Lives. Retrieved October 13, 2009, from www.associatedcontent.com: http://www.associatedcontent.com.

Hayes, R., 2008. CRISP REPORT: Strategies to Detect and Prevent Workplace Dishonesty. ASIS International Foundation, Alexandria.

In re: Westinghouse Air Brake Technologies Corporation, Litigation Rel. No 20457 (SEC February 14, 2008).

In the Matter of InVision Technologies Violation of FCPA, SEC Rel. No. 19078 (SEC February 14, 2005).

Jackson, E., 2008. Corporate security policies and standards: combining policies and standards under one jurisdiction. Continuity Planning & Management. CPM Press, Orlando.

Muhl, C.J., 2001. The employment-at-will doctrine: three major exceptions. Mon. Labor Rev. 45 , 3–5.

Patterson, D.G., 2013. Implementing Physical Protection Systems: A Practical Guide. ASIS Press, Alexandria.

Pinkerton, 2003. Top Security Threats and Management Issues Facing Corporate America. Pinkerton, Alexandria.

Rotvold, G., 2008. How to create a security culture in your organization. Information Management, New York.

Wells, J.T. (1999, August). A Fistful of Dollars. Association of Certified Fraud Examiners. *Improving Security Awareness*, by David G. Patterson, CPP, PSP. ABCHS.

APPENDIX 1—FRAMEWORK POLICIES, STANDARDS, AND PROCEDURES

Physical security framework involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent unauthorized access and protection of people, information, materials, and infrastructure. This includes designing measures that prevent, deter, detect, and delay unauthorized access, acts of damage, and violence. The measures will also provide for an appropriate response. The framework policies create the structure of how the security organization is staffed and how the security program operates.

Policies

- Security Organization Mission
- Organization Chart and Reporting Structure

- Roles and Duties of the Security Organization
- Physical Security Program and Applicable Elements of Prevention, Detection, and Response
- Security Considerations for Selecting, Designing, and Modifying Facilities
- Anonymous Reporting of Suspected Violations and Nonretaliation for Reporting of Violations
- Investigating Employee Violations of Standards of Conduct
- Employee Vetting
- Responding to Internal and External Requests for Documents or Other Investigations such as Search Warrants, and/or Subpoenas
- Company Documentation Classification, Retention, and Destruction
- Employee Exit Interviews
- Protecting Company Assets
- Privacy of Employee Information
- Workplace Violence
- Media Relations
- Business Continuity Planning
- Crisis Management and Response
- Office Site Selection
- Protection of Company Equipment and Other Assets

Standards

- Set Back Distances for Office Buildings
- Signage
- Information Required On Employee Background Checks and Items Identified for Acceptance or Rejection
- Acceptable Methods of Protection and Destruction of Company Information on Each Media Type
- Interior and Exterior Lighting Requirements
- Doors, Windows, Locks, and Keys
- Approved Fencing
- Approved Barriers
- Landscaping
- Asset Marking and Identification (Laptops etc.)

Procedures

- Reporting Standards of Conduct Violations
- Investigating Standards of Conduct Violations
- Disciplinary Actions for Misconduct

- Procedures for Responding to Internal and External Requests for Documents or Other Investigations such as Search Warrants and/or Subpoenas
- Conducting Exit Interviews
- Content and Frequency of Audits (Internal and External)
- Protecting Company Assets (Maintaining an Inventory of Equipment, Including Serial Numbers and Physical Descriptions, Who They Were Issued To, Date of Issue, Recovery, and Disposal)
- Protecting Intellectual Property (Securely Marking and Storing Sensitive Documents, Securely Disposing of Sensitive Information, and Security Notification if Sensitive Information is Disclosed or Misplaced)

APPENDIX 2—ALL EMPLOYEE POLICIES, STANDARDS, AND PROCEDURES

All employee (AE) security policies and procedures apply to AEs and should be provided to AEs along with training during their orientation. It is also very important that employees know where these policies and procedures are located on the company intranet and reviewed periodically.

Policies

- Reporting Dishonesty in the Workplace
- Alcohol and Drug Testing
- Employee Monitoring Processes for Telephone, Mail, Computer Use and Internet Use, etc.
- Company Identification Issuance and Wearing
- Preventing inappropriate Actions in Specific Risk Areas Identified as Likely Threats to the Company such as Petty Cash Accounts and Inventory Controls
- Ensuring Appropriate Behavior in Specific High-Risk Areas
- Periodic Internal Assessments of High-Risk Areas
- Documentation Requirements for Travel Expenses
- Key and Combination Controls
- Conditions for Allowing Visitors in the Office including Employee Escorts
- Business and Personal Deliveries
- Vetting of Employees
- Terminating Employees
- Vetting and Monitoring of Cleaning Contractors and Other Vendors
- Restricted Areas of the Company and Control of Unauthorized Visitors
- Sensitive Information Classification, Protection, Destruction

- Access Control to Company Facilities
- Accident/Injury Response and Reporting
- Bomb Threats
- Cash Handling and Storage
- Court Testimony by Employees
- DMV Periodic Review of Employee Driving Records (DMV Pull Notice)
- Drug and Alcohol Use and Testing
- Emergency Preparedness and Response
- Fraud Detection and Control
- Security Awareness Training

Standards

- First-Aid Supply Kit Contents
- First-Aid Supplies per number of Employees
- Emergency Supply Kit Contents for Employees
- Emergency Supplies per number of Employees
- Emergency Response Team per number of Employees
- Emergency Response Team Training
- Acceptable Results of Drug and Alcohol Testing
- Content and Frequency of Security Awareness Training

Procedures

- Access Violations Reporting
- Alcohol and Drug Testing
- Bomb Threat Response Procedures
- Bomb Search Procedures
- Documentation Requirements for Travel Expenses
  - Emergency response procedures related to:
  - Emergency evacuation
  - Shelter-in-Place
  - Who to contact in the event of a fire, flood, earthquake, or other natural disaster
  - How to perform certain key emergency repairs
- How to contact the companies or organizations that provide services such as electrical power, water, telephone, and internet access
- Employee Monitoring Processes (Telephone, Email, Computer Use, Internet Use, etc.)
- Escorting Visitors
- Fraud Detection
- Hazardous Materials Documentation and Disposal Procedures
- Incident Alerting and Reporting Procedures

- ID Lost/Forgotten
- ID Wearing
- Laptop Security Procedures
- Medical Emergencies
- Office Opening and Closing Procedures
- Parking Controls Procedures
- Personal Protection for Employees
- Petty Cash Withdrawals or Deposits
- Reporting Dishonesty in the Workplace
- Reporting procedures for disclosed or misplaced sensitive materials
- Rewarding Employees for Positive Security Performance
- Robbery Reporting
- Stationary, Forms, and Business Cards Controls
- Suspicious Persons and Activities Reporting
- Travel Safety and Security
- Weapons—Possession in Facility and Parking Lots

APPENDIX 3—SECURITY SPECIFIC POLICIES, STANDARDS, AND PROCEDURES

Physical Protection Systems only perform their functions well when there is an appropriate balance of the following elements:

- *Architectural elements*—such as barriers and locks, exterior and interior lighting, critical building services, space layout, parking, dock facilities, egress stairs, and adjacent facilities.
- *Operational elements*—such as organization and staffing, policies, standards and procedures, training, visitor control, security guard staffing, postorder assignment and execution, alarm and incident assessment, incident responses, administration of security systems, delivery processing, and emergency response.
- *Security systems elements*—such as automated access control, intrusion detection and alarms, closed circuit television, communications, and security control centers.

The operational elements consisting of the people, policies, standards, procedures, decision-making, common sense, and awareness must be included early in the implementation process during the time of the system design—not after the system has been designed and implemented. The security specific documentation provides the information needed by the people to properly interface with the security systems hardware and software such as

- Monitoring Security Systems such as Access Control, Intrusion Detection, and CCTV
- Controlling Access to Sites or Buildings
- Screening and Searching Visitors and Employees Entering or Leaving
- Assessing the Cause of Alarms
- Responding to Alarms or Attacks
- Escorting Visitors
- Escorting Employees to Parking Areas
- Reporting Security Incidents, Tracking, and Determining Trends

Policies

- Use of Guard Forces to Protect Assets
- Security Officer Staffing
- Facility Patrolling
- Access Control—Employees, Vendors, and Contractors
- Access Control—Visitors
- Alarm System Management
- Arrest Powers
- Cash Handling
- CCTV Management and Surveillance
- Criminal Violations
- Crisis Management and Response
- Demonstrations Against Company Facilities (Including Lockdown)
- Security and Safety Investigations
- Due Diligence Investigations on Strategic Partners and Major Support Contractors
- Employee Information Security and Privacy
- Security Assistance with Employee Terminations
- Enforcement of Security Policies
- Executive Protection
- Facility (Site) Protection Plan
- Fingerprinting and Photographing of Employees
- Fire Department and Emergency Medical Teams—Support Agreements, Authority, and Jurisdiction
- First-Aid and Medical Emergencies
- Fraud Detection and Control
- Hazardous Materials Documentation and Disposal
- Incident Alerting and Reporting
- Internal Investigations
- Inventory, Delivery, and Receiving Controls
- Key and Combination Issuance and Control
- Kidnap, Hostage, and Extortion

- Laptop Security
- Mail Screening (Explosives and Other Harmful Substances)
- Media Relations
- Possession and Carrying of Firearms
- Physical Inventory of Valued Assets
- Police Department—Support Agreements, Authority, and Jurisdiction
- Rewarding Employees for Positive Security Performance
- Risk and Vulnerability Assessment
- Search and Seizure of Evidence
- Security Awareness Program
- Security Staff Training
- Service of Legal Process
- Threat Advisory Levels and Terrorism Threat Response Plan
- Transportation of Currency and Valuables
- Travel Safety and Security
- Use of Force

Standards

- Design of Identification Credentials and Access Cards for Employees, Visitors, Contractors, Vendors, etc.
- Design of Parking Permits
- Security Systems (Standards for Deployment of Electronic Security Devices Based on Size or Location of Office)
- Assignment of Restricted Areas within the Office
- Penalties for Lost Credentials and Access Cards
- Schedule for Replacement of Credentials and Access Cards
- Schedule for Audit and Rekeying of Office Keys
- Security System Maintenance Schedules
- Limits on the Number of Executives Traveling Together
- Authorized Uses for Company Credit Card
- Security Staff Training Schedules and Topics
- Guard Force Clothing and Equipment
- Guard Force Training
- Guard Force Testing and Metrics

Procedures

Procedures that should be developed and implemented for the security program include the following:

- Access Control—System Override
- Accident/Injury Response and Reporting
- Alarm System Management

- Alarm System Mitigation of Nuisance Alarms
- Delivery and Shipping Monitoring and Documentation
- Documenting Security and Safety Investigations
- Employee Access Control Procedures
  - Assigning Access Rights
  - Access Violations
  - Credential Types
  - Credential Issuance and Retrieval
  - Lost/Forgotten Credential
  - Visitors Credential
  - Wearing of Credentials
- Incident Reporting
- Inventory, Delivery, and Receiving Controls
- Key Issuance and Control
- Kidnap, Hostage, and Extortion
- Mail Screening Procedures (Explosives and Other Harmful Substances)
- Media Relations (How to Deal with the Media)
- Office Opening and Closing Procedures
- Office Lockdown
- Outsourcing Security Services
- Parking Controls Procedures
- Personal Protection for Employees
- Petty Cash Withdrawals or Deposits
- Physical Inventory of Valued Assets
- Police Department—Memoranda of Understanding Authority and Jurisdiction
- Robbery Procedures
- Reporting Suspicious Persons and Activities
- Security System Malfunctions and Trouble Shooting
- Testing and Training Requirements for Security Officers
- Threat Advisory Levels and Terrorism Threat Response Procedures
- Vetting and Monitoring of Cleaning Contractors and Other Vendors
- Security Officer Postprocedures
- Security Officer Patrol Procedures

Index

Note: Page numbers followed by "*f*" and "*t*" refer to figures and tables, respectively.

C

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Z

SECURITY

FOURTH EDITION

CONTEMPORARY SECURITY MANAGEMENT

A clear and concise overview of the principal functions and responsibilities of contemporary security supervisors and managers

KEY FEATURES:

- Examines the evolving characteristics of major security threats confronting any organization
- Explains how to match one's personal expertise and interests with particular areas of security management
- Includes updated information on the latest trends in ethics, interviewing, liability, and security-related standards

Contemporary Security Management, fourth edition, identifies and condenses into clear language the principal functions and responsibilities for security professionals in supervisory and managerial positions. Managers will learn to understand the mission of the corporate security department and how the mission intersects with the missions of other departments. This book instructs managers on the critical interactions they will have with decision-makers at all levels of an organization, keeping them aware of the many corporate rules, business laws, and protocols of the industry in which the corporation operates. It includes updated coverage of the latest trends in ethics, interviewing, liability, and security-related standards.

Contemporary Security Management provides concise information on the managerial skills of budgeting, acquisition of capital equipment, employee performance rating, delegated authority, project management, counseling, and hiring. It also explains the building blocks of protection of corporate assets, monitoring of contract services, and guard force operations, and explores how to build quality relationships with leaders of external organizations, such as police, fire and emergency response agencies, and the Department of Homeland Security.

JOHN J. FAY is a security management professional, and has served as a special agent of the US Army Criminal Investigation Division (CID) and later the Director of the National Crime Prevention Institute at the University of Louisville, United States. He holds the Master of Business Administration from the University of Hawaii, United States, and has authored several books, including *Model Security Policies, Plans and Procedures* and *Encyclopedia of Security Management, 2e*.

DAVID PATTERSON is the Principal Partner at Patterson & Associates International, United States. He is an international physical security consultant with more than 30 years of experience. Mr. Patterson's specialties include risk assessment, security program assessment, security master planning, security systems design, project management, business continuity planning, emergency preparation and response, crisis response planning, and family contingency planning.

ELSEVIER

Butterworth-Heinemann
An imprint of Elsevier
elsevier.com/books-and-journals

ISBN 978-0-12-809278-1