Disaster Recovery and Corporate Survival Strategies

Disaster Recovery and Corporate Survival Strategies

Pre-emptive procedures and countermeasures

LOUISE BROBY

FT Prentice Hall
FINANCIAL TIMES

An imprint of Pearson Education

London ■ New York ■ Toronto ■ Sydney ■ Tokyo ■ Singapore ■ Hong Kong ■ Cape Town
New Delhi ■ Madrid ■ Paris ■ Amsterdam ■ Munich ■ Milan ■ Stockholm

PEARSON EDUCATION LIMITED

Head Office:
Edinburgh Gate
Harlow CM20 2JE
Tel: +44 (0)1279 623623
Fax: +44 (0)1279 431059

London Office:
128 Long Acre
London WC2E 9AN
Tel: +44 (0)20 7447 2000
Fax: +44 (0)20 7447 2170
Website: www.briefingzone.com

First published in Great Britain in 2002

ISBN 0 273 66162 0

British Library Cataloguing in Publication Data
A CIP catalogue record for this book can be obtained from the British Library.

10 9 8 7 6 5 4 3 2 1

Typeset by Monolith – www.monolith.uk.com
Printed and bound in Great Britain by Ashford Colour Press Ltd, Gosport, Hants.

The Publishers' policy is to use paper manufactured from sustainable forests.

About the author

Louise Broby is a financial writer who has writen extensively on a wide range of topics. Her publications include *Investment Regulation in Europe*, *Global Stock Markets*, *Pan-European Financial Regulations* and *Stock Market Globalisation*. She has worked in investment banking and as a business school academic.

Louise may be contacted at:

Stratos Multimedia LLC
6th Floor
175 Piccadilly
London W1J 9TB

Tel: 07802 882 554
E-mail: lb@stratos.demon.co.uk

Contents

Figures

Tables

Executive summary

The focus on disaster recovery and corporate survival strategy has heightened in recent months, following September 11 as well as deepening recessionary trends. Mission-critical data are the life-blood of many organizations, especially in the financial sector, and transport and communications. The 'it never happens to us' attitude has been badly shaken by the wide impact of the World Trade Centre attacks, with a roster of finance companies reading like a 'who's who' in finance, all affected, some seriously with loss of life, IT systems and offices. Companies are now revising their disaster recovery and business continuity plans and examining whether new hardware and software solutions, a repositioning of remote backup facilities or the creating of replicate facilities are the answer.

This Executive Briefing sets out to examine the state of the disaster recovery and backup market in the UK and the US, and the solutions that are being recommended by software vendors and implemented by industry.

CHAPTER CONTENT

- In Chapter 1, an overview is given of the potential disasters that can cause damage to equipment and backup data. With the fading of the impact of the bombings in the City of London in the 1990s, terrorist attacks were on the backburner for a while, but with the devastating attacks on the World Trade Centre, terrorism is right back on the agenda for backup strategies and disaster recovery plans. The chapter deals with the new phenomenon of multiple terrorist strikes, as well as other disasters such as earthquakes, floods and lightning causing voltage surges and fires. Also referred to in the chapter are systems failures and consequent loss of data, which can be caused by attackers either from outside or inside the organization. Human error is a common cause of loss or corruption of data, through sabotage, insufficient security and self-replicating malicious viruses, which can penetrate through the Internet at ever increasing speeds.
- Chapter 2 addresses the question of the extent to which corporations are ready to face a disaster, in terms of backup facilities and other strategies aimed at dealing with critical incidents. September 11 showed that on the whole, the finance companies had their backup systems in order, but nobody could have predicted or safeguarded against the immense loss of life and facilities. One company had its main processing systems in one of the two towers that collapsed, and its backup facilities in the other. Factors that affect a corporation's ability to withstand adverse events, such as defective backup systems, failure to back up, outmoded backup solutions and lack of training or insufficient manpower, are elucidated.

- Chapter 3 outlines risks associated with backup systems and discusses the approach to risk management. It refers to some of the protective measures taken by the industry to prevent attacks, such as remote locations, special software, firewalls, digital signatures, passwords and other access control systems. Recommendations for maintaining and improving security are set out.
- Chapter 4 discusses the two prevailing concepts of disaster recovery and business continuity planning, and draws a distinction between them, with disaster recovery plans tending to concentrate on IT, and business continuity plans involving the enterprise as a whole. The content and strategies involved in disaster recovery and business continuity are outlined.
- Chapter 5 looks at current backup and storage solutions. Traditional tape backup, still dominant in the market, is discussed and disk storage formats are outlined. New tape storage formats, such as LTD, AIF, DTF and S-DLT, are referred to. Developments in backup, such as intelligent backup, virtualization, clustering, mirroring and snapshots, are delineated. The impact of fibre channel technology on storage is assessed and the differences between the various networking configurations are illustrated.
- Chapter 6 looks at storage in remote location as an important way of securing data from disasters. As technology has advanced, so has the reach of networks, and storage centres can be geographically removed from one another, thus dispersing the risks.

  Rather than companies running and administrating their own duplicate backup facilities in remote site locations, many resort to the use of colocation centres, which provide up-to-date hosting and backup facilities in specialist centres. Some of the main colocation centres and their facilities are referred to. A cost-effective solution for companies having to cope with a disaster is the concept of mobile disaster recovery centres.

  As part of their revision of disaster recovery plans, many companies have modified their mobile phone strategies, since, as September 11 showed, the possession of mobile phones has proved to be a vital element in communicating with the outside world in case of disaster when all other communications links fail.
- Chapter 7 considers outsourcing which, for a while in the doldrums, has had a comeback with the increasing complexity of IT systems and the shortage of skilled IT staff. The many advantages of outsourcing are outlined, such as predictable costs, maintenance of systems and availability of trained staff. Insourcing, again increasingly popular, is also discussed. Managed service providers supplying software and upgrades are referred to, with examples. The results of a survey recently carried out into managed services are published.
- Chapter 8 looks at how, with IT budgets under pressure, backup and storage costs are under increasing scrutiny, but as an industry sector, storage has proved

resilient and indeed in an expansion mode. Methods of calculating IT backup costs, such as TCO and ROI, are explained. Costs not to be overlooked in protection against downtime include maintenance costs, insurance premiums, and the costs of protecting buildings and equipment against fire, water, voltage surges, etc. For those with remote storage facilities, a whole new set of costs has to be taken into account. Costs of catastrophic events as reflected in insurance claims are set out.

- Chapter 9 focuses on the financial services sector, which relies heavily on electronic systems not only for backup and storage but also for the operation of the businesses themselves. Regarded as the pioneer of new IT technology, and under constant regulatory scrutiny, the financial services industry has continued to invest heavily in IT equipment. As a result, many of the companies affected by the September 11 attacks were able to announce that clients' data were safe and they could resume operations shortly afterwards.
- Chapter 10 mentions some of the major vendors of IT backup and storage equipment, and refers to some of the latest products available in the backup and restoration area. It also looks at the main industry associations, such as the Fibre Channel Association and the Storage Networking Industry Association.
- Chapter 11 contains the conclusions for each chapter and summarizes the contents of the Executive Briefing.
- A glossary with many of the terms used in the storage and backup industry is included.

Acknowledgements

My thanks to all those who have contributed to the contents of this Briefing, including IT vendors such as Compaq, Hewlett-Packard, Dell, Dantz, Fujitsu, Optomedia, CMG, Bredon, network storage companies, tape backup companies, disaster recovery companies, business continuity planners, outsourcing companies, colocation centres, editors of computer magazines, and professional institutions. The Fibre Channel Association has been particularly helpful in contributing information on FC networks. I have also received enthusiastic advice and support from many of the PR companies representing the IT industry.

A special thanks to the Senior Acquisitions Editor of the FT Executive Briefings series, Laurie Donaldson, whose guidance has been invaluable.

Introduction

THE ELECTRONIC SOCIETY

With the advent of complete automation, the corporate world is increasingly dependent on fully functioning, reliable computer systems. In the lead-up to a computerized world, corporations relied on manual duplicate systems for backup if anything went wrong. But increasingly, the paperless electronic society is taking over. People are giving way to computers in backing up, storing and analyzing data and information. Only those responsible for administration of input and output, and interpretation, remain.

GREATER VULNERABILITY

With this increased dependency on technology comes greater vulnerability. If IT systems go down, business comes to a standstill. Millions, even billions, of pounds are lost, depending on the severity of the systems failure and the nature of the business. Records are no longer accessible, and in the worst case scenarios are lost permanently.

To guard against such eventualities, managers spend ever greater amounts on better, more secure technologies. But even the most advanced and most expensive technologies can fail. And not for just a few isolated reasons. Attacks on the system can be external or internal and can come from a variety of sources, some of them unexpected, as we saw in the devastating aircraft-turned-into-missile strikes on September 11, 2001.

DEFENSIVE TACTICS

The business community, however, increasingly aware of the threats to its systems, is not taking things lying down. A number of precautionary and defensive tactics have evolved, in boardrooms and in IT departments, with or without consultation with the IT vendors. Governments, official bodies and industry associations are also taking part in the fight to keep the high-tech IT systems alive and well.

Originally, the backup of critical data was left to simple backup disks and tapes on which data were stored en bloc at the end of each working day, or less frequently. Stories abound of the early backup devices being stored in the backs of vans, in garages and at other insecure locations. As the flaws in these methods became obvious, new solutions to a backup were developed. It soon became

apparent that it was not enough to store data and leave it at that. The bombings in the 1990s made the business community aware of the need for safekeeping and accessibility of backup tapes. Disaster recovery procedures were evolved which tested the backup storage set-up from time to time to ensure that access to recovery of data was possible at short notice even if disaster struck.

LESS DOWNTIME

In the early days, and even in many places today, the backup process interfered with the normal operation of processing systems, and downtime due to backup being carried out was normal. Speedier transfer of data was called for and the IT gurus complied, evolving ever faster and more complex systems. Data transfer to backup systems evolved from being a once-in-a-while affair through incremental to simultaneous. New backup hardware and software solutions were evolved which minimized or eliminated interference with day-to-day routine business operations.

THE FINANCIAL SERVICES SECTOR

Pioneering technological advances in introducing sophisticated backup systems was the financial sector, which to a higher degree than most other sectors was dependent on an efficient, reliable and fast number-crunching capacity. The financial services sector spent vastly more than other sectors on ensuring that its systems were running without disruption, and as a result this sector has the most advanced state-of-the-art systems available. However, this did not prevent some of the financial services firms hit by the devastating September 11 terrorist attack from losing data. Although backup facilities were in place, they were not always immediately accessible for a variety of reasons. One firm was reported to have its processing centre in one of the WTC towers and its backup facilities in the other. Others lost key personnel and were unable to carry on as normal with the remaining staff.

THE RATE OF TECHNOLOGICAL CHANGE

Technological change is progressing at a dizzying pace. In 1965 Gordon Moore, the founder of Intel, predicted that the number of transistors per square inch on integrated circuits would double every year. 'Moore's Law' was based on observations of the rate of change since the integrated circuit was developed. Although the pace subsequently slowed down, in large measure his predictions

have held true, with data density doubling approximately every 18 months. Moore himself has accepted this new version of his law, and the trend is expected to continue for the foreseeable future.

BACKUP AND STORAGE INDUSTRY GROWTH

The Storage Networking Industry Association has estimated that the expansion in storage capacity for the largest 2000 companies globally has grown from 40 terabytes in 1998 to 300 terabytes in 2001, and will exceed 1000 terabytes by 2003. The storage industry is predicted to become a US$ 60 billion industry by 2003. This explosive growth is fuelled by the growth in information, the increase in e-commerce and use of the Internet, the ever increasing need to store data in general, and the expansion in e-mail traffic to include more and more employees.

The increase in storage capacity is also likely to be influenced by the growing availability of broadband, which will make it less expensive and faster for companies to use local area networks (LANs), storage area networks (SANs) and wide area networks (WANs), thus making it possible for more and more small to medium enterprises (SMEs) to embrace the new technologies.

THE BENEFITS OF HIGH-TECH SYSTEMS

The benefits of having high-tech backup systems in terms of disaster restoration and recovery are many. Increasing client demands for 24×365 services can be met with high-tech solutions for maintenance and backup, which do not require extensive downtime. If disaster strikes, the recovery time is vastly reduced, with less disruption of business services. The higher levels of automation built into new software and systems allow for savings in terms of human staffing costs and reduce the element of human error. Automation also allows more data to be processed in less time. Again, the information explosion and the need to store ever-increasing volumes of data are fuelling this trend. The ability to restore data in turn protects the organization in case of legal disputes, provided the electronic trail is above board.

The retention of customer confidence is a corollary of improved systems, since disruptions are becoming minimal and do not cause the same degree of loss of reputation, lowering of service levels, and loss of communications and operability of electronic systems, such as trading systems. Information can be stored on a hierarchical basis, whereby mission-critical information is made readily and instantly available, and other information, which is rarely accessed, can be stored nearline or offline.

OUTSOURCING

With the higher levels of complexity and need for staff in a tight labour market and problems of budgetary control over IT systems, many organizations are looking at the option of outsourcing or insourcing their backup and recovery systems, or parts thereof, or indeed their entire IT function. Such a solution enables companies to be up to date as regards new systems and techniques at all times, without constantly having to scour the market for innovations.

TECHNOLOGY – THE WAY FORWARD

Technology has become an indispensable weapon in corporate entities' efforts to gain competitive advantage in retaining and expanding market share, in providing 24×365 service to their clients and indeed in their strategies for long-term survival should a major disaster strike.

1

Backup and storage: potential disasters

INTRODUCTION

Businesses have become increasingly vulnerable to attacks on their IT systems in recent years due to a change in a number of parameters, including technology and the Internet user profile, and above all the techniques used by attackers.

Disasters affecting IT systems, including backup solutions, can be ascribed to natural causes, malicious human intervention or attack, human error, inertia, incompetence, lack of training or systems failure. Looming large in impact, if not in numbers, in recent years is the terrorist attack. The bombings in 1995 in the City of London and Docklands, and most recently the September 11 attacks, overshadowed all other events.

The main causes of IT data loss in the US have been broken down by Ontrack Data International, recovery services providers (2001, pre-September 11), as shown in Table 1.1.

Table 1.1 **Main causes of IT data loss in the US**

Cause	*Percentage*
Hardware or system malfunction	44
Human error	32
Software corruption or program malfunction	14
Computer viruses	7
Natural disasters	3

Note: Terrorist attacks, bombings, etc. are not included, due to their infrequent occurrence.
Source: Ontrack Inc.

TERRORIST ATTACKS – SINGLE AND MULTIPLE STRIKES

Terrorist attacks have hitherto been a one-off event, but September 11 saw the multiple terrorist attacks in which the two World Trade Centre towers were attacked in separate strikes and collapsed altogether, along with the devastating attack on the Pentagon in Washington.

The financial services industry was particularly hard hit in the WTC attacks, with some 1700 people killed. Trade was lost due to loss of personnel office space and computer downtime, and for the first time ever, the stock markets were closed for four consecutive days.

The McKinsey Report (December 2001) analyzed the impact of September 11 on the New York economy, focusing on the financial markets. The report identified

'structural deficiencies in the financial sector, lack of geographic diversity in backup plans, insufficient access to sites, a lack of alternative networks and systems for telecommunications power, and a vulnerability to "choke points"'.

The attacks prompted a major revision of the security of stock exchange trading systems. Antonio Zoido, Chairman and CEO of the World Federation of Exchanges, called for the installation of both backup computers and backup telecommunications systems in different locations, and pointed out that electronic exchanges are easier to duplicate since they do not have a physical trading floor.

NATURAL DISASTERS

Major causes of natural disasters impacting the operation of businesses are as follows.

Earthquakes

Earthquakes are one of the most feared and least understood of natural disasters. What is known is based on geological facts. Earthquakes occur along fault zones, i.e. zones around active faults varying in width. The faults are fractures in the earth's crust along which rocks move relative to one another. 'Active' faults are faults that have erupted during the last 11 000 years. The San Andreas Fault in California, the western edge of the North American continental plate, is one of the best-known faults, with Los Angeles being in the top ten risk areas. Tokyo is classed as the number one potential risk, but the earthquake that hit Japan in 1995 was in Kobe, an instance of the unpredictability of earthquakes. The central commercial centre was particularly hard hit, with a very high death toll, and the collapse of major buildings, despite a strict seismic building code. However, the frequency of earthquakes cannot be predicted with any degree of accuracy.

The magnitude of earthquakes is measured on the Richter scale, which gives a relative indication of the seismic energy released by an earthquake. The scale, from less than 3.5 to 8 or more, is explained in terms of the effects felt:

Earthquake severity:

Richter magnitudes	Earthquake effects
Less than 3.5	Generally not felt, but recorded.
3.5–5.4	Often felt, but rarely causes damage.
Under 6.0	At most slight damage to well-designed buildings. Can cause major damage to poorly constructed buildings over small regions.
6.1–6.9	Can be destructive in areas up to about 100 kilometres across where people live.

7.0–7.9	Major earthquake. Can cause serious damage over larger areas.
8 or greater	Large earthquake. Can cause serious damage in areas several hundred kilometres across.

Although each earthquake has a unique magnitude, its effects will vary greatly according to distance, ground conditions, construction standards and other factors.

Seismologists use a different scale, the Mercalli Intensity scale, to express the variable effects of an earthquake:

I. People do not feel any earth movement.

II. A few people might notice movement if they are at rest and/or on the upper floors of tall buildings.

III. Many people indoors feel movement. Hanging objects swing back and forth. People outdoors might not realize that an earthquake is occurring.

IV. Most people indoors feel movement. Hanging objects swing. Dishes, windows and doors rattle. The earthquake feels like a heavy truck hitting the walls. A few people outdoors may feel movement. Parked cars rock.

V. Almost everyone feels movement. Sleeping people are woken. Doors swing open or close. Dishes are broken. Pictures on the wall move. Small objects move or are turned over. Trees might shake. Liquids might spill out of open containers.

VI. Everyone feels movement. People have trouble walking. Objects fall from shelves. Pictures fall off walls. Furniture moves. Plaster in walls might crack. Trees and bushes shake. Damage is slight in poorly built buildings. No structural damage.

VII. People have difficulty standing. Drivers feel their cars shaking. Some furniture breaks. Loose bricks fall from buildings. Damage is slight to moderate in well-built buildings; considerable in poorly built buildings.

VIII. Drivers have trouble steering. Houses that are not bolted down might shift on their foundations. Tall structures such as towers and chimneys might twist and fall. Well-built buildings suffer slight damage. Poorly built structures suffer severe damage. Tree branches break. Hillsides might crack if the ground is wet. Water levels in wells might change.

IX. Well-built buildings suffer considerable damage. Houses that are not bolted down move off their foundations. Some underground pipes are broken. The ground cracks. Reservoirs suffer serious damage.

X. Most buildings and their foundations are destroyed. Some bridges are destroyed. Dams are seriously damaged. Large landslides occur. Water is thrown on the banks of canals, rivers and lakes. The ground cracks in large areas. Railroad tracks are bent slightly.

XI. Most buildings collapse. Some bridges are destroyed. Large cracks appear in the ground. Underground pipelines are destroyed. Railroad tracks are badly bent.

XII. Almost everything is destroyed. Objects are thrown into the air. The ground moves in waves or ripples. Large amounts of rock may move.

Source: FEMA

In a high-intensity earthquake, destruction is almost total and there is not much that can be done to rescue corporate documents, etc. The proper backing up of data in a remote unaffected location is the best defence against such an occurrence. However, in earthquakes of lesser severity, other precautions can help to mitigate the damage. The following steps are recommended:

1. Identify the most vulnerable equipment – computers on desktops, shelving.
2. Fasten computers to the underlying surface to avoid them crashing on to the floor or toppling in the case of towers. Fastening products, such as straps, are available on the market.
3. Servers should be secure in racks.
4. Racks and bookshelves should be fastened to walls to prevent damage or injuries to people.
5. Earthquakes can give rise to floods or fires and/or power failures. Elementary precautions should be taken to minimize damage from such occurrences.
6. Revise disaster recovery plans at regular intervals. Consider simultaneous, automatic or overnight backup.

Fire

One of the most damaging disasters, especially for SMEs, is fire. A survey undertaken a few years ago by the Norwich Union showed that some 70 per cent of single-site companies suffering a major fire incident were not in business 18 months after the event. Terry Simister, of the Heath Lambert insurance brokers group (one of the world's ten largest insurance and re-insurance groups, based in Hong Kong), confirmed that based on the survey result and his own experience, more than 50 per cent of small enterprises go out of business following destruction of their premises by fire. 'Unless a business has made adequate business continuity plans, it is highly unlikely that a single-site business will still be operating 18 months after a serious incidence,' he said.

He added that most large plcs now have business continuity plans, inspired in large measure by the Turnbull Report (UK) 1999 and corporate governance, but he estimated that for mid-sized companies, only 50 per cent have a plan, and most

small companies do not have any form of formalized plan. Most companies have thought about it but have not put in any plan due to lack of manpower.

Terry Simister said that in his experience, the greatest risks for small businesses are fire and loss of reputation, which in turn can lead to loss of customers. If a single-site business is struck by fire it will be destroyed unless a sprinkler system is in place. 'Unless the company has a consequential loss of business interruption policy, the business will suffer grievously. If your factory burns down, say, before Christmas, you not only lose the Christmas season business, you may also lose your customers in the longer term,' he warned. 'Losing premises is often worse for a small business than a large group, which is likely to have replacement facilities elsewhere.'

Floods

Floods and flash floods are a common form of disaster and can occur after heavy thunderstorms, continuous rain or in northern areas after winter snow thaws. Floods and flash floods have become more frequent in recent years, with many areas not previously affected hit by severe flooding. The force of floodwater can be dangerous. Six inches of moving water can sweep people off their feet; cars can be swept away in two feet of moving water. Floods can best be protected against by leaving the affected area or seeking higher ground.

As protection against damage to assets, flood insurance should be taken out. However, in flood-prone areas, such insurance is becoming expensive or difficult to obtain.

Extreme weather conditions

Hurricanes (classed as anything above force 10 on the Beaufort scale), tornados, storms, thunderstorms, hailstorms and other extreme weather conditions are all potentially disastrous events. Lighting strikes in particular can lead to power failure. A lightning flash can induce a surge of 7000 volts per metre in power and/or telephone cables, and 70 volts per metre a mile away. Lightning activity can induce a power surge of between 10 000 and 20 000 volts through the main power supply. The normal maximum is around 6000 volts.

POWER FAILURE

Since computer systems rely on mains supply electricity for their operation, power failures and voltage surges can cause severe disruptions, although power failures are no longer a big problem in the UK. When they do occur, they can cause data loss and downtime but do not usually cause equipment failure. In contrast,

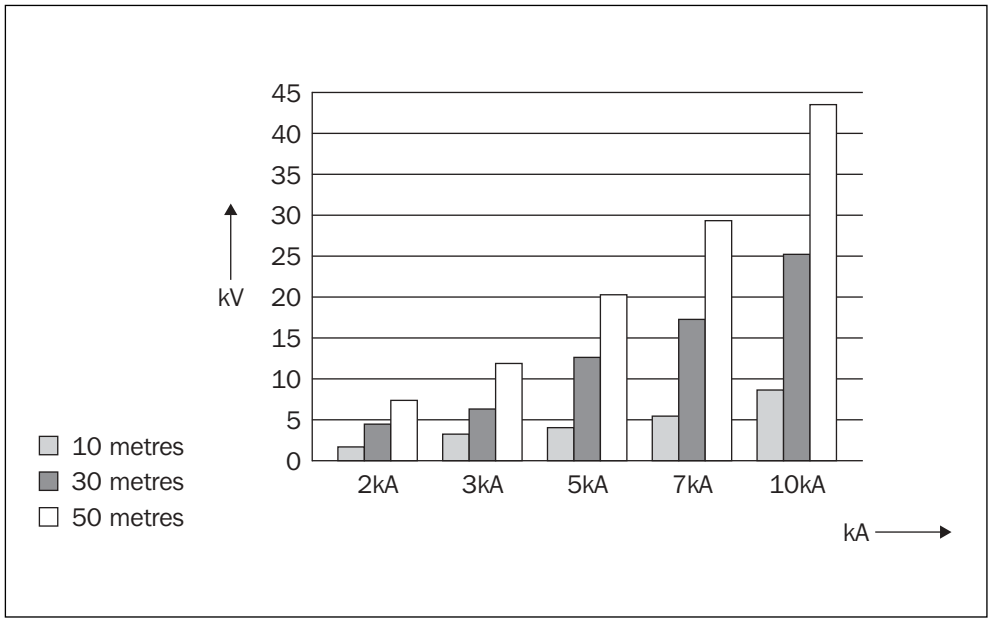
transient surges can cause equipment failure as well, from a soft fault to total failure. A UPS (uninterruptible power supply), although protecting the power supply to equipment, will not protect against transients and may itself be at risk.

A distinction should be made between power surges and transient surges. Power surges relate to an increase in the supply voltage above the usually allowed plus/minus 5 per cent. Such surges usually cause little damage to equipment and can be protected against with the inclusion of a UPS or a voltage stabilizer.

A power surge does not affect data/communication lines, but a transient, because of the large voltages and currents involved, can be induced anywhere along the lines. Modern electronic equipment is very susceptible to power failures and voltage surges. The UK's supply voltage is 240 Vac, whereas in the United States it is 110 Vac, i.e. a given piece of equipment will draw much higher current in the United States.

Transient surges involve much higher voltages of several thousand volts, but of short duration, i.e. a few microseconds (*see* Figure 1.1). Such surges have a much greater effect on equipment. Due to this potential damage, transient protection is more important than protection against power outages.

Fig. 1.1 **Transient surge with 10 microsecond rise time**



Source: Advance Galatrek, 2002

Transient voltage surges are often caused by the equipment installed in the companies themselves. Internally generated surges may not cause equipment failure, as they are of lower voltage. External transient surges, such as those caused by lightning strike, with a voltage surge of more than 20 000 volts going through the mains, can cause immediate and far-reaching equipment failure and

business disruption on a large scale. Voltage surges can be protected against with the right equipment, i.e. a surge suppressor that comes in different types.

Mick Burgoyne, Chief Engineer at power quality management specialist Advance-Galatrek, explains the phenomenon: 'It may seem surprising, but the majority of transient voltage surges are actually generated by an organization's own equipment. Research indicates that up to 80 per cent of voltage surges come from internal sources such as motors, fluorescent lights, photocopiers and other switching devices. Because modern mains-powered electronic equipment is highly susceptible to sudden voltage variations, this makes voltage surge suppression an essential part of an organization's power protection regime.

'The remaining 20 per cent of transients, generated externally, tend to receive more attention because they are more dramatic. However, it is important to distinguish between internally and externally generated voltage surges, because they will frequently have differing effects on electrical equipment.

'For example, because internally generated transients will normally be of a lower peak voltage, they will usually not cause immediate equipment failure. However, they will often cause cumulative damage, leading to premature failure. This, in turn, will result in data loss and corruption, with consequent downtime and increased costs. On the other hand, externally generated transients often result in very high peak voltages over a very short duration. Take, for example, a typical lightning strike, which can lead to a voltage surge of well over 20 000 volts being transmitted through the mains supply. Not surprisingly, this can cause instantaneous and catastrophic equipment failure, resulting in immediate operational shutdown and business disruption.

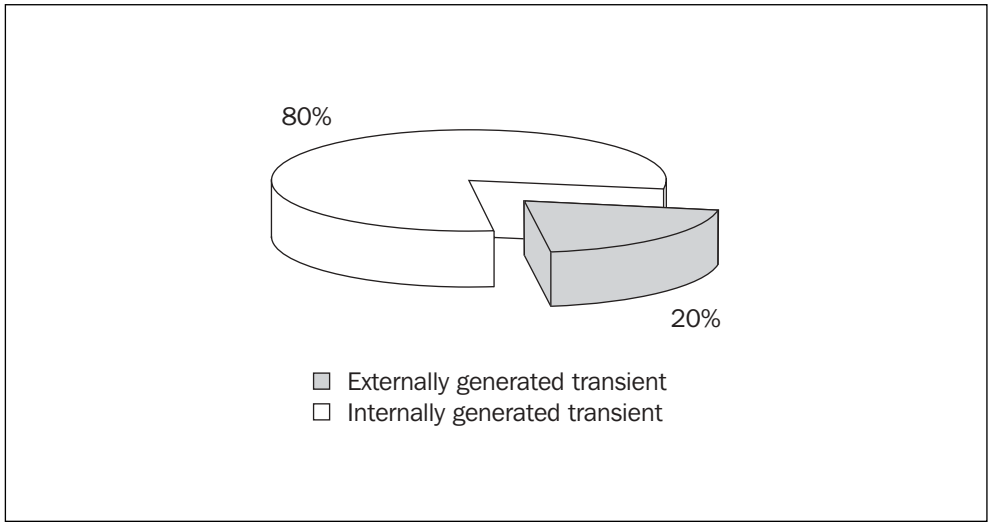
'In essence, a transient voltage surge suppressor (TVSS) is a component that limits the amount of energy arising from a transient and as a result protects electrical equipment from damage. However, although this definition is very straightforward, as with most things, the reality is rather more complex. In fact, it is always worth bearing in mind that the motive for adding a TVSS to an individual piece of equipment is not always to protect it, but may also be to protect the rest of the system from equipment known to produce transients.'

Mick Burgoyne presents the following summary schema:

- **Internally generated transients:** up to 80 per cent of transients are generated from internal sources (*see* Figure 1.2) such as inductive load switching and minor equipment operations causing:
  - cumulative damage
  - premature equipment failure (data losses, system resets and downtime).
- **Externally generated transients:** at least 20 per cent of transients are generated from external sources such as lightning and power company grid switching, possibly causing:

– catastrophic equipment failure
– immediate operation shutdown
– long-term disruption of business (expensive equipment repair and replacement costs).

Fig. 1.2 Transient surge generation



Source: Advance Galatrek, 2002

LIGHTNING

Lightning is a dramatic event, but in reality less damage is caused from lightning than transients generated internally or externally. The UK is less exposed to frequency and severity of lightning strikes than the US, where lightning strikes per square mile are far more frequent and severe. The same applies to hurricanes and tornados.

In summary, equipment and backup can be protected against power surges by the installation of UPS, since power surges do not as a general rule cause a lot of damage. In contrast, transient surges as the cause of problems continue to rise, affected by factors such as growing interconnectivity between networks. The financial effects can be devastating, due to hardware damage and costly systems downtime. The business continuity plan therefore predicates the ubiquitous use of UPS systems and wherever possible the protection of sensitive or valuable equipment and data by transient surge protection equipment. Companies supplying such equipment include Advance Galatrek which also offers, among other services, lightning and transient audits, mains power monitoring, maintenance plans and 'health checks' for clients' piece of mind.

ATTACKS CAUSED BY HUMAN INTERVENTION

Hackers

Computer attacks through hackers is a real threat to security. A March 2002 survey traced breaches of cybersecurity to Asia. The study, carried out by Predictive Systems, New York, found that the main source of attacks was from the US, but 91 per cent of attacks from outside the US were traceable to Pacific Rim countries, with South Korea counting for 34 per cent, China 29 per cent, Japan 10 per cent and Taiwan 7 per cent. The data were obtained from intrusion detection devices, which track incidents from hackers as well as work viruses. However, many attacks originate in the US and Eastern Europe and are sent via South Korea as the point of setting off the attacks.

Virus attacks

A virus is a piece of software which attaches itself to programs such as spreadsheets, and every time the program runs, the virus runs too.

E-mail viruses

With the spread of viruses via e-mail attachments, e-mail security has become an important issue. Computer viruses have led to billions of pounds worth of losses worldwide in terms of downtime, lost productivity and the cost of eliminating the virus.

The situation has been made worse through the explosion of e-mail traffic in recent years. Studies in the US show that two-thirds of the US workforce use e-mail. Traffic is between a company's clients, suppliers, buyers and others, as well as internal messages. E-mail traffic is further enhanced by the vast number of unsolicited e-mails (spams) sent out. A common way of transmitting viruses is via an e-mail attachment, and users may be unaware of the presence of a virus until they open an attachment.

Like hurricanes, viruses are given names. Melissa wrought havoc in 1999 when it forced Microsoft to shut down its e-mail system. The virus multiplied itself every time it was triggered by sending itself to 50 other e-mail addresses, as well as corrupting a central file, which meant that any file subsequently saved would also contain the virus. It was the fastest spreading virus ever.

Similarly, the 'I love you' virus had a devastating effect. It consisted of a piece of code in an attachment. Whenever an attachment was opened, the code sent copies of the virus to every address in the recipient's address book and also corrupted files on the recipient's machine.

Worms

A different type of virus is the worm, which replicates itself by using computer networks and security loopholes. From the original machine, the worm starts scanning the network, and once it has found a security loophole, it copies itself to the machine and starts replicating. One of the most famous worms was Code Red, which appeared in 2001 and managed to replicate itself 350 000 times in nine hours. The worm attacked Microsoft Windows NT 4 and Windows 2000 servers running Microsoft IIS 4.0 or IIS 5.0. Experts believed its effects would shut down the entire Internet. However, although the Internet was slowed down, the effect was not as severe as had been expected. A patch issued by Microsoft fixes the security loopholes on the system. If the worm finds a server without the security patch, it will copy itself to the server and the new copy will do likewise.

Trojan horses

A Trojan horse is a computer program which pretends to be what it is not, e.g. a game, and when it is run, it will do damage such as erasing data on the hard disk. Trojan horses do not replicate automatically.

VULNERABILITY TO MALICIOUS ATTACKS

The increase in the incidence and propagation of attacks in recent years can be ascribed to a number of factors.

- **Automation of attacks.** Scanning for potential victims has increased during the past five years. Advanced scanning techniques are used for maximum impact.
- **Speed of attack.** The vulnerability of systems was previously exposed through scanning. However, new techniques make it possible to attack the vulnerable systems during the scanning, leading to an increase in the speed of the attack. The discovery by intruders of weaknesses in software has also become more effective and such vulnerabilities may be discovered before patches have been issued or adopted.
- **Self-propagation.** The triggering of attacks required human intervention before 2000. Today, however, attack tools will self-propagate more attacks (e.g. Code Red). Attack tools can also be co-ordinated and distributed more effectively.
- **Advanced software.** The developers of methods of attack also have at their disposal more advanced software, and the originators of attacks are more difficult to detect.

- **Firewalls.** The widespread use of firewalls as a method of protection has come up against further developments in technologies designed to bypass typical configurations. Firewalls are therefore becoming increasingly vulnerable to attack.
- **Infrastructure attacks.** Attacks affecting key components of the Internet are becoming increasingly common. Such attacks include worms and self-propagating codes. Due to their high level of automation, they can attack a large number of systems within hours.

A special category of attacks, denial of service, denies service to users. Attackers can also hijack top-level domains through attacks on the domain name system, or the attackers may modify data on DNS (domain name system) servers. Attacks on top-level domain servers can cause the Internet to slow down. Attackers can also modify the data on vulnerable servers.

Attacks may be directed against the routers in a network if they are not properly secured, for instance by overwhelming them with incoming traffic.

Human error

Human error is a frequent cause of computer breakdown. When human error occurs, experts investigate not only the state of the person responsible for the incident, his training, negligence, etc. but also the system itself, particularly the design of the interface, which may not have been sufficiently 'user-friendly' or may not come up to the standards expected.

Human error can be simply accidental deletion of files or trauma caused by dropping a computer. It was human error that caused the loss of a satellite on its way to Mars when a wrong code triggered the wrong response. Human error is widespread across industries.

As far as backup is concerned, human inertia rather than human error is often to blame for the failure to back up systems properly and on time. This in turn can be traced back to lack of control from senior management, or inadequate procedures.

SYSTEMS FAILURES, DISRUPTIONS

Systems failures/disruptions are extremely common and account for up to 60 per cent of failures in IT systems. The failure of printers in the air traffic control system in the UK installed in April 2002 caused several hours' delays to incoming and outbound flights. Frequently, companies when contacted over the telephone report that 'their systems are down' and that they cannot therefore deal with enquiries. Many firms cover for such eventualities by calling in IT experts under maintenance

and/or service contracts to fix the problem in record time. Examples of failures include software corruption, configuration complexities and failed backup.

EFFECTS OF DISASTERS

Water damage

Water-damaged structural components and electronic equipment can sometimes be saved by drying instead of needing to be replaced. This can save up to 70 per cent of reconstruction costs and reconstruction time and retraining on new equipment. Effective drying requires an immediate response. By adjusting humidity and temperature levels, water damage can be temporarily halted. For this purpose professional dehumidifying equipment is needed, supplied by disaster recovery specialists such as Belfor. By surrounding the wet areas with dehumidifying air, the air extracts moisture from the water-affected object to evaporate. Through daily monitoring with special equipment, the return to normal of the water-exposed objects can be measured.

Water is a conductor of electricity, and a company affected by water damage should initially ensure that all power supplies are switched off. Electronic equipment should be removed from the electricity supply. The water should be removed as far as is possible and equipment placed in dry surroundings. Seawater has a corrosive effect and should be washed off affected metal surfaces as soon as possible.

Fire and smoke

Fire is destructive due to high temperatures and can also create dangerous chemical reactions leading to explosions or corrosive surface agents. The combustion of PVC, for instance, causes corrosion of metal surfaces and releases hydrochloric acid, which in turn will contaminate the atmosphere. The humidity generated from fire extinguishing can also cause corrosion of certain surfaces.

Carbon deposits can cause damage to electronic equipment if not removed. However, contaminated equipment is often restorable, depending on the length of the fire and the temperatures to which it has been exposed. Smoke contamination can travel far through a modern building, conducted through air conditioning systems, cable ducts and maintenance service conduits, as well as ceiling and floor cavities.

Dust

Dust can arise for a number of reasons, from construction sites with inadequate dust emission control to dust storms, etc. Dust in computer equipment and other

electronic components may cause power shortages which in turn may result in cable burns.

Dust needs to be combated on an immediate basis, to protect against further damage. Dust should be removed and exposed machine and equipment disassembled to clean them properly.

Explosions

In case of an explosion, whether caused accidentally, by detonation or by criminal activity, experts called in will assess and attempt to stabilize the damage immediately, limit further secondary damage and remove the effects of the explosion, such as extinguishing fire, removal of dust, water and other materials causing contamination.

FIRST LINE OF DISASTER RECOVERY

In case of a disaster, as part of the disaster recovery plan (if any) first-line disaster recovery specialists such as Belfor should be called to the scene to deal with the damage in general, as well as to specially protect and restore electronic equipment.

CONCLUSION

The threats to IT systems and backup are many and unpredictable, and data losses are on the increase, despite advances in the reliability and sophistication of storage devices and the availability of security and anti-virus software. Added to this, more mission-critical information than ever is now stored on computers rather than other media. With advances in technology, the virulence of attacks is on the increase and 100 per cent reliance on even the most advanced backup system is not always sufficient to recover data. In the fight against natural disasters and attacks caused by humans, backup and recovery solutions, together with defensive strategies, should be kept under constant review to ensure the best protection of data at all times.

2

Corporate state of readiness

INTRODUCTION

Is your company prepared if a disaster occurs? The risks to your business of losing valuable data could be catastrophic. In the past, there has been a tendency for companies if not exactly to throw precaution to the winds, at least to give preparations for disasters a low priority at the expense of more instantly gratifying activities such as pursuing new business opportunities. Drawing up disaster recovery plans and contingency plans does not have an immediate effect on the share price in the same way as a successfully concluded contract. However, there are signs that businesses are waking up to the importance of being prepared for disaster to strike and of being able to preserve mission-critical data if exposed to attack. There is a growing realization that corporate survival, although a long-term goal, could suddenly take on a new dimension, against which it is best to be prepared.

Stumbling blocks

Research findings give cause for concern. Terry Simister, of the Heath Lambert insurance brokers group, estimates that more than 60 per cent of all small businesses do not have a disaster recovery plan. He points out that too many directors look at the issues involved for the first time after a disaster has occurred. In other reported cases, when disaster strikes, managers cannot find the disaster recovery plan that has been carefully prepared but then assigned to oblivion. The need for speed after a disaster is paramount, to ensure that no further time is lost in restoring data and operations.

One aspect of disaster recovery, which came to the fore with September 11, is the availability of people and the logistics of moving them around. When the WTC towers collapsed in New York, those who got out of the buildings were unable to relocate to other areas since not only Ground Zero but also the surrounding area had been shut down.

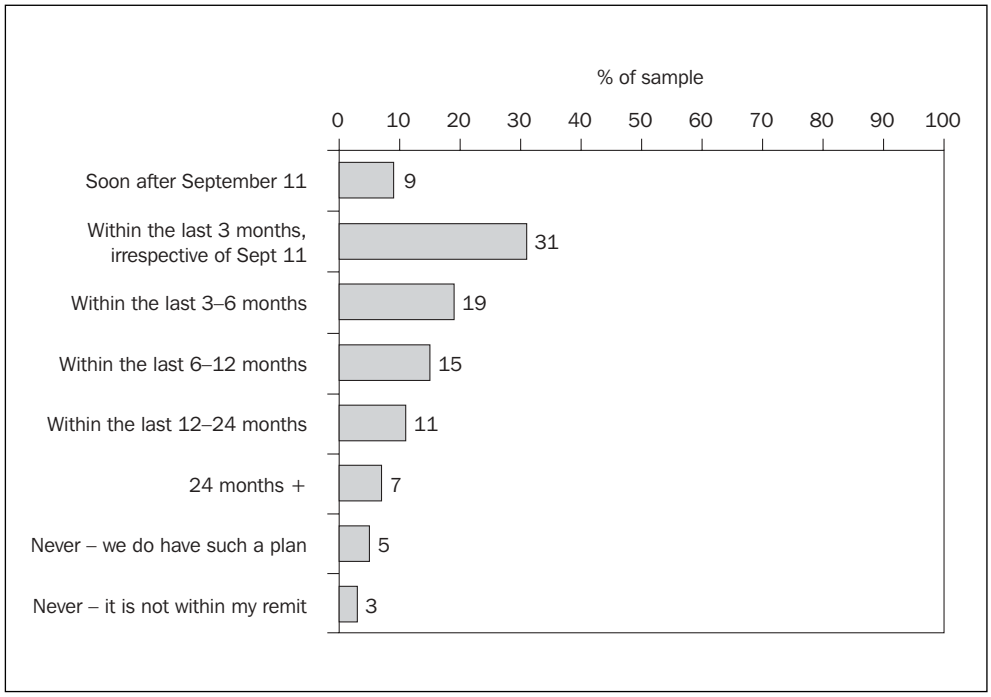
As it happened, the Internet did not go down during and after the catastrophe and those with laptops were able to continue with some business activities either when they eventually got back home or by plugging into the net from other venues such as Internet cafes.

RECENT SURVEY

Following September 11, disaster recovery is creeping to the top of boardroom agendas. In a 2001 survey of 100 IT decision makers in UK businesses, carried out by Dynamic Markets on behalf of CMG (a European IT services group), the results showed that only 9 per cent reviewed their disaster recovery plans immediately following the WTC attacks in 2001. But the great majority did keep their finger on

the disaster recovery pulse – 31 per cent said that they had reviewed their plans within the last three months (to December 31), irrespective of September 11, and 19 per cent said plans had been reviewed within the last 3–6 months. Only 5 per cent admitted to not having a plan, and another 3 per cent did not review their plans for other reasons (*see* Figure 2.1). Despite the losses, spending on security as a percentage of total IT budget spend was low at around 1 per cent.

Fig. 2.1 **Response to the question: When did you last review your organization's disaster recovery plan?**

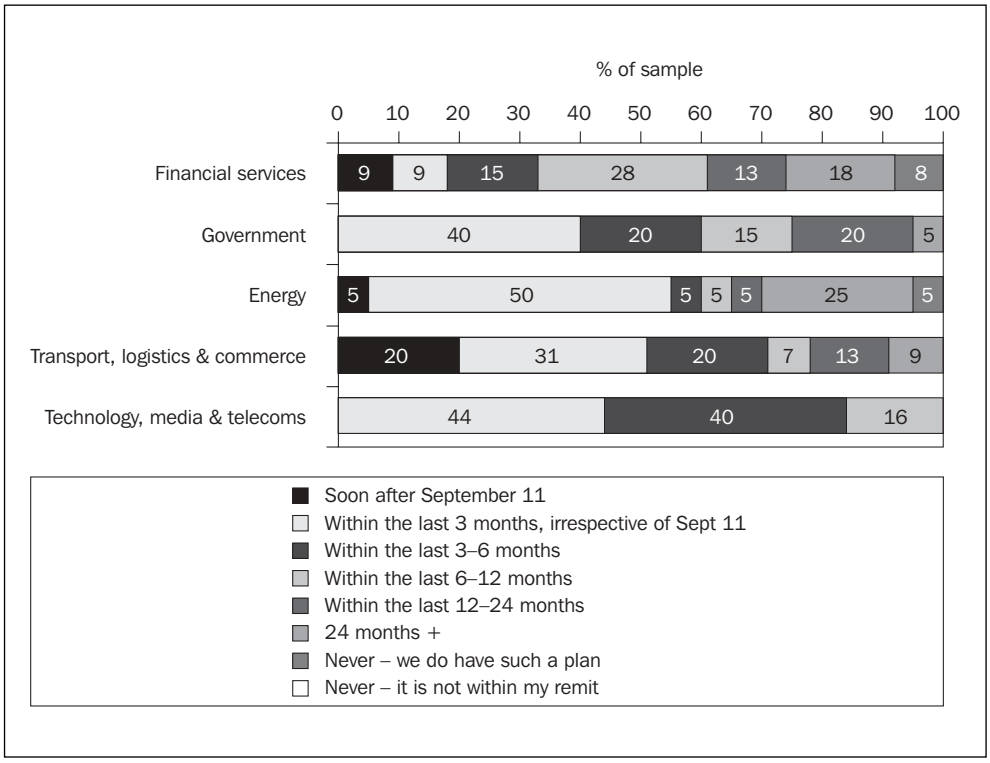


Source: CMG, Dynamic Markets, December 2001

Figure 2.2 shows that there was some sector variation in companies' reviews of plans. As would perhaps be expected, financial services, particularly hard hit in the WTC attacks, showed a higher percentage reviewing their plans immediately after the tragedy (9 per cent), together with transport, logistics and commerce (20 per cent). In energy, 55 per cent of the sample had reviewed their plans within the last three months, followed by transport, logistics and commerce (51 per cent) and technology, media and telecoms (44 per cent). Government organizations also fared well, with 40 per cent revising their plans within the last three months of the survey.

CMG UK Chairman Geoff Neville called for greater awareness on the part of companies: 'Nobody wants to think about the impact of a terrorist attack on their organization, but they can at least be prepared for the worst. Having the ability to work from a remote location is a step in the right direction. But it is no good unless overall business continuity plans are also in place.'

Fig. 2.2 Sector variation in companies' reviews of disaster recovery plans



Source: CMG, Dynamic Markets, 2002

Training was a big part of the problem. 'Our research found that more than a third (37 per cent) of IT decision makers have never had any training in risk management or disaster recovery planning. This may be why it does not sit high enough on the IT agenda. Unfortunately, it is an area that most businesses cannot really continue to neglect.'

Coping with recessionary trends

The recessionary trends had an effect on IT budgets, but none of the companies surveyed had reduced their budgets by more than a third, 50 per cent of budgets had not been cut, and 31 per cent had increased their budgets during the period August–December 2001.

Respondents were asked what business skills they thought were most important in the company in times of recession, and 82 per cent replied 'technical know-how', by far the largest group. The effect of recession on buying behaviour was also analyzed. There was a tendency to take more time over decisions. A minority turned to independent third parties for advice and 11 per cent chose outsourcing rather than direct buying as a prudent alternative.

HOW TO COPE WITH ECONOMIC FLUCTUATIONS

At a briefing organized by Compaq in 2002, senior executives warned against the cycle of boom and bust, which tended to accompany the slowing of business. The company had the following 'top ten cycle-busting tips' for IT decision makers:

1. Conduct an audit on your IT capabilities – you might be surprised to discover how much capacity you have on offer.
2. Before you commit money to IT, make sure that you know what the risks are as well as the returns.
3. Consider innovative business models, such as next-generation outsourcing, as well as innovative technologies, to keep costs low.
4. Make sure all the more ambitious IT projects are justified in cost, competitiveness and credibility terms.
5. Get the board into the habit of thinking of IT projects over a whole economic cycle rather than just in the short term.
6. Get the whole organization behind IT thrift, incentivize people to come up with cost-savings ideas, e.g. how to cut storage needs for e-mail.
7. Set your sights on the future and plan for it now. Don't let yourself get into the mindset of thinking only one quarter at a time, as it will leave you weaker in the long term.
8. Make sure that you get board-level commitment to your strategy and that they stick to it when times get tough.
9. Stay on top of your IT budgets – know where every penny is being spent.
10. Do not wait for infrastructure cuts to be imposed on you or your department. Continually look at cost saving over time.

MCKINSEY FINDINGS

The state of readiness of US companies hit by the terrorist attacks on September 11 was better than at first expected, but subsequent studies found that recovery sites were not necessarily located in positions where people could reach them. McKinsey pointed to insufficient access to backup sites, not enough geographical diversity in backup plans, and the existence of key 'choke-points'. Some disaster recovery plans did not include alternative backup facilities or refer to any transport problems that might arise in connection with a disaster, not to mention alternative infrastructure and power systems.

DATA AVAILABILITY

A survey in 2001 from MacArthurStroud International of 450 users in France, Germany and the UK found that a majority of users needed data availability 7×24 within the data centre, and just over one-third had a requirement for 7×24 data to be available outside the data centre. The survey showed that virtually all users had tape storage within the data centre for primary and secondary backup, and recommended 'better understanding of the disciplines of managing storage and building confidence in the technologies available to build better service. The capabilities of the storage management tools need to be highlighted. Building on backup processes, the disciplines need to deliver the features of securing and sharing data across the enterprise and multiple system platforms.'

FACTORS AFFECTING CORPORATE STATE OF READINESS

The ability to cope with disaster as far as backup is concerned is affected by a variety of factors, including:

- ineffective backup systems
- outmoded backup solutions
- failure to back up
- lack of sufficient or trained manpower
- lack of reserve-trained manpower for overcoming disasters (remotely located and/or working from home)
- conflicting or unco-ordinated backup systems (PCs, main systems)
- PCs: no backup system.

PRECAUTIONARY STEPS

Some of the steps that should be taken to prepare for any of the above events are listed below. Backup systems should be updated regularly to ensure that they work as intended and that the latest technology affordable is available. This ensures higher availability of data through faster restoration rates.

Checks should be made to ensure that employees are on top of their backup activities – loose control may cause a slippage in backup and backlogs develop. The quality of the backup should also be monitored. If there is a lack of trained

personnel for the backup, the right procedures may not be followed and in the worst cases the backup tapes/disks may be blank.

What is the procedure for restoration of backup in the event of disasters? In the case of September 11, employees were decimated. This led to calls for reserve-trained manpower to assist or take over in case of future disasters. More people should be trained to be able to work from home or a greater percentage of the workforce should be remotely located to minimize the risk of losing key people.

Are the backup systems sufficiently removed from the main processing centres? In the September 11 attacks, one company had its main processing plant in one tower and its backup in the next. Other companies failed to reach their remote backup facilities since their employees were unable to leave Lower Manhattan because transport facilities were shut down.

Backup systems may have been installed on an ad hoc basis and may not be synchronized. In many organizations, PCs are outside the main backup system or are unco-ordinated with the main systems. In companies with many geographical locations, systems in one location may not be compatible with systems in another. The systems should be designed to cater for the backup requirements of the entire organization, with matching systems being available in different divisions/ geographical locations.

MOBILE PHONES PROVE THEIR WORTH

On September 11, mobile phones proved to be an effective means of communication, and many companies are revising their policies and issuing mobile phones to employees to enable them to cope with emergencies as well as day-to-day communications.

Mobile recovery services

For those who are not ready for the moment disaster strikes, mobile recovery services are available in various forms. If, for instance, restoration to normal business operations involves local access to systems but with no suitable accommodation, a mobile recovery unit may be the solution. Such a unit is a complete data centre and end-user recovery service, which provides not only physical space but the entire infrastructure required to restore critical business functions. Units are fully prewired for data and telecommunications, generators, desktop PCs, furniture and other features.

Fixed recovery centres are also available, such as those operated by Compaq. The centres offer computer rooms, hardware and network facilities as well as IT staff.

CONCLUSION

Whilst companies' state of readiness is not 100 per cent, there has been much improvement in recent years. September 11 found a high level of readiness to cope with disaster among affected companies. Surveys also confirm that companies are in a higher state of alert when it comes to disasters than they were a few years ago. Whilst recessionary influences have an effect on companies' ability and preparedness to invest in IT systems, backup and storage expenditure is not the first item to be slashed. Rather it tends to be given priority, due to the importance of maintaining access to critical data in adverse circumstances.

3

Information security

INTRODUCTION

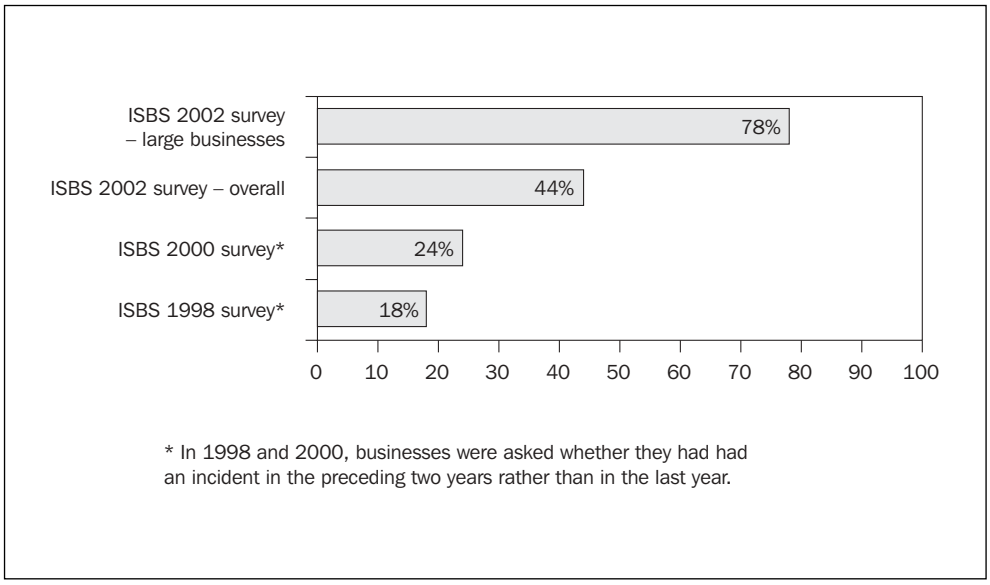
To secure IT systems and backup against risks, an information security policy consisting of a combination of control procedures and technological applications (e.g. privacy and security software) should be in place. Below is a summary of the results of a Department of Trade and Industry (DTI) survey sponsored by PricewaterhouseCoopers and others into information security in UK firms, as well as some of the results from a previous DTI survey (2000), together with an outline of the basic protective measures an organization can take to prevent unauthorized access, corruption of data or loss of information.

DTI SURVEYS

A vital part of protecting IT systems from disasters is information security. The DTI survey 'Information Security Breaches Survey 2000' (ISBS) analyzed information security issues in 1000 British companies of varying sizes. A follow-up survey was published in April 2002. The main findings of the two surveys are as follows.

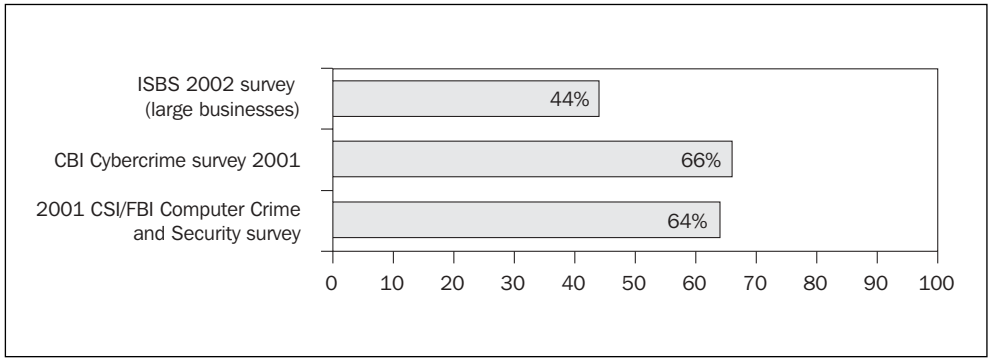
The 2002 survey results showed that 78 per cent of large businesses in the sample had suffered security breaches from premeditated or malicious attacks. The figure for all respondents was 44 per cent, up from 24 per cent in the 2000 survey. Twenty per cent said the breaches were 'extremely serious'. (*See* Figures 3.1 and 3.2.)

Fig. 3.1 **What proportion of UK businesses have suffered security incidents (arising from premeditated or malicious intent) in the last year?**



Source: DTI, Information Security Breaches Survey, 2002

Fig. 3.2 **What proportion of UK businesses have suffered a serious security incident in the last year?**

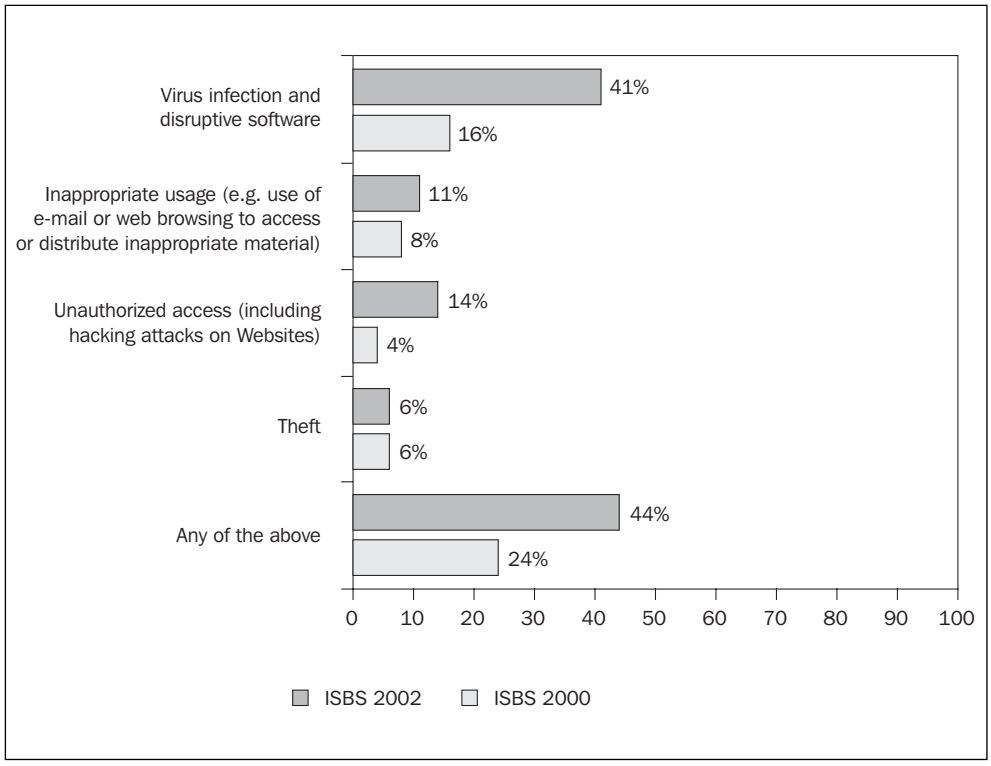


Source: DTI, Information Security Breaches Survey, 2002

Contrary to widespread beliefs, most security breaches in the sample were caused by external sources (66 per cent). This is consistent with results from other surveys abroad.

Most breaches were caused by viruses (up from 16 per cent in the 2000 survey to 41 per cent in the 2002 survey – *see* Figure 3.3). Unauthorized access (mainly hackers) rose from 4 per cent in 2000 to 14 per cent in 2002. The most serious breaches were caused by viruses (33 per cent of respondents).

Fig. 3.3 **What proportion of UK businesses have suffered security incidents in the last 12 months?**



Source: DTI, Information Security Breaches Survey, 2002

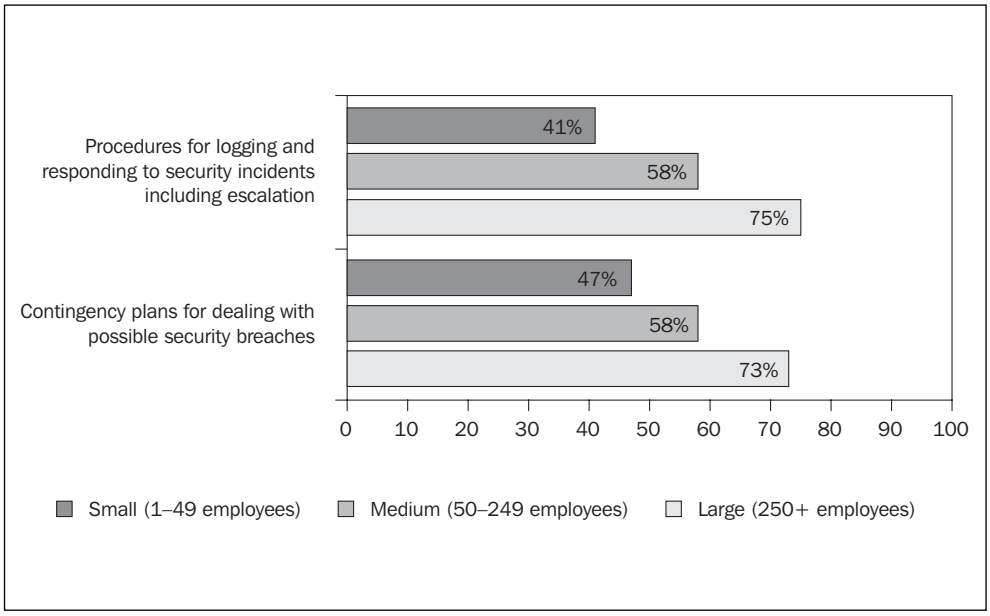
Security policy

In the 2000 survey only 14 per cent of respondents had a specific information security policy, but of those that had, 54 per cent had a formal document and 38 per cent made new staff aware of the policy on joining. Fifty seven per cent of staff received some form of training, either by line managers and colleagues or by specialists. Of the 14 per cent, 75 per cent reported that policy was a matter for board review, but the remainder responded that the policy was reviewed below board level.

In the 2002 survey, the situation had improved, with 27 per cent of companies having an information security policy, while 76 per cent of respondents who had a policy undertook a regular review of their security policy (2000: 68 per cent). A detailed risk assessment had been carried out by 66 per cent of respondents, compared with 37 per cent in 2000.

A fairly high percentage of companies had incident response procedures in place. The results are illustrated in Figure 3.4 which shows that smaller companies were much less likely than larger companies to have in place procedures such as logging in and having contingency plans.

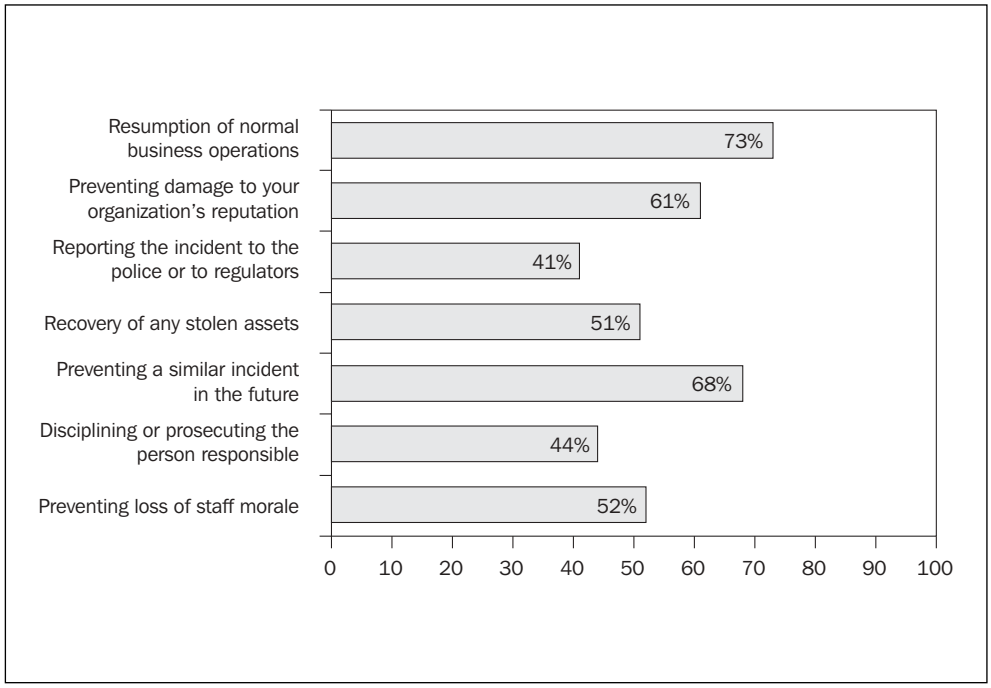
Fig. 3.4 **What proportion of UK businesses have incident response procedures in place?**



Source: DTI, Information Security Breaches Survey, 2002

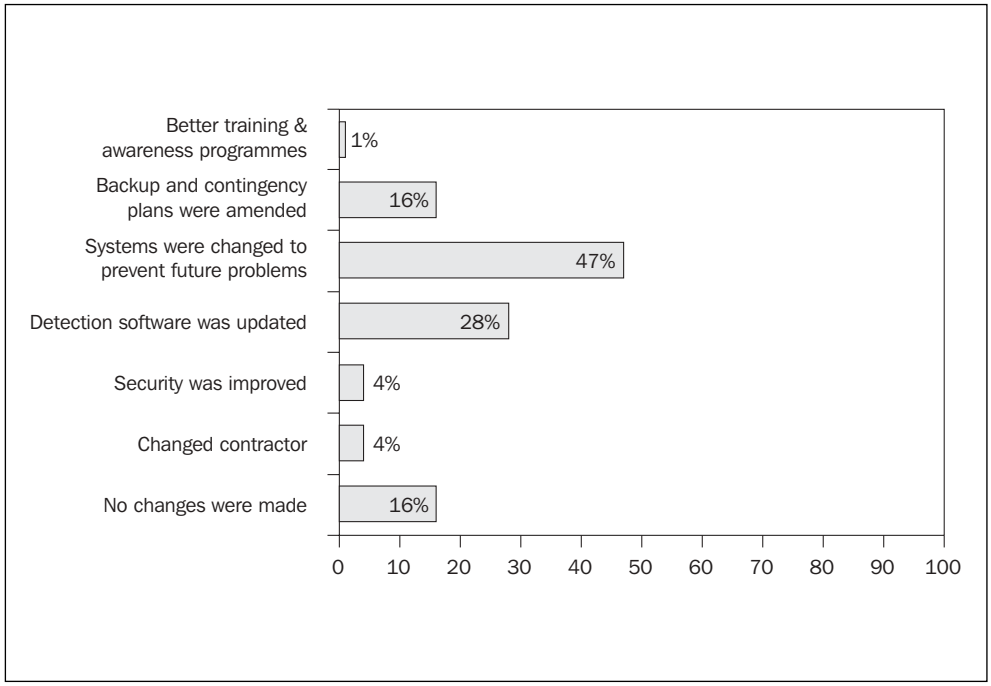
In the event of a security breach, the objectives listed in Figure 3.5 were 'very important' to companies in the sample. Resumption of normal business operations came top of the largest group of companies. The changes that were made to prevent future incidents in case of a security breach are shown in Figure 3.6.

Fig. 3.5 **Which of the following objectives are very important to UK businesses in the event of a security incident?**



Source: DTI, Information Security Breaches Survey, 2002

Fig. 3.6 **After the security breach, what changes were made to prevent future incidents?**



Source: DTI, Information Security Breaches Survey, 2002

Use of technology as security measures

The 2000 survey found that use of passwords was the most common protective measure. In large organizations, all companies made use of passwords, whereas in smaller companies it was less common – 68 per cent of companies with less than nine employees used passwords. Overall, 75 per cent of the companies surveyed had passwords installed. The 2002 survey results were not directly comparable.

Of the organizations in the 2000 survey, 75 per cent had anti-virus protection. However, again smaller organizations came out worst – of companies with less than nine employees, 32 per cent did not have virus protection. Table 3.1 shows the percentage of companies using technology.

Table 3.1 The percentage of companies using technology

Technology	*Percentage*
Passwords	75
Other login devices	5
Virus control	75
Firewalls	15
Website protection	16
Data encryption	8
DMZ	1

Source: DTI Survey 2000

Companies had various reasons for wanting to avoid the loss of critical data or interruption of sensitive information flow. The two most common reasons were that such events would be 'of benefit to customers' or lead to 'loss of customer confidence', followed by 'lack of staff confidence'. However, 31 per cent of organizations, mainly small in size, claimed that they did not possess any sensitive information. Of those that did, 43 per cent had suffered an 'extremely serious' breach of security and another 20 per cent had suffered a 'moderately serious' breach in the past two years.

Procedures for dealing with viruses included detection on all systems, regular virus updates, e-mail scanning software, Internet scanning software, regular checking facilities, user awareness program, and management procedures for reporting and recovering from viruses.

Access to the Internet varied with organizational size, but overall 70 per cent of companies allowed their employees some form of access. In the larger organizations in particular, access tended to be restricted to certain areas.

The DTI outlines three important steps in practising an information management security system:

- Definition of the aims and objectives of information security. A policy that has the commitment of senior management.
- Assessment of the security risks. A policy that is grounded on an assessment process. A process that considers the value of the information and other assets at risk and balances this against the spending on security controls. A process that reviews the risks periodically to take account of changing circumstances and new risks.
- Selection and implementation of controls.

Reasons for implementing an information security policy included good business practice, meeting legal requirements, reassurance for customers and making staff more aware of their obligations (checking, testing).

After a serious incident, the 2002 survey showed that most businesses made changes to prevent incidents occurring in the future – 42 per cent changed their systems, 28 per cent updated their detection software and 16 per cent amended their backup and contingency plans. However, 16 per cent did not make any changes. After the security breach, 53 per cent of respondents were able to restore business within an hour.

Most companies did not report security breaches to the authorities. Only 16 per cent took legal action – 52 per cent of respondents thought the incident was not serious enough to pursue legal avenues, 20 per cent said no laws were broken and 4 per cent did not want bad publicity. A small percentage did not know who to take legal action against.

PROTECTIVE MEASURES

The top ten actions recommended by the DTI for a board of directors to take to improve security are:

- Create a security-aware culture by educating staff about security risks and their responsibilities.
- Have a clear, up-to-date security policy to facilitate communication with staff and business partners.
- Have people responsible for security with the right knowledge of good practice (e.g. BS 7799) and the latest security threats. Consider supplementing their skills through external security experts.
- Evaluate return on investment on IT security expenditure.

- Build security requirements into the design of IT systems and outsourcing arrangements.
- Keep technical security defences (e.g. anti-virus software) up to date in the light of the latest threats.
- Have procedures to ensure compliance with data protection and other regulatory requirements.
- Have contingency plans for dealing with a serious information security breach.
- Understand the status of your insurance cover against damage as a result of information security breaches.
- Test compliance with your security policy (e.g. security audits, penetration testing of the company's Website).

Most important of all, do not wait for a serious security incident to affect your business before you take action.

GENERAL CONTROL PROCEDURES

Protection of software and hardware assets is part of a risk assessment and an inventory of assets should be made. Software is subject to licensing laws imposing obligations on users. Both hardware and software could be the subject of theft. Software is intellectual property and should not be copied. It should not be removed from the IT location without authorization. If equipment leaves the office, it should be checked out and checked back in when it returns. Illegal software should be deleted from computers in use. Random checks should be made to ensure that software and hardware are in place.

Elementary precautions such as locking up backup tapes and sensitive disks/CD-ROMS should be part of the control procedures. Risks such as fire and floods should be considered. Controls should also be carried out vis-à-vis staff to ensure that procedures are adhered to. Unauthorized access to IT systems should be prevented by using a password-protected screen saver, especially for equipment which is left running and unattended during office hours or after work.

Authentication

Authentication of users provides a measure of security against intruders. User authentication is a method of identifying the user of the services of a Website. Message authentication intercepts and detects changes in the text of a message. Examples are electronic signatures. Authentication is typically used in sensitive information transfers, such as transfer of funds. The DTI survey 2002 found that

72 per cent of businesses required some form of authentication such as passwords for electronic data processing or e-procurement. Digital certificates or PKI (Public Key Infrastructure) were used by 40 per cent of large organizations (28 per cent of the total sample).

Methods of authentication include personal identification numbers (PINs) or passwords, electronic keys or biometrics (retina, iris or palm scan). Methods of retina identification involve the blood vessel patterns on the retina or the pattern of flecks on the iris. Retina identification is currently the most promising method. According to the DTI survey, retina identification is being used for high-security control at military establishments and banks. Only 3 per cent of large businesses use biometrics. A wider field trial on biometrics as a method of authentication is being carried out at a London airport at the instigation of the UK authorities. The intention is to incorporate iris prints and fingerprints into entitlement cards which will have to be presented in future if the holders are to receive NHS services, unemployment benefits, etc. Initially, the government intends that such ID will be voluntary, but inevitably this gentle approach will lead to biometric ID cards becoming ubiquitous and probably compulsory.

Encryption

Encryption converts a readable message into a coded one through algorithms. The message can be converted back into readable text (decrypted) by those who have an encryption key. Encryption is highly successful in preventing unauthorized access and increasing the security of the transmission of business-critical information. Encryption can also be applied to data storage. The level of encryption necessary should be assessed according to the degree of sensitivity of the information. The level of encryption can be sufficient to ensure corporate confidentiality, but governments put a limit on the extent to which encryption can be utilized so that they can effectively use high-powered super computers to decrypt communications, should they deem this in the best interest of national security, or combating crime, etc. The DTI survey 2002 found that 35 per cent of UK respondents providing employees with e-mail access had encryption procedures in place (large organizations: 48 per cent).

Firewalls

Firewalls provide security against unwanted intrusion. They come in varying degrees of sophistication. High-end firewall solutions made by suppliers such as Symantec, a world leader in security technology, will protect gateways and servers in local and remote systems against viruses and other intrusions. Another vendor,

Cisco Systems, provides firewalls ranging from plug-n-play desktop firewalls for personal or small office use to gigabit firewalls for large corporations.

Shelters

Security measures to protect whole IT systems and backup-and-restore facilities include the building of bombproof shelters and 'strong rooms' which are fire protected and air-conditioned. Such facilities are typically provided by server farms/colocation centres. Some of these are former cold war bombproof shelters and command centres. In the US, customs buildings have been designed to resist earthquakes, fire, hurricanes and other natural disasters, as well as creating an environment that is totally secured against unauthorized entry through sophisticated access control.

CONCLUSION

Statistics show the varying level of risks associated with different types of attack, with external attacks ranking high in frequency, if not necessarily in severity. But whatever the form of attack, an important weapon in ensuring the retention of backup data and mission-critical information, and consequent limitation of losses, is a thorough risk assessment of IT systems leading to a knowledge of the inherent risks associated with various types of attack, as well as implementing access control and other measures to protect systems as a first line of defence.

4

Corporate disaster recovery/ business continuity plans

INTRODUCTION

Disaster recovery strategies centre around three phases: the preparatory phase, during which details of the plan are drawn up and tests and drills carried out, the actual incident or catastrophic event, and the recovery phase, during which action is taken to resume normal business operations. To prepare for this sequence of events, two systematic approaches have been developed: the disaster recovery plan and the business continuity plan.

DEFINITIONS

The disciplines of disaster recovery (DR) and business continuity, embracing business continuity management (BCM) and business continuity (also referred to as business continuance) planning, suffer from lack of definitions and unanimity of terms. Not only are the individual terms interpreted differently from one practitioner to another, there is some overlap between the two, and in some cases managers who think they are practising business continuity management are in fact focusing on disaster recovery. Global Continuity plc, an international provider of continuous business processing solutions, has now taken the initiative of setting up a group of experts drawn from DR and BCM the world over, with a view to working out between them a glossary of terms that can be universally applied and understood. The group is being set up via e-mail and at the time of writing numbered almost 100 members.

Current definitions of business continuity vary. Global Continuity uses 'The proactive management of a business or organization to ensure maximum continuity of operations on a day-to-day basis'. The Business Continuity Institute's (BCI) definition runs as follows: 'A proactive process which identifies the key functions of an organization and the likely threats to those functions. From this, information plans and procedures can be developed which ensure that key functions can continue whatever the circumstances.' Essentially, the two definitions have the same emphasis, although the BCI definition is slightly more elaborate.

Other relevant definitions used by The Business Continuity Institute are as follows:

- Business continuity plan: a collection of procedures and information, which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster. (Associated terms: business recovery plan, disaster recovery plan, recovery plan.)
- Business continuity management: those management disciplines, processes and techniques which seek to provide the means for continuous operation of the essential business functions under all circumstances.

Tim Cousins of Tim Cousins & Associates Pty Ltd, Australia, juxtaposes the two definitions used by his company:

- Disaster recovery: the process of preparing for, responding to and recovering from an unplanned interruption in normal business operations for a specific business function; typically the information technology function.
- Business continuity: the co-ordination of key business functions within a company in its preparation, response and subsequent recovery from an unplanned interruption in normal business operations.

With the emphasis shifting towards business continuity rather than the narrower concept of disaster recovery, more and more management disciplines are getting involved. Business impact assessments, emergency management, emergency response, risk management, crisis management, training, testing, safety drills and contingency planning are all concentrating on business continuity in one form or another. Examples of jobs involved in business continuity planning include business continuity planner, emergency planner, disaster recovery manager, information protection manager, risk management manager and others.

John Starling, Senior Manager, Business IT Strategy and Financial Services, Deloitte Consulting, explains the difference between the two concepts of a backup and recovery strategy and business continuity planning: 'Backup and recovery strategies execute regular procedures to back up critical data. This is done with the expectation that backup copies will be available for complete file restoration from isolated events such as disk crashes, temporary power outages or to cover regulatory requirements. In contrast, disaster recovery planning needs to assume that widespread impact is experienced and that many applications, systems and users will contend for recovery resources. This fact, coupled with the new demands of continuously available applications (for example, web-based systems) and the explosion in the volumes of data from enterprise systems, challenges the appropriateness of traditional recovery approaches.'

FACTORS AFFECTING THE ADMINISTRATION OF PLANS

The effect of change

The disaster recovery/business continuity plan is prepared under a given set of circumstances. But businesses change, and the recovery/business continuity plan needs to be constantly updated with reference to changes such as expansion and relocation of staff, new premises and new IT applications. For bigger changes such as mergers and acquisitions, a complete overhaul of the plan is likely to be needed.

Testing

The question also arises as to whether any current plan has been tested, and when. There should be at least a quarterly review and testing of the plan to ensure that it is up to date and relevant. Part of testing of the plan can be in the form of computer simulations.

A culture of awareness

The whole organization should be involved in the plans for disaster recovery, since the human element in its implementation is vital. If only a few people know what steps to take, they may not be available at the time of the disaster and the business will run into immediate difficulties. Risk identification and elimination should be imbued in the company culture and not just left to the few.

Lessons learnt

The effects of disasters have been studied in detail around the world by Survive, a worldwide membership group for business continuity management professionals, and lessons for disaster recovery have been learnt through hard-won experience. The destruction of mainframes through fire, for instance, has crystallized the need for having agreements with suppliers of such equipment in case of disaster. An inventory of vital equipment should be kept and the storage areas for crucial records should be identified. If vaults and safes are used, are they really fireproof? 'Fire resistant' may mean fireproof for a certain period and at certain temperatures only.

TERRORIST ATTACKS – SHOULD THEY BE GIVEN PRIORITY?

Disruptive events have a wide variety of causes, such as human error, power outage, hardware and software error, network failure, power surges, earthquakes, fires, floods and hurricanes, and malicious attacks. There has recently been a tendency to relate disaster recovery to terrorists' threats, no less so after September 11. But up to now, terrorist attacks have been infrequent in statistical terms, and with the new focus on war against terrorism, hopefully will remain in this low-risk category. The problem is that although they are infrequent they can have devastating effects, not only on equipment and systems but in terms of loss of human lives. Accordingly, they should be given emphasis in any disaster recovery plan.

GLOBAL BUSINESS CONTINUITY

A disaster recovery strategy is often drawn up as part of a wider business continuity plan rather than as a stand-alone exercise. Business continuity services supplied by outside providers to global companies should ensure that systems are operational on a global basis. Disaster-tolerant solutions should be invoked which are not only based on the recovery of hardware and software but also incorporate benefits to the business in the long term in terms of flexibility and cost-effective solutions and extending the reach of networks across countries.

In February 2002 leading enterprise storage company Compaq announced a 'business continuance solution' comprising the availability of fibre channel and Internet protocol technology which extends the reach of SAN systems around the globe through the implementation of global data replication networks.

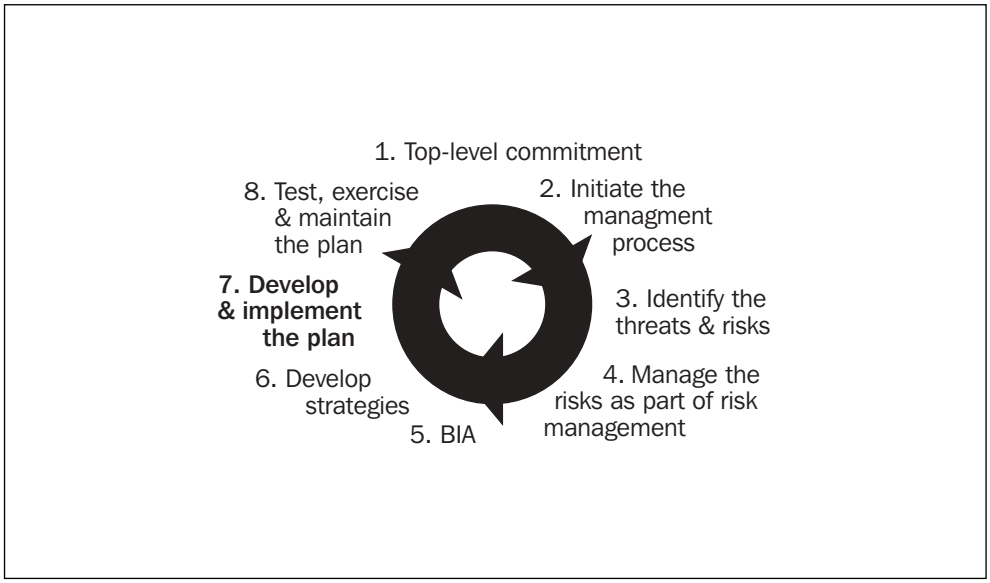
THE BCM PROCESS

The BCM process will be most effective if it has board-level support. Typically, a business continuity management team who will draw up and implement a plan over a period of time will be set up. The BCM process will be ongoing rather than a once-for-all effort and will involve an identification of threats and risks to a particular business, which will depend on the nature of the business and its environment. A development of strategies for dealing with such risks is part of the process and should include a business impact analysis (BIA). An ongoing management of the risks is part of the risk management team's responsibilities. The ongoing plan prepared by the team identifies the various crises that may evoke the elements of the plan, in terms of threats and risks. The plan should develop written guidelines for procedures to be followed in the event of a disaster of a particular kind.

The DTI has presented a schematic diagram of the BCM process, shown in Figure 4.1. The stages are as follows:

1. Top-level commitment secured.
2. Initiate the management process.
3. Identify the threats and risks.
4. Manage the risks as part of risk management.
5. Business impact analysis (BIA).
6. Develop strategies.
7. Develop and implement the plan.
8. Test, exercise and maintain the plan.

Fig. 4.1 BCM – an ongoing process



Source: DTI, Information Security Breaches Survey, 2002

The implementation phase

In the initial stage of the BCM management process, a time scale for the drawing up and implementation of the plan should be worked out. What is the budget available in terms of paying for tangibles such as new disaster recovery systems if required (hardware and software), training of staff, the cost of management time, etc.? Are there any regulatory/statutory obligations that have to be met, such as the need to keep data for a certain number of years or, on the personnel front, the obligation to provide a safe environment for employees? Would it be necessary to bring in assistance from outside to implement the plan? Is there a separate crisis management team in place, as distinct from or the same as the BCM management team? What would happen if disaster struck before the business continuity plan has been formulated?

An important aspect of the success of the business continuity plan is risk management, which relates to all types of risk. One of the first objectives of risk management is to look at the risks that may exist and be a threat to the organization, and to categorize such risks according to relevant criteria. Are they technical or economic in nature, are they people related? Are they external or internal to the organization?

Examples of the different areas of crisis are given in Table 4.1. These relate not only to risks against IT systems but also to risks to the organization as a whole. The BCM process is therefore not only aimed at IT systems failure but takes in threats in all its forms, which should be guarded against to ensure corporate survival.

Table 4.1 The different areas of crisis in the BCM process

	Technical/economic		
	IT systems	!	Industrial accidents
	breakdowns	!	Government crisis
	Contamination	!	Utilities failure
	Industrial	!	Natural disasters
	accident	!	Supplier failure
Internal			External
	Onsite product	!	Sabotage
	tampering	!	Terrorism
	Malicious acts	!	Labour strikes
	Organizational	!	Offsite product
	failure	!	tampering
	People/social		

Source: DTI, Information Security Breaches Survey, 2002

INSURANCE AGAINST DISASTERS

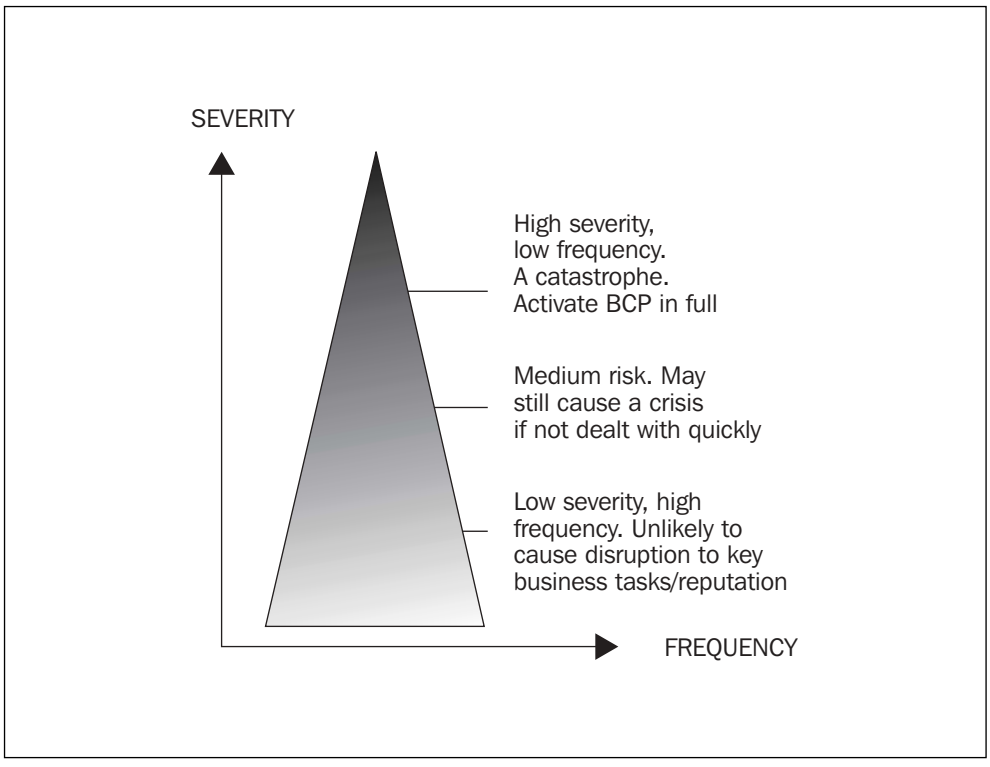
Actuarially, risks in the shape of disasters can be categorized as insurable risks and uninsurable risks, and insurance policies reflect this grouping. Natural disasters such as flooding, for instance, are insurable, but actuarial risks can change following natural disasters, such as the flooding in the UK in 2001. Following such events, insurance companies are revising their policies and certainly their premiums for such risks. Exclusion clauses such as earthquakes and other force majeure events, etc. are well known. As part of their risk assessment, BCM teams should revise existing policies to establish what is and what is not covered. However, just because a risk can be insured against, it should not be ignored, since the loss of business which may ensue is not necessarily insurable, certainly not in the longer term, and no amount of insurance will help if the enterprise goes out of business as a result of a particular disaster. The old adage 'prevention is better than cure', is as applicable as ever.

FREQUENCY OF RISKS

In Figure 4.2 the frequency of risks is plotted against their severity. The DTI recommends the ABC method, a rule of thumb method for assessing the more physical risks which may relate to corporate premises. This method identifies

three key areas of risk: A – area, B – building and C – contents. The A category identifies risks to premises from the area as a whole. The area may be prone to flooding or may contain rivers with contaminated flows. Neighbours may not be suitable in terms of industrial activity, which may cause air, noise or water pollution. The B category addresses whether the building or corporate structure is vulnerable to sabotage. This question has become particularly relevant following September 11 when the tower blocks thought to be invulnerable and built to the highest safety specifications imploded following the terrorist attacks. Not only structural questions arise. What about the water supply, electricity, telecommunications? The C category relates to contents. A complete itinerary of contents and assets should be drawn up and the contents considered from the point of view of vulnerability to sabotage, disasters, overheating, contamination, pollution, equipment, etc.

Fig. 4.2 **Risks measuring/probability**



Source: DTI, Information Security Breaches Survey, 2002

Ernst & Young includes business continuity planning as part of a wider strategy of providing technology and security risk services. A business continuity plan newly developed and implemented by E&Y for an insurance company was put to the test on September 11. Because the plan had been recently reviewed and tested and vulnerabilities exposed and minimized, when put into action the plan ensured a successful recovery process.

REVIEW OF THE BUSINESS CONTINUITY PLAN

The business continuity plan addresses the question of recovery from a disaster event on an enterprise-wide basis. To keep the more comprehensive business continuity plan up to date, it should be reviewed at regular intervals. The underlying assumptions of the plan should be challenged, since they may have changed since the inception of the plan. Does the plan contain a distinction between getting critical systems online and a full recovery? Can advances in technology and their implementation help strengthen the plan? Has any outside help for recovering been considered, such as emergency services, vendors, IT providers, business partners?

Business impact analysis

As part of the business continuity plan, or as a separate exercise, a business impact analysis should be conducted. A BIA attempts to quantify the cost to the business of protecting assets under a security programme. Is the cost of a particular asset worth the expense of protecting it? And does the element of risk justify the expense? The aim of the BIA is to analyze what the critical assets, resources and processes of the business are, and the financial impact a loss or destruction of some or all of the resources would have on the organization.

Elements of the business continuity plan

The business continuity plan should involve all levels of management and functions. It should also address such points as the cost of an outage of a particular application. How much business will the enterprise lose if any particular application goes down? In other words, how critical is the application to the continuation of the business? This will help to prioritize available applications. The most important application would need to be recovered first if a disaster occurs. Applications may also be interdependent, in which case not only the critical applications should be restored but also those upon which the critical applications depend.

It is also important to determine the critical time for recovery and whether the backup systems can be restored within this timeframe. It is worth looking at this particular aspect as the backup systems installed may not be able to meet the requirements in this respect and may need updating or replacing.

THE DISASTER RECOVERY PLAN

The importance of having a disaster recovery action plan was illustrated vividly not only in the September 11 attacks but also in the London bombings in the 1990s when the Commercial Union headquarters was blown up.

The disaster recovery plan should be preceded by a risk assessment which will give an idea of the risks to a company, its property in detail, and an impact assessment which will examine the consequences of a catastrophic disaster, such as the loss of an entire office block. The impact assessment will identify essential core activities and critical activities and look at other functions in order of priority, from important functions down to non-essential support functions and other non-critical aspects of the company.

The disaster recovery plan will look at the best way of supplying resources in the event of a disaster, whatever the source. The speed of response can be vital in protecting the company and ensuring its continuation as a viable business. The Commercial Union building was sabotaged on a Friday evening, and showed its speedy response in the placing of an advertisement on the following Monday morning in the dailies, with a photograph of the damaged headquarters and a 'business as usual' message. The same day, the company's computer systems were up and running, in a different location and on a reduced scale, but sufficient to cope with the processing of critical data.

Lines of communication are extremely important in a disaster situation and should be pre-established, with the names and contact numbers (including mobiles) of key managers and their assistants/deputies and their usual whereabouts and activities. A plan of steps to be taken should be produced, including a determination of alternative premises and computer systems and their backup.

Do customers/relatives need to be notified of the disaster? In the wake of the WTC attacks, several of the major financial firms immediately posted messages on their Websites with condolences, notifications of losses and reassurances that clients' financial records were safe. As soon as possible after the disaster, customers should also be notified of when things are expected to return to normal and any changes in business operations, such as relocation to new premises.

The disaster recovery plan should contain guidelines for fire drills and evacuation procedures to be followed. Once a document in the form of a disaster recovery plan has been prepared, it should be circulated to the relevant members of staff.

Check list – disaster recovery plan

The elements of a disaster recovery plan are supplied by Janco Associates, a US firm of consultants. The DR plan includes the following steps:

1. Business impact analysis.
2. DRP organization responsibilities (pre- and post-disaster).
3. Recovery strategy, including approach, escalation plan, process and decision points.
4. Disaster recovery procedures (in a check list with approval format).

5. Planned administration process.
6. Technical appendix (including necessary phone numbers and contact points).

Part of the plan is a full test, including:

- disaster recovery manager responsibilities
- distribution of the disaster recovery plan
- maintenance of the business impact analysis
- training of the disaster recovery team
- testing of the disaster recovery plan
- evaluation of the disaster recovery plan tests
- maintenance of the disaster recovery plan.

It is recommended that the plan itself should contain the following sections:

1. Plan introduction.
2. Business impact analysis.
3. Recovery strategy.
4. Disaster recovery organization.
5. Damage assessment and salvage team (pre- and post-disaster).
6. Disaster recovery emergency procedures.
7. Plan administration.
8. Appendix, to contain address lists, inventories, etc.

BAM (BUSINESS ACTIVITY MONITORING)

An upcoming ongoing technique, which does not rely on a disastrous event or mission-critical happening to kick into effect, is BAM. Through BAM, the key information and real-time technology solutions available combine to enable managers to make decisions in response to critical events at any given time, based on the most up-to-date business intelligence combined with elements of technology such as database management systems. The new technique is still in its infancy and has its detractors who claim that a business can suffer from overload of information, thus stifling initiative.

CONCLUSION

Disaster recovery and business continuity plans broadly aim to cope with disasters that may or may not threaten the survival of the business, and to bring the business back to normal as fast as possible. The plans differ in scope, with disaster

recovery typically being more narrowly focused on IT systems and business continuity involving functions throughout the enterprise. The plans also differ in design, revolving around the modus operandi of a particular organization, its size and its industrial/commercial sector. Whatever the format and content of a plan, an important aspect from a management point of view is to keep it alive and to update it constantly in the light of changing circumstances. Such a strategy will enable the organization to cope with disasters immediately they occur, thus minimizing the consequences.

5

Data backup and storage solutions

INTRODUCTION

The backup and storage industry has come a long way since the early days of disk and tape backup where backup tended to be given low priority and the storage of data amounted to taking a floppy disk or a tape home at the end of the working day. But with the explosion of data to be stored, the increased dependency of commerce and industry on electronic data, and the advances in technology, the backup and storage function has moved from being a low-level activity right to the fore of corporate awareness. With new technology and the development of storage networks, backup devices can now be installed away from the processing centre and storage can be offsite. The speed, reliability and scalability of backup have increased, and backup has progressed from an obscure, once-in-a-while activity to a highly focused, regular or even instantaneous operation.

TAPE BACKUP AND RESTORATION OF DATA

With the increasing reliance on technology for the storing of data and the explosion in critical and non-critical data to be stored, storage products have proliferated. But despite the many new solutions on the market, traditional tape backup is still very much to the fore and remains the predominant method of storage in corporate environments.

ADVANTAGES OF TAPE BACKUP

Tape has several advantages, one of which is its cost effectiveness. This is particularly important for SMEs with their smaller budgets. The proponents of tape drives list the advantages as follows:

- **Cost effectiveness** – tape is the most cost-effective method of storing large databases. With special software, backup can be performed automatically at times to suit the user.
- **Speed** – with data constantly expanding and the time available for backup constantly being cut down, speed is critical. The speed of tape drive backup has increased in recent years and is now typically up to 30 MB per second.
- **Uncomplicated** – tape drives allow the user to back up data on servers of small to medium size on a single cartridge. Tapes are easily portable and can be removed and stored offsite.
- **Reliability** – tape drives are reliable and are constantly improving in quality.

TAPE FORMATS

The tape backup market is constantly bringing out new products with higher capacity and transfer rates. Tape formats are based on a variety of technologies, the major groupings of which are listed below:

- DDS – digital data storage
- DAT – digital audio tape
- LTO – linear tape open
- DLT – digital linear tape
- AIT – advanced intelligent tape technology
- DTF – digital tape format
- SLR – scalable linear recording technology.

DAT in the original technology, a standard developed by Hitachi. DDS is a modification of DAT and is a low-level formatting standard developed by Hewlett-Packard (HP) and Sony. The DDS format is a desktop/server backup product. Four generations on, it is now produced as DDS4, native capacity 20 GB and transfer rates of 2.4 MB/sec. It is marketed by Hewlett-Packard, Sony and Seagate, among others.

LTO is an open format tape technology designed for mid-market companies and networking environments. It is available under licence to all manufacturers, and major manufacturers (Hewlett-Packard, IBM) have entered this market. The Ultrium LTO product is marketed by IBM and Hewlett-Packard (marketing the half-height Ultrium 215, native capacity 100 GB).

DLT provides reliable technology for business-critical application and compatibility across the range. It has been widely installed around the world. It is used for mid-range to high-end backup and is available in desktop, internal and rack-mounted models, as well as one-slot autoloaders, and mid-range and high-end libraries. DLT has been complemented by DLT-1, a low-cost alternative. The half-height DLT-1 product has been launched by Benchmark and is now part of the Hewlett-Packard portfolio. Quantum has come out with a next-generation DLT, the S-DLT (native capacity 110 GB, transfer rates 11 MB/sec). DLT tape drives are being manufactured under licence by Tandberg. DLT tape libraries are available from a number of well-known companies.

AIT is highly compact, reliable and one of the best performers on the market. It has full read/write compatibility across the range. It is replacing DDS technology due to its better performance and higher reliability and is being marketed as an upgrade to the DDS-2 and DDS-3 products. It uses the latest high-density heliscan recording technology. AIT drives deliver up to three times more GB than DDS-3 (91

GB); they are up to six times more reliable and will back up data in a quarter of the time used by DDS-3 (backup rate of up to 37.4 GB per hour and a compressed capacity of 130 GB in a single tape). They offer up to 300 per cent more capacity than a DDS-4 drive, but are marketed at the same price. A new generation AIT, the AIT 3, is being launched for multi-server and multi-user environments. A single 8 mm cassette will give 260 GB, at a native rate of 112 GB. Vendors endorsing AIT technology include Compaq, Legato, Hitachi, Exabyte, Sony, Qualstar, Spectra Logic, Dantz and BakBone and Network Appliance.

The digital tape format tape drive and data cassette was marketed by Sony in 1995 and is aimed at the video editing and broadcasting market. Its latest product in the range, DTF-2, gives 200 GB uncompressed capacity and transfer rates of up to 20 MB/sec (sustained transfer rate 12 MG/sec). DTF is based on metal tape technology.

Tandberg is promoting a highly scalable technology, the SLR. The scalable linear recording technology includes seven different generations, from the SRL 2-4 through the SRL 5, SRL 24, SRL 40, SRL 50, SRL 60 to the SRL 100 (native capacity 50 GB, native data transfer rate 5 MB/sec). In the offing are SRL 150 and SRL 400. Tandberg's cartridge library, based on the SLR 100, has up to 2 TB of native storage capacity, with up to four drives. The company is also partnering with Qualstar to offer its high-end libraries.

Optomagnetic data storage

A Tandberg subsidiary is developing the optomagnetic data storage format. There is some curiosity in the industry as to whether the new technology is tape or disk based. The product is expected to be launched in 2003–4.

CD-ROM and DVD

CD-ROM has captured part of the storage market but is now likely to be overtaken by DVD-ROM, although there is disagreement about when this crossover will be effected. Due to the low price of CD-drives in the recordable/rewritable market, the lifetime of this market may be extended and will continue to appeal to low-end users.

BACKUP PRODUCTS: SERVICE AND MAINTENANCE

Like all computer systems, backup products, single drives as well as libraries, require maintenance and service. The importance of keeping downtime to a minimum with a high level of availability makes this requirement even more vital.

Tape backup providers

Well-known tape backup providers include major companies such as Hewlett-Packard, IBM, Sony, Seagate and Veritas. Other specialists/products in the storage arena include Arkeia, Ecrix, Exabyte, Legato, NCE, Plasmon, Syncsort, Tivoli, Spectra Logic, BakBone, Benchmark, Iomega, Syquest, Dantz, Overland, Computer Associates, Storagetek and Quantum.

NEW BACKUP TECHNOLOGIES

Intelligent backup

The information a typical company needs to store includes general information, financial records, employees' details, marketing plans, production schedules, stores records, disaster recovery plans, e-mail correspondence, etc. The loss of much of this information could be disastrous. The role of intelligent software is to ensure that the information available is as recent as the last backup.

Unlike traditional backup, intelligent backup offers the advantages of the original full backup, with incremental backups linked to the full backup set. The intelligent backup software therefore gives the advantages of both full and incremental backups, with a saving in time and space. The software identifies which fields are new or have been altered since the last backup and enables the original backup to be built upon, in a progressive backup process. Restoring software of this kind has been developed and is marketed by Dantz. Its product Retrospect can restore with snapshots of entire volumes to the exact state prior to the loss of information. It copies everything it needs to make the backup set complete and obviates the need to restore from multiple backup sets.

Virtualization

A new concept in storage is hailed as a cutting-edge technology which will allow users greater flexibility in the use of their storage disk space, and due to better utilization of capacity will cut cost. Effectively, the storage capacity available on all devices in a network is merged into a virtual pool. This means that all storage data will be 'shared' in a single place. Industry leaders such as HP, Dell, EMC, Veritas and Hitachi are enthusiastic about this new concept although it is still viewed with scepticism by many clients. To enhance its acceptability, the Fibre Channel Industry Association Europe has called for standards to be developed. Also embraced by the concept of virtualization is SAN storage abstraction, an indirect representation of storage, which is under development.

Interoperability

There is a growing demand for interoperability, or the ability of one vendor's servers to be used for another vendor's storage devices. Several vendors have adopted this new approach and have formed alliances to meet the demand. Storage systems from Hitachi, for example, are being sold through HP and Sun Microsystems. IBM has also recently gone in for the 'open systems' approach.

Snapshot

The new snapshot technology is another facility which provides reliable SAN backup solutions. Snapshot can reduce or eliminate the backup window, but needs additional online disk storage. This technology has been described and named in several ways, but basically, the aim is to create a point-in-time image of a file system and use this image as the reference point for the backup. Once the snapshot has been taken, the primary data can be modified without interfering with the backup operation. Some of the available solutions provide a 'copy on write' facility which allows the old storage blocks to be copied to a second storage area before the updates to primary disk storage are made. With copy on write techniques, storage space can be minimized since the end result is a virtual copy and only those blocks that have been modified have both an old and a new data block. An alternative is to provide a mirror copy of the data and split the mirror, using the split copy as the source of backup.

Mirroring

The mirroring of data from one system to another results in two identical systems, one backing up the other. The duplicate backup can be located locally or at a remote site. Whenever a change is made to the data, the mirroring software automatically duplicates the change. The software will also monitor the primary system and will switch operations to the backup system in cases of failure of the primary system. Manual switching to the backup system is also possible when the primary system requires maintenance. In this way, consistent, predictable access to mission-critical applications and data is maintained. Thus, downtime is virtually eliminated, whether it be from planned events, e.g. nightly backups, upgrades and database reorganizations, or unplanned events, e.g. server failure, fire, floors and outages.

An example of mirroring software is Immix Availability Management Software (Mimix/400 and Object/Object) produced by Lakeview Technology. The solution has been installed under licence with various clients, including Bayerische Landesbank's New York branch which wanted a solution for protection of its

AS/400 data (IBM). The software is run over a WAN. The bank says that with the mirroring system uninterrupted business processing is maintained, despite human error and environmental disasters. The software dramatically reduces the cost of disasters. It also sustains the bank's reputation for reliability, especially as far as the bank's clearinghouse functions are concerned. The software frees up information systems (IS) staff from lengthy restore projects and eliminates the need to re-enter lost data.

Clustering

Clustering is a technology that enables highly available and scalable Websites to be built. A cluster consists of a group of machines or servers running applications between them as if they were a single entity. Cluster implementation methods provided by vendors vary from one vendor to another. Examples of cluster enablers are Silverstream Application Server 3.7, BEA Weblogic server 6.0, Sybase Enterprise Application Server and Bluestone Total-Eserver 7.2.1. In some configurations, each individual machine is not aware of what the other machines are doing, in others, machines are fully integrated. Extra servers can be added to clusters, providing more capacity and increased scalability.

Clusters also provide for high availability through redundancy. If any one machine fails, another machine will take over. In 'shared disk' clusters, a single storage device is used by all application servers to obtain the applications required.

For storage purposes, the main use for clusters is within SANs. Users can write and read data to the network through a SAN switch which connects the various servers and databases to a storage medium of disk arrays. Failover is to mirrored disk arrays via the SANs.

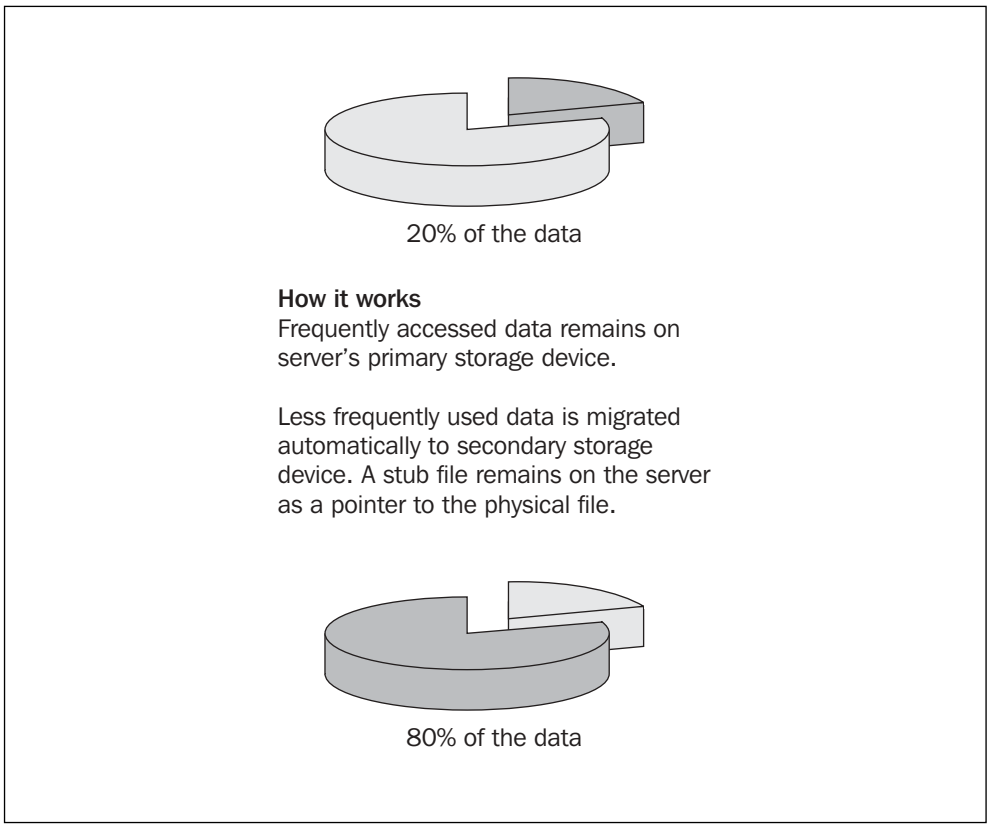
RETRIEVAL – PRIMARY AND SECONDARY STORAGE

The need for retrieval of data varies with the importance to the business of the data stored and the length of time of storage. Ageing of data means that the data are required less frequently. In most organizations, the data more frequently accessed are those generated within the past 24 hours. Up to 7–14 days later, data are accessed with less frequency, and after 21–18 days, access is infrequent. A model has been developed round these findings, estimating that some 20 per cent of data is required frequently and 80 per cent less frequently. If the 80 per cent of data remains in the primary storage, the backup window available is reducing at a high rate, not to mention the overall increase of data for storage, estimated to be 80–90 per cent. This follows Pareto's principle, also called the 80:20 rule, developed by the Italian economist Vilfredo Pareto on studying the distribution of

wealth in various nations around 1900. He found that in most countries, some 80 per cent of the wealth was controlled by about 20 per cent of the people.

With secondary storage, this problem can be alleviated. The data frequently required remain on the primary storage device and the rest is migrated to the secondary storage (secondary storage migration). This can now be done automatically by applying special storage solutions, which remove the infrequently used storage to near line storage, making it possible to retrieve it easily if required. Automatic secondary storage software migrates the data according to a set of parameters, such as the minimum file size and the time the file was accessed, e.g. for modification. Different strategies can be applied to different files, e.g. Word files can be migrated every week and Excel files every two weeks.

Fig. 5.1 Secondary storage migration



Source: Optomedia, 2002

Remote storage

To reliably meet application recovery demands, organizations have implemented systems designed to replicate data and hold real-time copies of files on a separate standby site. To do this, a variety of hardware and software techniques can be

employed, from database replication, using products such as Oracle's parallel server, right through to real-time physical mirror hardware solutions. Two examples of this are EMC's Symmetrix Remove data facility and Compaq's data Replication Manager.

New open standard protocol

Network Data Management protocol (NDMP) is a new open standard protocol for backup of network attached storage (NAS). Developers are Network Appliance and PDC Software, part of Legato Systems. The protocol provides users with choice, due to interoperability.

One of the vendors endorsing the protocol is BakBone (with offices in Poole, Dorset as well as in the US). All major operating systems are supported by its software (Unix, Linux, NT). The BakBone interoperability laboratories certify vendors' products to be fully functional over a wide range of topologies. Its central backup administration software includes NetVault, which supports NDMP.

BACKUP ARCHITECTURES

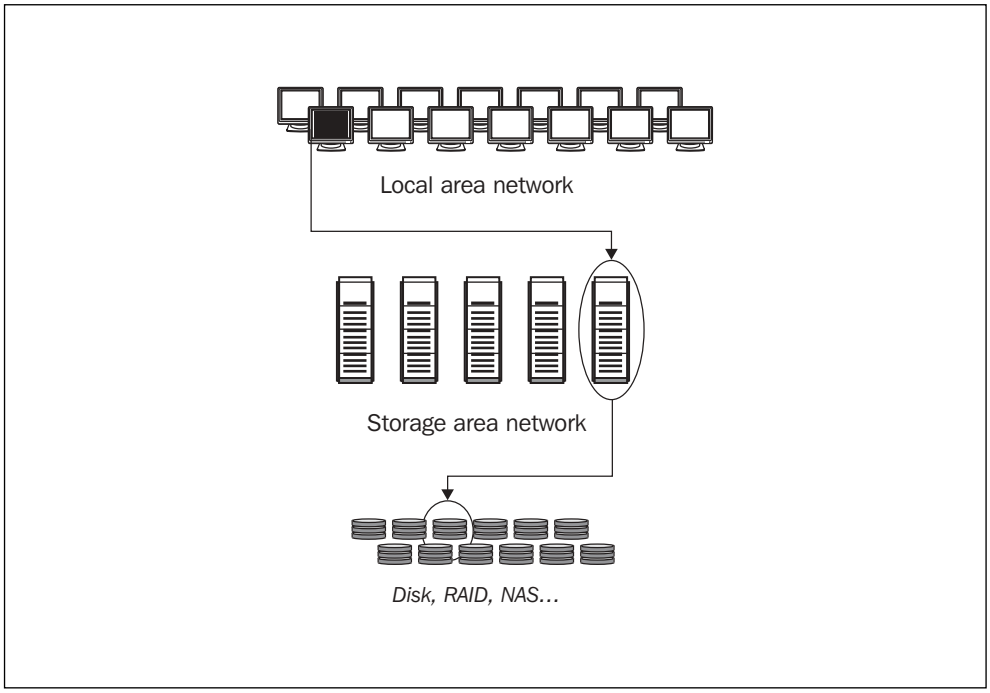
Local system backup

Local backup has been around for a long time, copying data from primary disk to storage devices, most commonly tape (*see* Figure 5.2). This traditional method is employed in stand-alone systems as well as large servers and relies on various types of software, some of them tailor-made by the users themselves to suit their requirements. Such a local system backup is self-contained and does not rely on networks or other servers. The main drawback is that it requires a dedicated storage device for every server.

Storage area networks

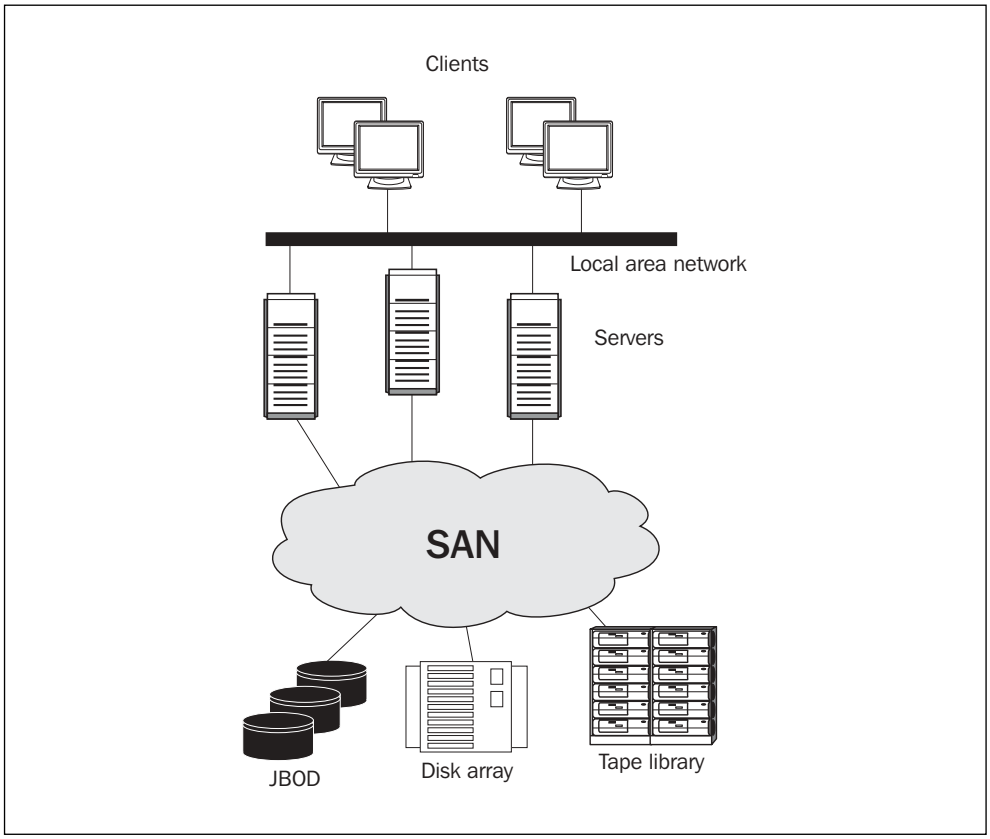
The requirements for storage and recovery vary widely and this has spawned a number of backup architectures, taking into account different types of storage connectivity. Many of the new backup solutions are suitable to a SAN environment (*see* Figure 5.3). The transition to SANs typically takes place if there are shortcomings in a direct attached storage environment and taking applications out of service to perform backup means loss of revenue. In addition, firms which are relying on the Internet for their operations can remain online all the time. Direct attached storage architecture also did not allow for centralized storage and management backup, nor for quick changes in storage and server configuration. Scalability, necessary for business expansion, is another problem which SAN overcomes.

Fig. 5.2 Local backup



Source: FCIA Europe, 2001

Fig. 5.3 SAN example



Source: The Evaluator Series, 2001

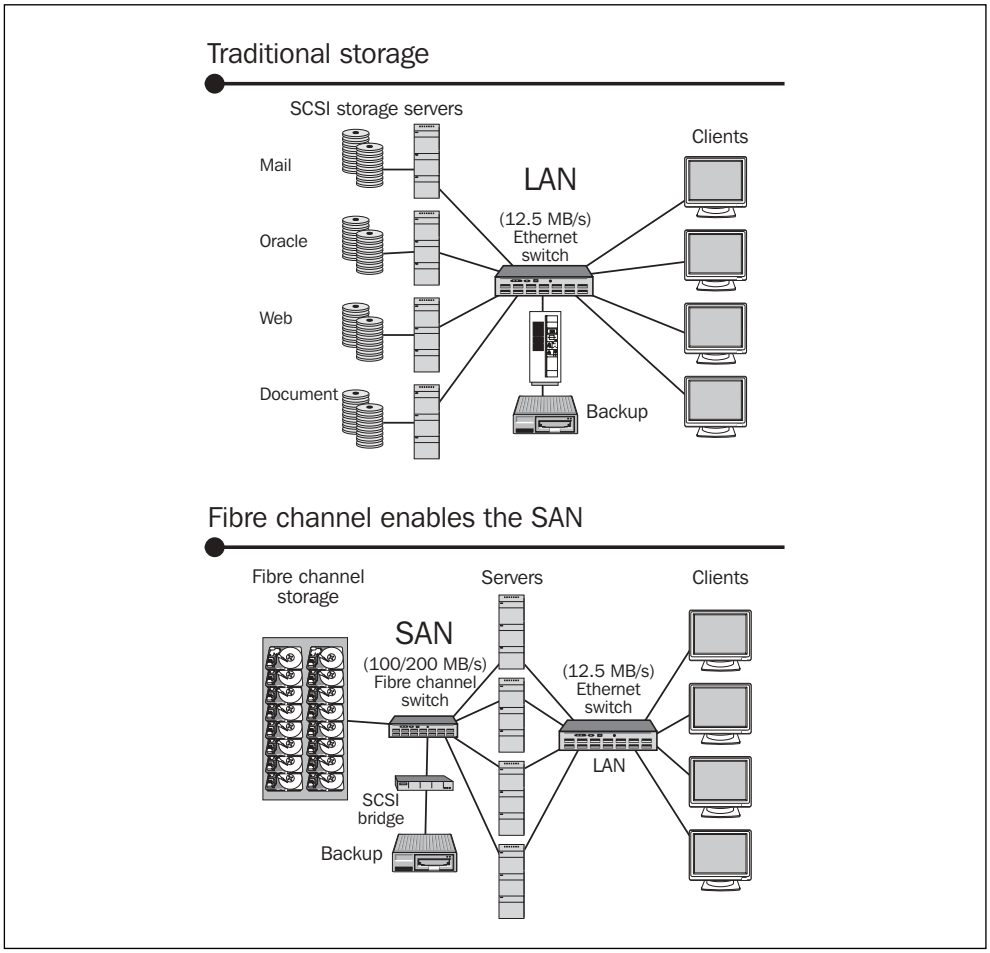
TYPES OF NETWORK

LAN is a local area network consisting of a group of servers connected by cable and allowing users to share resources. The WAN (wide area network), covering long distances) is the alternative to the local backup storage. LANs are in-house networks. The term MAN stands for metropolitan area network. Some companies have their own LAN/WAN facilities; others lease them from specialized suppliers. LAN-to-LAN connections are also supplied by telecommunications companies under a variety of arrangements.

SANs are becoming widespread as a method for attaching storage and servers through a network, separate from the traditional LAN. Today's SANs are based on fibre channel. The SAN consists of hardware components such as servers' storage devices attached to the SAN via switches, hubs, bridges and host-bus adapters, as well as a SAN appliance or SAN server.

Figure 5.4 juxtaposes traditional storage based on a LAN with the fibre channel-enabled SAN.

Fig. 5.4 **Traditional storage vs fibre channel-enabled SAN**



Source: FCIA, 2002

SAN MANAGEMENT SOFTWARE

A major element of SANs is the management software, used for the management of the fibre channel storage network and the management of the storage. The functions carried out by storage management include the following:

- storage network monitoring
- event management and alerts (e.g. remote management and diagnostics)
- security management (authentication, access controls, encryption).

BENEFITS OF FIBRE CHANNEL STORAGE NETWORKING

The benefits of fibre channel, including backup, are outlined by Andrew Batty, Chairman of the FCIA Europe: 'Fibre channel, a data transport technology that can run over fibre optics or copper connections, is the dominant available technology to enable SANs. Ideal for applications such as remote backup or disk mirroring, it allows the fast transfer over the long haul (up to 120 kilometres in one stretch over fibre) of vast amounts of data. Also, because fibre channel can travel over IP and SONET, and thanks to its wide acceptance, reliability, performance and viability, it allows its users to maximize the potential of their stored data and their networks thanks to features such as LAN-free/server-less backup, disaster-tolerant clusters and storage virtualization. In terms of backup, fibre channel SANs allow companies to backup and archive data while staying online and minimize costly downtime, and also protect their information by remotely replicating data to other locations either in the same city or in different countries. Backup storage solutions have changed over the years from decentralized storage, back to centralized storage, through network attached storage solutions to SAN environments, which has developed backup solutions in new directions.'

Fibre channel storage networks are attractive to users for a number of reasons. The networks are able to cope with the exponential growth in the requirements for more storage as a result of the explosion in information and data that are to be stored, including e-mail traffic. Competitive pressures to perform on a 24×7×365 basis are increasing rapidly. Storage area network infrastructure is capable of meeting the need for flexibility and delivery of information on an instant basis to the end user.

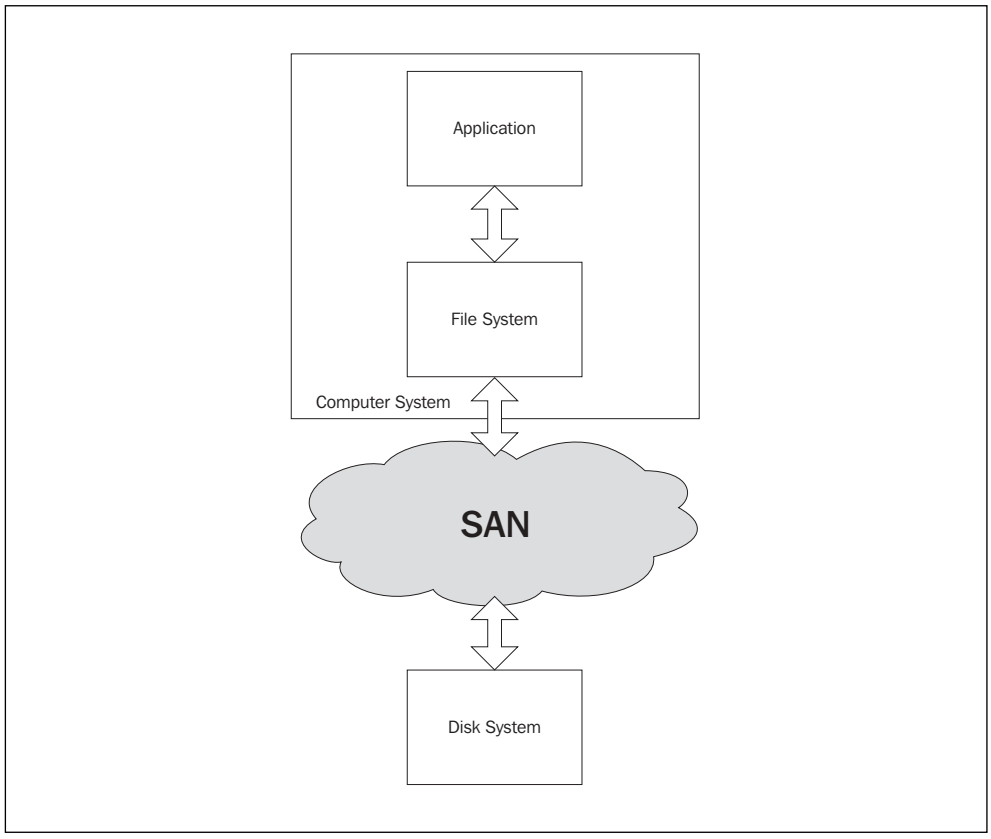
Areas of cost savings resulting from a fibre channel SAN should be looked at from different angles. A sophisticated hardware and software system means better identification of spare capacity within the storage system, which in turn can be allocated to new applications requiring storage. The new mirroring techniques lend themselves to storage over long distances and therefore provide better disaster recovery protection. A comprehensive network-based storage also requires fewer servers and storage units overall.

The main benefits of storage networking based on fibre channel technology are summarized as follows:

- It allows multiple servers, clusters and workgroups to share storage.
- Management of backup data is simplified.
- There is high bandwidth between servers and storage devices.
- There are good interconnects for offsite replication of data (mirroring).
- It reduces server overheads.
- It offers a high degree of fault tolerance (no single point of failure).
- There is a high degree of scalability.
- It improves ROI.

In terms of return on investment, SANs have shown themselves to pay excellent dividends. Despite expanding storage requirements and workloads, storage resource and management costs have remained constant or decreased.

Fig. 5.5 Storage area network



Source: The Evaluator Series, 2001

ENVIRONMENTS

SAN backup architectures are more suitable for some environments than others. The SAN-based architectures work better for a small number of large files than a high number of small files. In the latter case, the overhead of mapping the objects and exporting the copy operation is high. Database environments (e.g. Oracle) lend themselves well to SAN backup architectures, since typically they consist of a small number of large objects. Exporting copy services to an offsite facility is also suitable for image backup of high-population file systems. Since the entire file system rather than individual files within the file system is being copied, this reduces the mapping and copy operations.

THE FIBRE CHANNEL MARKET

SAN technology is forever moving forward and in the world of backup, fibre optics is the talk of the town. Fibre channel SANs are increasingly popular with financial services in particular, as they allow for the storage of large amounts of backup data in a radius of 100–120 kilometres away from the main data operating centre. The backup device can simply be a tape in the offsite location through a fibre channel connection. Like a black box in an aircraft, tape is resilient and recoverable if a catastrophe occurs.

The fibre channel market has expanded by leaps and bounds in recent years. In 2001, an estimated 17.5 per cent of European businesses were deploying fibre-based SAN. The development of international standards for networked storage is a further catalyst for growth, ensuring the interoperability of certified configurations of equipment from different vendors.

INTEROPERABILITY STANDARDS

One of the delaying factors in making fibre channel the preferred choice in setting up storage networking has been the lack of open standards. The Fibre Channel Industry Association (FCIA) has been working towards achieving interoperability standards and has announced the joint approval by FCIA members and the T11 (the committee responsible for fibre channel device interfaces within the NCITS (the National Committee for Information Technology Standards) of the FT-SW-2 standards for switch interoperability.

WIRELESS LANS

Vendors and carriers are experimenting with wireless LANs and despite security concerns, these are gathering momentum. British Telecom is among the pioneers in introducing wireless LANs, having announced plans for selected areas of wireless LAN availability to be operational in a few years' time. The new service, which will be charged for, will operate initially from public places such as airports, railway stations, bars and hotels.

CONCLUSION

From traditional tape storage to LAN, SAN and WAN, the backup and storage industry has progressed rapidly in recent years. New technologies have created highly reliable backup solutions, with much increased speeds, high availability, performance and scalability. Most importantly, the new high-speed networks have enabled backup to be performed in locations sufficiently remote from the processing centres to put backup and storage out of the reach of disasters striking in one location or area, thus safeguarding mission-critical information. Future challenges facing the industry include new SAN development areas and the wireless network, which is already being planned and beginning to appear in experimental form in the US and the UK.

6

Spreading of risk: remote backup and storage facilities

INTRODUCTION

Increasingly, large firms are realizing the need not only to have a backup IT facility offsite but to have an entire operational entity in a remote location from which business can be carried on, complete with office equipment and a full backup and restoration IT facility. This substantially reduces the risk of a major disaster paralyzing critical operations of a company.

A whole new industry sector has sprung up in response to this need for remote facilities, the colocation industry. The colocation facilities provided by this sector are also known as Internet hotels, carrier hotels or server farms. The colocation centres provide a neutral and secure environment for corporate IT backup systems on a contract basis. The companies looking for remote backup and restoration services may also set up duplicate centres themselves, or simply have emergency locations or other facilities on standby. The following gives an overview of some of the solutions on offer.

THE COMMAND CENTRE

Prior to the setting up of a functional recovery location, some businesses set up a temporary command centre, in a location that can be used immediately following the disruption, to do the initial assessment and evaluation of damage and to start off the actual recovery process. The command centre should be adequately equipped, with communications and other facilities.

THE RECOVERY CENTRE

The recovery centre will typically be a facility other than the primary location, used for restoration of data and data processing. Such a centre is equipped with power and telecommunications. A recovery location can be a cold, warm or hot site. A cold site is an offsite remote location, which has no equipment apart from infrastructure such as raised flooring and air conditioning. For the facility to duplicate the functions of an organization, it should have the right infrastructure in place. A warm site is partially equipped and does not require much extra work to be put into operation. A hot site has all the equipment, including backup computers and resources needed to continue business operations after a disaster. The hot site may offer facilities targeted at critical business operations such as data processing and backup.

COLOCATION FACILITIES

Facilities provided by colocation companies are not limited to the duplication of data storage space but include a range of services linking telecom fibres to other networks, Websites hosted and Internet services managed in a highly specific, secure environment. Specifically, colocation companies serve new technology service providers such as Internet service providers (ISPs) and telecommunications providers (telcos), as well as application service providers (ASPs), managed networking and hosting providers. They also provide facilities for e-commerce companies to locate their hardware in the same place or building. Environments can be carrier neutral, i.e. offering customers access to a wide choice of carriers, as opposed to being carrier specific.

Growth industry

According to Ovum, a research company, the colocation industry is expected to increase in size by some 30 per cent a year, and it is estimated that there will be some 10.5 million square metres of colocation space worldwide by 2005.

DUPLICATE FACILITIES

A company can have its own remote duplicate facility, i.e. office space facilities equipped with sufficient electrical connectivity, communications access, space and access to accommodate sufficient staff to continue critical operations in the event of a disaster. Such a facility is a complete, unmanned operational unit, which can be occupied at a moment's notice. Following September 11, major US financial companies looked to London, Scotland and Scandinavia to set up such duplicate facilities, out of reach of possible further terrorist attacks.

Alternatively, such space can be provided as and if required by an outside provider under a contract. Problems giving rise to the need for such accommodation can be hardware communications failure, data corruption, power failure, flooding or other environmental considerations. Disruption can also arise from events such as the UK fuel crisis of 2000 (during which, according to the Institute of Management, 93 per cent of businesses surveyed suffered disruption), rail strikes or other infrastructure problems. The loss to a business following a disaster is well documented. A company may not only see a drop in business for a short period of time but may lose business to competitors or go out of business altogether.

EMERGENCY FACILITIES

Emergency office facilities for the recovery of data may be set up by the organizations themselves or through a provider of office space, such as Regus and Abbey. Regus advertises 'continuity and disaster recovery offices' worldwide as part of its services. The offices are fully equipped not only with the latest telecoms and IT infrastructure but also with desks and other office equpment, and are ready to step into at short notice. The space is guaranteed to be available in a pre-arranged location, as and when needed for key staff, with direct IT links to the existing offices and with participation in the 'link scheme' which provides a dedicated telephone and fax, with telephone answering in the company's name.

Although not specifically a colocation centre provider, Abbey Business Centres provides similar facilities for colocation, if required, with fully equipped offices, LAN, high-speed broadband Internet access, ISDN and digital telephony. A major utilities group has an office for 60 operators on permanent standby in one of Abbey's UK locations. The office is unmanned, but fully equipped and ready for use.

Centres providing companies with facilities for immediate relocation following a disaster have been set up by providers such as ICM Computer Group plc. The group's facilities include an up-to-date telecommunications structure, telephone systems allowing digital switching, and datacomms recovery allowing a reconnection to LAN/WAN. The recovery service agreements making these facilities available also include regular testing and drills. The offices available have from 75 work positions, complete with PCs and telephone access, all office support facilities, including an operational data centre. Multi-vendor systems and platforms are supported. Access control and CCTV monitoring are in place. All sites have their own UPS generator in case of power failure.

Mobile recovery

SunGard, the leading disaster recovery services provider in the US, operates a mobile recovery service activated within 48 hours of a disaster call, with the facility up and running within an hour. Its large fleet consists of mobile recovery centres delivered to the site on a truck. The fleet is positioned in strategic locations around the US, representing 40 centres. SunGard offers a high bandwidth network for recovery, testing and high availability services. The mobile centres provide a 50-seat workstation environment. SunGard recommends converting the company's car park into an IT disaster recovery centre, if necessary. A mobile recovery service is also provided by other companies such as Compaq.

In April, SunGard announced takeover talks with one of its rivals, Guardian IT, a UK disaster recovery provider with a market capitalization of £39.3 million and a forecast loss of £28 million. SunGard acquired some of Comdisco's assets in 2001 in a US$ 825 million deal.

COLOCATION PROVIDERS

Examples of colocation providers and their facilities are given below.

Global Switch

A leading carrier colocation company, Global Switch manages facilities for the colocation of mission-critical services for the telecommunications and data markets. Global Switch provides access to a range of bandwidth connectivity. One of its centres is located in Docklands, close to the City and Canary Wharf. In this location, the company is able to tap into the increasing demand for remote data centres from financial companies.

To ensure maximum protection of data, the company offers a secure environment with purpose-built cages for maximum protection of data. It provides 24×7×365 support, security and access, with uninterruptible power supply, and offers a cost advantage since it can provide power in bulk from major suppliers.

Global Switch operates across Europe, Asia and the Americas, and offers web hosting, data storage, load balancing and firewalls through its subsidiary Internet managed services provider company, KeyBridge Corp. Clients of Global Switch include telecoms companies, ISPs, ASPs and e-commerce companies. Twelve facilities are provided in gateway cities worldwide, consisting of 3.7 million square feet of space. Apart from providing secure controlled environments and multi-fibre connectivity, the company offers basic 'shell and core' space to complex managed services. Global Switch was founded in the UK in 1998 and having partnered with two property groups, it was incorporated in Luxembourg in March 2000 as Global Switch Sarl. The company is one third owned by Unicorn Assets Ltd, TrizecHahn and Chelsfield.

COLT

The COLT telecoms group, a £901 million turnover operation (2001), has set up a wide network of hosting centres across Europe. Its COLT Internet solution centres are aimed at high-end corporate users, SMEs, content providers, applications service providers and start-ups. COLT will pre-configure, manage and maintain servers on the client's behalf. One of the largest telecom operators

in Europe for data transfer, it provides direct access to Colt Euro LAN, Europe's first seamless long-distance fibre optics network.

COLT refers to an explosive demand for colocation server facilities, driven by an ongoing need for web presence and an increasing size and complexity of existing sites.

Exodus (acquired by Cable and Wireless)

Exodus was an early pioneer in the provision of managed data centres for the management of servers, storage space and backup facilities for corporate clients and Internet service providers. Its headquarters in the Silicon Valley, highly secured and in a secret location, was a model of colocation, including hosting and leasing out of data centre space with or without administration and management, and a control centre constantly monitored and managed online. Clients' servers located in the Exodus data centre in California were unmarked for confidentiality and security, and ranged from a few to several racks of servers in air-conditioned environments. However, despite blue chip clients, ambitious plans for expansion ran aground and the company ended up in a chapter 11 bankruptcy process. But Cable and Wireless saved the company's name from extinction when it stepped in and bought up assets and business activities in an all-cash deal concluded in 2002. Cable and Wireless took over 26 data centres in the US and as Exodus was a strong brand, decided to retain the Exodus name there and market it as 'Exodus, a Cable and Wireless service', under the Cable and Wireless logo.

Cable and Wireless is confident that it can build on and strengthen the global IP network initiated by Exodus and is negotiating to take on a further four centres in Asia.

Scolocate

Scolocate in Edinburgh is Scotland's largest colocation facility. Scolocate counts among its clients WorldIX and 14 of the largest telcos in the UK, including BT, Cable and Wireless, Energis and Global Crossing. Following September 11, Scolocate has had an upsurge in interest from financial companies wanting to colocate away from London. Scolocate also advises its customers on disaster recovery planning.

Worldport

Worldport is a UK company with facilities in Central London and Slough, which started in 1999 as Advantage but was later acquired by Worldport in 2001. It is quoted on the London Stock Exchange under the symbol wrpd. Through partnerships and affiliates, the company can provide services in an additional 15 locations.

Worldport caters for SMEs and large companies in the UK and includes among its clients the British Gas Group, Crocus and Quintessential. SMEs do not necessarily need a complete remote centre backup facility and they also differ in the extent to which they rely on computer backup, depending on the extent of e-commerce activities and other services offered on the Internet, as well as the extent of their customer database.

The company offers the full range of services depending on what level of support the client wants, from basic colocation where customers bring their own equipment and put it in the Worldport data centre, through to fully managed services which can include a two-tier system with databases, web servers and multiple backup facilities in multiple locations. Worldport provides the hardware and software and manages everything on a 24×7×365 basis, including installation and configuration. In some cases, Worldport simply monitors the client's equipment, in others, Worldport also runs its database. Costs run from a modest £1000 a month, but each client's requirements are different and costs are related to the needs of the client. An estimated 80 per cent of the company's business is managed services.

Worldport's Product Marketing Manager, Neil Downing, said there had been a rise in customers looking at their disaster recovery operations since September 11. 'It is important for us to work with the client to understand how quickly they need the information to be available. How long can an individual company afford to be without their data before they go out of business?'

ONLINE BACKUP: NETSTORE

Netstore (netstore.net) offers as one of its online services the 'online backup and restore' service which effects efficient automatic backup to Netstore's secure storage facility from where files can be restored over an Internet or extranet connection. The process is password-protected and with fully encrypted file transfer. Online backup is provided as a hosted service and the company does not need to set up a central infrastructure or obtain skilled staff to support and manage the backup solution. Netstore's storage centre has a capacity in excess of 50 terabytes and the centre is mirrored to eliminate the possibility of data loss.

ADVANCED SECURITY CENTRES: ERNST & YOUNG

As part of its technology and security risk services, Ernst & Young has set up seven advanced security centres to test enterprise security and technology infrastructure across the United States. The centres do not host and administer clients' facilities but

design and test specific enterprise security and technology infrastructure solutions with the latest technologies. The company's 'security agenda' includes intrusion and virus detection, incident responses (incidents stemming from malicious contents or intrusions), privacy, policies standards and guidelines, physical security, protection against theft, vandalism, accidents and physical security breaches, asset and service management, vulnerability management, entitlement management (PKI, single sign-on (SSO), Internet key exchange and business continuity, i.e. planning, reviewing, implementing and testing continuity plans and disaster recovery plans. As part of the service, Ernst & Young's specialists help corporations work out business continuity strategies. The centres also test organizational resilience by testing for weaknesses which may be exploited by hackers.

BUSINESS CONTINUITY DATACENTRES: IBM/TELEFONICA

On April 15, 2002 IBM announced that it had entered into a business continuity partnership with Telefonica Data USA (a subsidiary of Spanish Telefonica Datacorp SA). Under the US$ 90 million three-year partnership contract, business continuity and disaster recovery services are offered to clients, with data being replicated via Telefonica's network. Initially, IBM will support Telefonica's datacentre in Miami. Systems to be installed include servers and DB2, Tivoli and Websphere software. Other datacentres run by Telefonica include locations in New York, Puerto Rico, Argentina, Brazil, Chile, Peru, Mexico and Spain.

THE ROLE OF BROADBAND

High-speed Internet access has developed from the modem via a telephone link, through ISDN, ASDL (broadband) and broadband via satellite, offered by BT. This technology has been one of the key factors in making the provision of colocation and other remote centres possible on a large scale, through the provision of links across countries and continents on a global scale.

ISDN moves data across existing telephone lines at speeds of up to 128 Kbps. It uses digital signals rather than analogue (as used by a normal phone line). ISDN is used not only for fast Internet access but also for an ISDN compatible phone system. It is particularly useful for call centres where fast dialling and clear lines are important. High-speed Internet access is provided by a variety of means. The fastest is broadband. BT offers broadband services via its satellite throughout the UK, which offers fast downloading of up to 500 Kbps. This is almost ten times faster than a typical modem speed of 56Kbps.

ADSL (asymmetric digital subscriber line) technology relies on a network of copper telephone wires and covers 70 per cent of the UK, but it cannot reach remote areas. For average use, ADSL is considerably less expensive than the satellite offering, but satellite broadband will be cost effective for users of large-scale data applications and images.

ADSL is a further development of the ISDN concept, and for customers to use this technology, they need to be located within a radius of 3.5 km of the local exchange, although with the latest extended reach, this distance is now about 5.5 km. The level of service downstream will be up to 500 Kbps, but upstream will vary depending on the distance from the local exchange, between 64 Kbps and 250 Kbps. Speeds may vary according to usage and weather interference.

In November 2001, BT Openworld launched a pilot scheme consisting of a new broadband two-way satellite service for home users and small and medium businesses in Scotland and Northern Ireland. In early 2002, the broadband Internet access by satellite was made available across the UK. Businesses previously out of range of their local exchange which were unable to gain fast-speed Internet access can now install a two-way VSAT satellite dish, which sends and receives data at high speed via a satellite linking to the Internet via the BT Openworld hub. This service does not rely on telephone lines and is always open.

Up to four computers can be connected simultaneously to the satellite broadband service offered by BT Openworld, with a BT VSAT satellite system modem/router connecting directly to the LAN through an Ethernet port. Planning permission may be required to set up the satellite.

CONCLUSION

Facilities provided by independent contractors in colocation centres, server farms and other facilities for remote storage and duplicate data centre facilities are expanding across the globe. Some providers are offering permanent remote facilities for replicating and storing data. Servers may belong to the client or can be leased from contractors. Other providers are ready to step in with facilities, such as mobile disaster recovery units, should a disaster occur. The advantages of colocation facilities to clients are that the centres are purpose built and permanently manned by highly skilled staff, with advanced IT systems and a high level of security, and with a range of services available, spanning from simply storing a company's servers to monitoring and managing backup and online services.

7

Outsourcing/insourcing/ ASP/MSP/SSP/WASP

INTRODUCTION

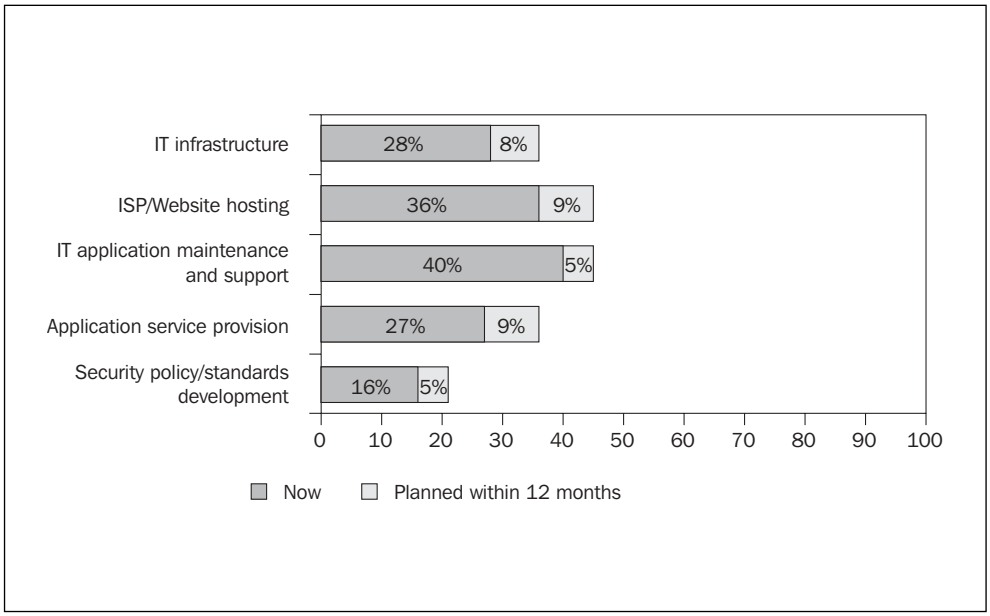
Outsourcing of IT functions and the use of providers such as ASPs to outsource software applications are possible solutions for companies seeking to concentrate on core activities and/or cut costs and alleviate IT personnel problems. In the following, an insight into outsourcing/insourcing as well as the various categories of providers will be given.

TRENDS IN OUTSOURCING

Outsourcing of IT functions was declining for a while, especially following the dot.com crisis, but it has now come back into the marketplace, following a series of high-profile outsourcing deals.

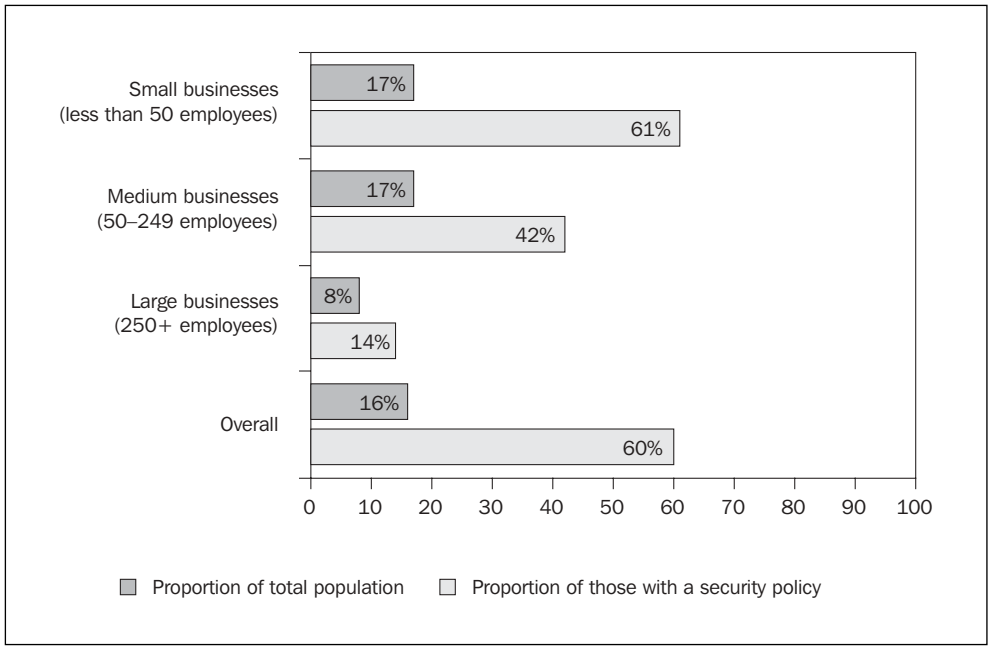
The DTI Information Security Breaches Survey 2002 found that outsourcing is increasingly being used by UK companies, particularly for non-core elements of the business. IT applications maintenance and support top the list of outsourced functions. Figure 7.1 shows the order in which the major IT systems are outsourced. Security policy comes bottom of the list, with 16 per cent. However, results from the previous DTI survey (2000) showed that firms outsourcing their security policy exceeded the total number of firms having any kind of security policy in 2000. Small companies are most likely to outsource their security policy (61 per cent of those with a security policy – *see* Figure 7.2).

Fig. 7.1 **Which of the following significant systems or security processes are outsourced?**



Source: DTI, Information Security Breaches Survey, 2002

Fig. 7.2 **Which UK businesses are outsourcing security policies and standards development?**



Source: DTI, Information Security Breaches Survey, 2002

A report by ComputerWeeklyCW.com (2002) predicted a bright future for outsourcing. According to the study, 56 per cent of the FTSE100 companies have a strong commitment to outsourcing of technology and/or processes. Business process outsourcing (BPO), i.e. outsourcing of entire business processes such as accounting, human relations and customer relations management, is becoming increasingly common. The study also found that the most popular driver for outsourcing was cost saving. Other reasons included impending M&As and the freeing up of capital. Contentiously, the study also claimed that there was compelling evidence that outsourcing can result in an increase of up to 5.3 per cent in a company's share price.

The demand for web outsourcing services was estimated to be around US$ 50 billion in 2002 (Forester).

Outsourcing partners are now playing a more central role than was previously the case. The upswing in outsourcing is driven by the increasing complexity of IT systems and the shortage of IT professionals. New providers have sprung up which are able to offer a competitive advantage to business in that they are able to handle mission-critical IT systems at a lower cost and with fewer problems than the businesses themselves. Outsourcing web hosting can provide a more scalable, flexible 24×7 solution than the companies themselves, without the companies giving up total control of the management of their operations. The new providers of web hosting services therefore need to be reliable and accessible, and need to be able to communicate at board level as well as with existing Internet support staff. They are expected to provide a reliable network backbone and continuous Internet connectivity.

MAJOR DRIVERS OF OUTSOURCING

In considering whether to use an outsourcing provider, the question of skills shortages plays a part. Taking this into account, it makes sense for a company to utilize the services of a provider. In start-up companies, the IT function could be done away with altogether. In existing companies with capital investment in IT equipment already in place, a middle-of-the-road approach could be adopted, where certain IT functions, such as monitoring of equipment, could be outsourced.

Non-core functions

Outsourcing of non-core functions is often done to avoid conflict between the need to invest in core business and the need to increase efficiency. If non-core internal functions are left unattended, overall efficiency can suffer. Since IT backup is vital to an organization's success, this should not be used as a reason for outsourcing. However, the advantages of outsourcing may be such that it should be considered from the point of view of gaining benefits for the organization.

Competitive advantage

IT is a highly specialized area and outsourcing may be a way of gaining access to outstanding capabilities at less cost than if they were to be employed internally. Outsourcing could benefit an organization in terms of competitive advantage. The latest technology will be employed at all times, and the cost of training and keeping up to date is no longer borne directly by the company. By outsourcing, the organization is able to redirect its personnel to focus on the organization's core activities, thus strengthening its ability to compete.

Updating of IT systems

A company may take a decision to outsource its IT infrastructure if faced with a large investment to improve or replace existing infrastructure to keep up to date with technological developments.

Lack of qualified staff

Another driver is often the difficulty of finding sufficiently qualified IT personnel to cope with the increasing complexity of IT operations, networks, etc. A company may also find that its managers are increasingly dealing with IT issues rather than core profit-making operations. As a result, strategic issues go by the board in the increasing involvement with the IT side. The need to focus on core

businesses is becoming ever greater, and the complexity of the IT infrastructure is going the same way, thus resulting in a conflict between the two when it comes to allocation of management time and resources.

Managerial time constraints

The problems in IT can reach such a level that the problems of managing the function are out of control. This may interfere with the allocation of managerial time to other functions and may even impact on the day-to-day serving of customers. By outsourcing, the company will free up management time and its focus will therefore be sharpened.

Disaster recovery

Drawing up disaster recovery plans and testing and monitoring them can take up valuable management time. Outsourcing to experts will ensure that a company gets back online with no major disruption if a disaster occurs.

Survey: top ten drivers of outsourcing

In 2001 the Outsourcing Institute carried out a survey of the top drivers behind today's outsourcing decisions. They were, in alphabetical order:

- accelerate re-engineering benefits
- access to world-class capabilities
- cash infusion
- free resources for other purposes
- function difficult to manage or out of control
- improve company focus
- make capital funds available
- reduce operating costs
- reduce risk.

Through outsourcing, a company contracts out a complete area of operation. Traditionally, outsourcing has been popular in fields such as training and recruitment. System security is a speciality which can also beneficially be outsourced. Outsourcing is becoming a more realistic option as technology advances, IT systems are becoming faster and more advanced, and therefore more complex, and new skills, software and hardware need to be modified and kept up to date on an ongoing basis.

INSOURCING

An alternative solution to the enlisting of outside support is insourcing, i.e. support with an in-house solution as distinct from support external to the company. Such a solution is highly flexible and involves staff, premises, communications, management and supervision.

Insourcing may be the preferred option for several reasons. There may be a high level of pressure on existing staff, cost control may be ineffective, or there may be a need to keep up with technology which the organization cannot fulfil. Typically, insourced services from an insource provider would include hardware and software support, and installation and configuration services. Other services such as disaster recovery and business continuity planning may be included. IT training and hosting services may also be available.

Some providers provide insourcing as well as outsourcing services on a flexible modular basis, with both remote and onsite elements. It is up to the customers to choose the level of service they need, considering factors such as cost, control and core operations. Support can be tailored to the size of the business, to avoid small companies being overcharged for services they do not need.

INSOURCING OR OUTSOURCING?

There are several factors to consider in choosing between insourcing and outsourcing.

- **The cost of floor space.** If space is at a premium, as it is in some city centres, outsourcing may be the most cost-effective solution. Insourcing will take up valuable space, which can be used more profitably for core activities.
- **The cost of employees.** Both insourcing and outsourcing provide people, and the cost element can be compared with the cost of employing staff in one's own company. Parameters such as qualifications, experience and ability, supply of talent in the marketplace and the cost of hiring should be taken into account.
- **Training** is a function which can often be beneficially outsourced or insourced if the equipment for training is in place. It should not be forgotten that training is an ongoing process, best left to experts in the field, and a company may not have sufficient personnel able to devote time to keep up with technological developments.
- **IT investment.** If a considerable investment has already been made in IT, the pros and cons of insourcing versus outsourcing should be carefully looked at from a cost point of view. Factors such as the cost of maintaining and upgrading systems should be examined.

- **Economies of scale.** A company may choose outsourcing due to lower IT costs brought about by economies of scale on the part of the provider and greater budgetary control through predictable costs.

APPLICATION SERVICE PROVIDERS (ASPs)

A growing trend is to contract ASPs to take over the provision of software applications from a remote location via an IP network. This enables companies to utilize the latest software applications available at all times, without themselves having to invest in new software every time a new application comes along, as this is being provided on a continuous basis by the ASP. The client also does not have to employ a full complement of specialist staff to administer the software. Since the ASP will be serving many clients, economies of scale and methods of delivery make the approach cost effective. The cost of buying hardware, such as servers, to run the applications is no longer borne by the organization, since the application services are delivered by the network.

It should be noted that an ASP contract, unlike an outsourcing arrangement, is not a complete replacement of all IT services. Nor is an ASP a web hosting service, although in certain circumstances it may take over this role. ASP services can be supplied by different providers specializing in different fields to the same client, i.e. e-mail, accounting, CSM (customer services management). In the foreseeable future, the ASP market is likely to remain relatively small compared with outsourcing.

The ASP provides the software to a company on an agreed basis, such as rental, based on usage. The applications are hosted offsite and delivered to the user via a network. For SMEs which are restricted on budgets, the ASP is able to offer a wider range of applications than the company would normally have installed if operating its IT in-house.

The provision of ASP services has been made possible through the development in networks over recent years. ASP applications range through basic software, e.g. e-mail, to high-end applications normally reserved for big companies, including backup and restore facilities. As soon as upgrades are released on the market, they are made available to the user as part of the agreement.

The ASP is able to set up the services speedily. This is particularly so if the client is local. The speedy implementation is also not dependent on training the client's staff, which would normally delay the implementation of an in-house application.

As far as budget planning is concerned, the costs associated with an ASP contract are predictable. In addition, the total cost of ownership (TCO) is lowered, and predictable; since no capital outlay is required, capital is preserved.

Due to the expertise of the ASP, downtime due to IT failure or application errors is reduced, thus benefiting the business overall. Availability of the latest software at all times is also a source of competitive advantage, vis-à-vis competitors.

Examples of ASPs include:

- Accpac (a Computer Associates subsidiary), which hosts business solutions, including its Advantage Series (accounting solutions), eTransact (e-commerce solutions) and eCRM (customer relationship management)
- SAP, which provides software worldwide, mainly for the midmarket. With more than 17 000 customers in 120 countries, SAP runs more than 44 500 installations of SAP-tailored industry software packages.

MANAGED SERVICE PROVIDERS (MSPs)

Outsourcing is also referred to as managed IT services or MSP. This form of application service provider manages the IT infrastructure that runs the applications rather than the applications themselves. The services are provided on a remote basis and include monitoring of traffic on sites and security against hackers and other sources of attack.

An example of an MSP is Interliant, which provides managed infrastructure solutions, such as messaging, security and professional services products. Interliant has several large clients, including British American Tobacco. BAT initially outsourced its e-mail system, which had become increasingly complex and took up a disproportionate amount of IT time. The contract was entered into in 1998 and on expiry was extended for a further three years in a deal worth US$ 4 million. Interliant provides a high level of service and has been successful in sorting out e-mail problems such as unwelcome spams and installing virus scanning. In 2000, the service was migrated to London.

Some ASPs are vertical service providers (VSPs), specializing in a particular commerce or industry sector, such as NSB Retail Systems.

STORAGE SERVICE PROVIDERS (SSPs)

The SSP, or storage service provider, provides specialist services in the storage area, along the lines of an MSP.

WIRELESS APPLICATION SERVICE PROVIDERS (WASPs)

WASPs provide applications orientated towards the new generation of mobile, wireless networks, which provide permanent connectivity.

Multiple service providers offer a range of services, including the above online services and other services such as ISP.

CHOICE OF PROVIDER

In taking on outsourcing companies, a word of warning comes from industry-wide key players. Changing environments mean different demands on outsourcing providers and it is therefore important for companies to ensure that the providers are able to be flexible as well as being financially stable. With competition strong in the marketplace, flexibility is particularly important; many outsourcing providers are new to the marketplace and a check-up on the breadth of their services offered and the depth of their experience is worthwhile. The facilities offered by a reliable outsourcing company should include access to established network backbones and professional staff, on call 24 hours a day, the provision of additional bandwidth as and when required and the ability to cope with fluctuations in demand.

As in all business arrangements, a degree of caution should be exercised in entering into an outsourcing contract and to counter the eventuality that the ASP does not perform in the way it was expected, or runs into difficulties, an exit route or break clause should be incorporated into any contract.

MANAGED SERVICES – SURVEY FINDINGS

CMG, a major international IT services and solutions group, provides managed services, with outsourcing expertise developed over many years. The company's clients are governments, oil companies and Internet banks, among others, and the group is quoted on two exchanges, Amsterdam and London. Under its Managed Services programme, CMG takes over the responsibility for managing all or part of a company's application software programme. Its services range from routine support and maintenance to providing the development and production infrastructure for applications.

In CMG's 2001 survey (published 2002), commissioned from Dynamic Markets Ltd, 100 IT decision makers (IT directors, managers, heads of IT) from companies with more than 500 employees were sampled. Sectors represented were finance, government, transport, logistics, commerce, energy and TMT (telecoms, media and technology).

Companies were asked which areas they managed in-house or outsourced to partners. Systems integration was the most commonly outsourced function, with 14 per cent outsourcing some of it and 29 per cent outsourcing all of it. In second place was systems support (13 per cent some of it, 24 per cent all of it). Five per cent did not have any disaster recovery planning, 20 per cent outsourced it and 11 per cent outsourced some of it. IT strategy and planning was rarely outsourced; only 3 per cent outsourced all of it, with 3 per cent outsourcing some of it. For customer support, the figures were 16 per cent outsourcing some of it, 7 per cent all of it and 8 per cent did not have this function.

The sample was also asked to what extent their attitude to managed services had changed, taking into account the current economic climate. Forty-seven per cent of the sample expressed scepticism about managed services, while 26 per cent were positive. There was a shift towards being more open towards ideas from third parties (17 per cent) and as many as 32 per cent said they had become more confident about managing a third-party relationship, while 39 per cent said they had become more confident about a third-party relationship working successfully.

The top three factors in determining a successful managed service relationship were perceived to be:

1. Finding a partner that is a good cultural fit (92 per cent).
2. Finding a partner that understands their business (84 per cent).
3. Having a clear plan for measuring ROI (64 per cent).

The top three success factors for delivering real ROI from a managed service relationship were:

1. Allowing the business to focus on its core competencies (84 per cent).
2. Improving productivity and efficiency (60 per cent).
3. Delivering to an agreed service level (56 per cent).

Pressure to cut costs in an economic downturn was given as the main reason for outsourcing in such conditions. The top three drivers were:

1. Pressure to cut costs (72 per cent).
2. Pressure to improve efficiencies (64 per cent).
3. Lack of necessary skills in-house (56 per cent).

CONCLUSION

Outsourcing, out of favour for a while, is again gaining ground in the field of IT. The consensus is that with the increasing complexity and high-tech nature of IT systems, and the consequent demands on budgets, skill levels and management time, outsourcing/insourcing or the services of an ASP or SSP should be considered as a serious option by large and small organizations alike, taking into account the benefits such as rapid deployment, gains in management time, predictability of budgets, reduced IT downtime and improved backup and restoration facilities.

8

Backup and storage costs/disaster costs

INTRODUCTION

Backup and storage costs are escalating all the time due to changes in technology, as well as the need to store ever more information. But escalating costs do not amount to out-of-control costs, and models exist for predicting costs at various rates of change. Techniques such as business impact analysis are designed to quantify costs associated with disasters in critical areas such as IT systems and backup.

The costs of disasters overall are huge and cannot easily be quantified. Natural disasters such as earthquakes and hurricanes have been top of the list of mega-events, causing billions of pounds in terms of damage and lost revenue, but these have recently been overshadowed in impact by the tragic event of September 11. This catastrophe was all the more unpredictable in scale due to its multi-strike nature in the shape of civilian aircraft turned into missiles, a type of attack never witnessed before.

BACKUP AND STORAGE COSTS

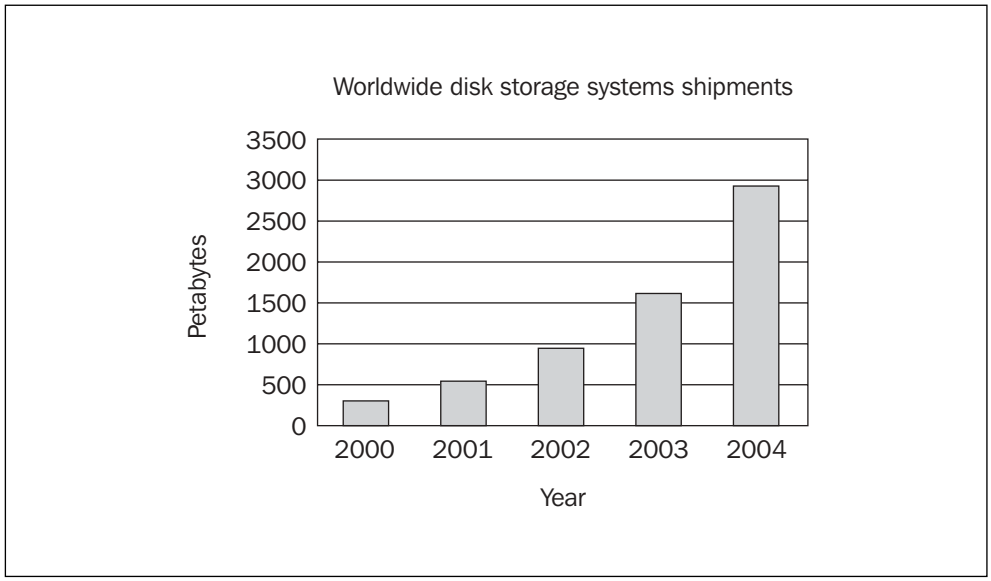
No serious company can be without a storage strategy in today's technologically-oriented environment. With the continued growth of corporate data, a well thought-out storage strategy is the only answer. But apart from storing historical data, investment in storage technology can give a company a competitive advantage, which in the long term is likely to lead to significant gains. A storage strategy is a necessary business practice to be formulated and implemented at board level.

A coherent storage strategy is different from just adding on storage as and when needed. Acquisition of storage should be planned as part of a wider strategy. An important part of this strategy is the cost of acquisition and implementation. The arguments in favour of making the right decisions within the framework of what is economically possible should support the contribution of storage to the future economic potential of the organization, as well as the day-to-day need for storage and the important aspect of avoiding downtime.

The critical dimensions of storage are sometimes difficult to quantify, apart from common-sense arguments such as the need to be able to retrieve data at any time and use them in day-to-day operations. If the business is growing, this need becomes even more paramount, quite apart from the fact that the volume of information coming in or being created by the organization is growing in an absolute sense.

More and more companies are now filing electronically, not only current records but past records as well, and this has increased the demand for storage phenomenally. Figure 8.1 illustrates the growth in storage requirements based on worldwide disk storage shipments.

Fig. 8.1 Storage growth industry estimates



Source: The Evaluator Series, 2001

To judge the soundness of a storage strategy, the various elements should be evaluated in turn. Is the storage solution used the most up to date or the most suited to the needs of the business? What are the scalability requirements of the storage? Are new critical applications likely to be introduced, which in turn take up extra storage capacity? Is there a long-range plan for the adoption of new technologies or the replacement of existing technologies? What is the position as regards the retention of electronic records to meet expected or unexpected legal requirements? What is a consistent storage strategy going to cost?

ROI AND TCO MODELS

ROI models are used to work out the return on investment. However, an ROI investment model tends to be based on individual decisions, whereas a long-term strategy is based on more comprehensive business assumptions. The latter approach is reflected in the total cost of ownership model. An ROI model for storage decisions usually operates with a one-year cycle, although the decisions on which it is based often have much wider implications. The ROI model is used for many IT projects.

In working along the lines of the TCO model, the first step is to identify as accurately as possible the need for storage. What are the main drivers behind the demand for storage? The growth of storage requirements in some organizations has been estimated at 100 per cent per year. Whereas e-commerce even a couple of years ago did not rate as a major factor in storage, it is now a significant

component in the storage equation and this expansion is likely to continue. The length of time the storage is needed is also expanding – banks, for instance, which are major users of online facilities, keep their data for up to seven years.

The two models are shown in Tables 8.1 and 8.2. Note: the two models contain both 'hard benefits' and 'soft benefits'. Hard benefits (or hard dollars) are measurable, whereas soft benefits contain an element of subjectivity. Capital or operational savings, for instance, are viewed as hard benefits, whereas soft benefits may include cost avoidance.

Table 8.1 **Total cost of ownership model**

TCO – total cost of ownership

Typically annual costs of systems/solutions

Elements of TCO include:

- Product costs – software and hardware
  - Implementation costs
  - Training costs
- Administration (operational) costs
  - Support – monitoring and tuning
  - Maintenance (including power, space, etc.)
  - Upgrade
- Data unavailability cost
  - Direct – additional support
  - Indirect – lost business

Source: EvaluatorGroup Inc., Evaluator series, October 2001 issue

Table 8.2 **Return on investment model**

ROI – return on investment

Calculated on a per project basis

Assessment of return on investment for savings or gains from project implementation

For storage decision, this will include:

- Cost of solution (hardware and software plus implementation costs)
- Savings in administration/operations
- Gains in increased business, productivity, customer service, etc.

Usually expressed as a percentage of gain with a payback period of time

Source: EvaluatorGroup Inc., Evaluator series, October 2001 issue

The ROI and the TCO models both contain technology and business elements. The technology side includes the cost of the hardware and software plus associated staff costs, such as operations support and advice. The business side includes availability, or the cost of outages, performance, assessed in terms of response time and the impact a poor response time can have on the business, and recovery time, which if excessive may lead to lost business.

COST OF DOWNTIME

The disproportionate impact of downtime has prompted IT vendors to strive to develop backup systems with high speeds of restoration of data, thus improving the availability of data in percentage terms. Whereas in the early days of backup, the backup process itself meant that systems were down for hours, this backup window has now been reduced to a minimum; many organizations require practically 100 per cent uptime and availability. As far as the vendors are concerned, zero downtime is the latest marketing tool in promoting disaster recovery solutions.

The cost of decreasing downtime can be considerable and the question arises as to whether a small decrease is worth the cost. Erik Ottem, of Gadzoox Networks, estimates that some 80 per cent of downtime is due to systems outages. Environmental causes (fires, floods, power outages, etc.) account for the remaining 20 per cent. Increasing the safeguards against downtime has to be viewed in terms of the importance to the business. According to Erik Ottem, 99 per cent availability translates into unavailability of data for the equivalent of 3.9 days per year. Raising the availability to, say, 99.9 per cent might be disproportionately expensive, depending on the value of the application to the business. The loss of critical applications may cost the business, say, £1 million per hour of downtime, whereas the loss of non-critical applications may cost much less.

The cost of implementing an adequate storage system should be weighed against the cost of downtime of IT systems if disaster strikes. Downtime can have any number of causes, depending on the type and severity of the disaster, but the consequences do not allow for the causes of IT failure. The main threat in the event of downtime remains loss of business or loss of customers and consequent loss of revenue. While sympathy with a company will have some influence on customer loyalty, sympathy can extend only so far and in the end customers may go elsewhere. The reputation of the company is at stake.

A serious instance of downtime may signal to affected parties that the company has not got its backup and recovery systems up to scratch, and can cause loss of confidence not only by customers but also shareholders or potential investors, partners, suppliers, banks and the financial market in general. The interdependence between people and technology is now such that one cannot exist without the other.

A weakening of these elements can have repercussions in the wider marketplace and may affect brand value and market share as customer loyalty wanes.

In the US it has been estimated that the cost of even minutes of downtime can run into hundreds of thousands of dollars. Special software has been designed to minimize the risks associated with downtime, enabling companies to achieve higher availability of data. Network Appliance, for instance, markets SnapMirror for rapid replication of mission-critical information, Snapvault for faster online backup and recovery, and Snaprestore for instant file recovery.

The cost of downtime can thus have serious repercussions and has even translated itself into companies going out of business, as was seen in the aftermath of the Oklahoma bombings on April 19, 1995.

Ontrack Data International, a provider of data recovery solutions around the world, has made an estimate of the average hourly impact to businesses of computer downtime and data loss in the US. Its figures for 2001 are shown in Table 8.3.

Table 8.3 **Impact to businesses of computer downtime and data loss in the US**

Sector	*Average hourly impact US$*
Retail brokerage	6.6 million
Credit card sales authorization	2.6 million
Home shopping channels	110,000
Airline reservation centres	90,000
Package shipping service	28,250
Manufacturing industry	26,761
Banking industry	17,093
Transportation industry	9,435

Source: Ontrack, 2001

COST OF SECURITY INCIDENTS

The DTI 2002 survey found that in most cases, costs from security incidents, including lost business, recovery of data, downtime and staff costs, were only minor (two-thirds of the most serious incidents cost less than £10 000). But some UK businesses in the sample had lost more than £500 000 following a single incident. In a web poll conducted by the DTI (published 2002) more than 7 per cent of respondents had incidents causing a total loss of over £500 000. This

compared with the DTI 2000 survey, where the worst incidents ranged in cost from £20 000 to £100 000. The average cost of incidents was £30 000. The DIT survey estimated the total cost to UK business during 2001 to be in the region of several billion pounds.

UNDER-INVESTMENT IN IT SECURITY BY UK COMPANIES

The DTI 2002 survey showed that compared with what is considered to be a realistic benchmark of 1–5 per cent (up to 10 per cent in high-risk sectors such as financial services), UK companies are under-investing in IT security. Only 27 per cent of companies surveyed spent more than 1 per cent on IT security. Only 40 per cent of businesses evaluated their ROI. This was assumed to be due to the difficulties in carrying out such a calculation, but the DTI maintains that guidelines are increasingly available.

Quite apart from the effect of downtime on customers, the cost of restoring systems to normality through bringing in IT engineers also has to be added, unless a maintenance contract is in existence, as would be the case for large companies, but not necessarily for SMEs. Compared with the thousands of pounds – and in the case of larger companies, millions of pounds – that can be lost due to downtime, the cost of protection against downtime is considerably less, even though it includes measures such as the protection of buildings and their pathways (mains, networks, etc.) through the installation of various protective devices such as lightning conductors, adequate fire protection to meet standards and flood defences as recommended by the authorities. The cost of training personnel to appropriate standards should also be taken into account. Companies are increasingly considering the option of outsourcing disaster recovery and IT functions in general, to gain tighter budgetary control.

THE ROLE OF BUSINESS IMPACT ANALYSIS

The exposure of the company in terms of lost data should be quantified through the business impact analysis, a precursor of the disaster recovery plan and a fundamental first step, although often ignored, in the business continuity plan. The BIA will assess the financial impact and give an indication of how long a business can last after a disaster, or how long the business can cope with having a particular function, such as IT, out of auction. The BIA should clearly illustrate the potential losses in terms of graphs to depict financial information, number of customers that may be lost and potential loss of market share resulting from downtime. The impact on revenue, customer services and possible legal liabilities should be assessed and on this basis a

numerical value can be assigned to downtime. If a speedy recovery from a disaster can be effected, this will obviously reduce costs.

The BIA thus provides a valuable way of projecting the losses that can arise and the need to protect the organization as far as possible against vulnerabilities of an internal and external nature. A risk analysis should also be conducted in association with the BIA, to anticipate and plan for disasters. What would be the likely causes of disruptions from external sources, for instance? Is the company located in a hurricane belt, on a floodplain, or close to a geological fault which could cause earthquakes?

COSTS ASSOCIATED WITH MAJOR DISASTERS

Claims from September 11 together with claims from other major catastrophes, resulted in the largest ever loss to the insurance industry and negatively affected the 2001 earnings of major insurance companies. September 11 presented the insurance companies with an entirely new loss dimension. Losses of such magnitude had hitherto been caused by natural catastrophes such as hurricanes, floods and earthquakes. The trend towards higher losses was further exacerbated due to an increase in risk factors such as higher population densities and higher concentrations of insured values.

Natural and man-made disasters in 2001 resulted in claims of US$ 34 billion worldwide for the insurance industry. An estimated US$ 19 billion was directly attributable to property and business interruption losses from September 11.

In general, losses associated with disasters can run into billions. Lloyds of London announced a projected loss of £3.11 billion for the year 2001, £1.98 billion of which stemmed from the September 11 attacks. Other claims following disasters involved tropical storm 'Allison' and the sinking of the world's biggest offshore oilrig owned by Petrobras, off the coast of Brazil in March 2001. However, Lloyds was confident that 2002 would see a return to profit.

The estimates of the insured loss (all lines of business) from the terrorist attacks of September 11 are outlined in Table 8.4.

Swiss Re also lists the five most costly insurance losses in 2001 in property and business interruption, as shown in Table 8.5.

The cost of total property damage on September 11 was estimated by McKinsey at around US$ 30 billion, with financial services firms accounting for around $4.4 billion (most of their premises were leased). The majority of the property damage was covered by insurance. The cost of business disruption for the financial services industry was estimated at US$ 1.8 billion, due to market closures and dislocation expenses, again mainly covered by insurance. However, the loss of life and intellectual capital was devastating, especially for medium-sized firms such as the bond firm, Cantor Fitzgerald.

Table 8.4 Estimates of the insured loss (all lines of business) from the terrorist attacks of September 11

Lines of business	*Range, in US$ billions*
Property	10–12
Business interruption	3.5–7
Workers' compensation	3–5
Aviation	3–6
Liability	5–20
Other on-life	1–2
Life and health	4.5–6
Total	30–58

Source: SwissRe/Sigma study 'Catastrophes 2001', March 13, 2002, CET

Table 8.5 Most costly insurance losses in 2001 in property and business interruption

Insured loss US$ billion	*In (start date)*	*Event*	*Country*
19.0	11.09.2001	Terrorist attacks, NY and Washington	US
3.2	05.06.2001	Tropical storm 'Allison'	US
1.9	06.04.2001	Floods, hail and tornadoes	US
1.4	21.09.2001	Explosion, fertilizer factory in Toulouse	France

Source: SwissRe/Sigma study 'Catastrophes 2001', March 13, 2002, CET

Hurricane Andrew, which hit the Florida coast in 1992, caused damage estimated at US$ 25 billion and brought insurance claims of US$ 16 billion. Insurance for buildings in hurricane-prone areas is higher than elsewhere, depending on location, type and age of construction (which may be hurricane-proof). In Miami, the premium for insurance of buildings east of Interstate Highway I-95 is higher than buildings to the west of the highway, since hurricanes cause most devastation on initial impact with the coastal areas.

The Kobe earthquake in 1995 caused the most extensive damage to property ever seen. Particularly heavy losses were suffered in the shipbuilding, steel production, chemicals and food processing sectors. Damage to property was estimated at some US$ 137 billion. The Nikkei index dropped 5.6 per cent in one day, but insurance claims were relatively limited, due to the structure of the Japanese insurance industry and the recognition that Japanese exposure to earthquakes is unusually great and many aspects of damage are uninsurable. Also the take-up of insurance was very low.

COST ESTIMATE SURVEYS

Attacks against computer systems in the form of hacking, fraud and viruses have been estimated by the DTI to cost several million pounds a year in the UK, with 80 per cent of large companies having fallen victim to attacks of one kind or another during 2001.

In the US, a survey (March 2001) by the Computer Security Institute showed that 90 per cent of 500 large companies and government agencies surveyed had been exposed to computer attacks during the past year and 80 per cent had suffered financial loss as a result. Almost half the companies in the relatively small sample quantified their financial losses, totalling US$ 455 million. Theft of proprietary information caused losses of US$ 170 million.

INSURANCE

Ordinary insurance policies do not automatically cover theft of computers or damage to computers, but such losses can normally be incorporated in a policy against a higher premium or in a separate policy. Some insurance companies specialize in insuring computers. The most common cause of computer loss is accidental damage, followed by theft and power surges.

New insurance dimension

The multiple-strike disasters on September 11 represented an entirely new loss dimension which did not meet the traditional insurance criteria, and the events have caused the industry to rethink the question of terrorism cover. The costs of downtime and data losses resulting from such disasters are high, particularly in the online retail brokerage and credit card services sectors.

Insurance can offer a valuable contribution to the costs of recovering from a disaster. However, this is not an option that is always taken up. The DTI 2002 survey showed that more than 50 per cent of respondents were not covered for damage arising from security breaches or did not know whether they were covered. Many insurance companies are excluding damage from IT security breaches from their policies and are instead setting up special policies to cover such events. In the DTI survey, only 8 per cent of companies had taken out such a policy.

As far as insurance premiums are concerned, astute negotiations on the part of companies could result in significant discounts on the disaster insurance cover premiums for corporations with enough foresight to have viable business continuity plans in place, thereby significantly offsetting the cost of a major disaster.

CONCLUSION

With costs of backup and recovery solutions rising, companies are keen to find ways of predicting costs and controlling budgets, and more precise methods of estimating IT associated costs are being developed. But the effects of disasters are unpredictable, with the major ones being hugely expensive, as reflected in recent insurance claims. Those organizations with proper procedures for estimating the cost of backup, with insurance in place and supported by proper disaster recovery and business continuity planning are in the best possible position to ensure their survival should catastrophic events occur.

9

Backup and restoration in financial services

INTRODUCTION

The financial services are among the biggest spenders when it comes to the installation of the latest IT technology, including backup systems. In their striving towards being at the cutting edge of technology, they are one of the best-equipped sectors to withstand a disaster. This was demonstrated on September 11 when their backup systems were put to the test, and in most cases passed with flying colours. Their secret weapon, data stored and backed up in remote locations, was in place in the majority of cases. IT vendors deserved part of the credit for the speedy recovery of systems and data. They were at Ground Zero within minutes, offering restoration services, duplicate facilities and support staff.

PIONEERS

For a variety of reasons, financial services firms have been pioneers in installing the latest disaster recovery and backup solutions, along with IT systems in general. Financial data and records are core elements of their business and computer-based transactions are taking over from the human element. Electronic data and equipment have replaced securities and physical handling of currencies and securities. Physical certificates from stock trading are being replaced by electronic entries in paperless trading. In the banking sector, typical computer-led operations include foreign exchange deals, money market and securities transactions, options and loans. Clients are withdrawing money from the ATM network daily and increasingly conducting transactions on the Internet. The storage and retrieval of client records is of paramount importance. Loss of data could result in massive lawsuits from clients as well as huge compensation claims.

COMPETITIVE ADVANTAGE

Having state-of-the-art IT systems is an important weapon in the battle for competitive advantage. Having viewed the Internet with caution in the initial phases, no self-respecting bank is now without a web presence and most offer their customers Internet access to accounts and account movements in the form of statements.

In their ongoing efforts to stay at the forefront of technology, financial institutions are continually installing better IT systems. Scalability, speed of transmission, reliability and security are all at the forefront of their requirements.

For stockbrokers and dealers, speed, accuracy and continuity of trading are of the essence. Downtime can be a catastrophe in terms of loss of trading. The latest backup and storage systems offer immediate restoration of data through incremental backup or mirroring.

EXPOSURE OF BANKS

Systems failures and downtime can cost the banks dearly, since they can incur penalties for late payments by agencies such as SWIFT, CHIPS (Clearing House International Payment System) and Fedwire. Immediate restoration of backed up data is therefore vital to the banks.

With the increasing amount of data storage required, more time is required for systems maintenance. But at the same time customers expect 24×7×365 service, and systems reliability and continuous availability are becoming top priorities. Increasingly, banks are dependent on technology to deliver their services and products, and accordingly the risks to the banks from operational failures are on the increase. The risks are not only transactional, i.e. arising from product or service delivery failures, they can also arise out of non-compliance with rules and regulations.

Risks to reputation loom large. Adverse IT events such as downtime can affect the public's perception of the bank's ability to deliver services. Barclays Bank's technology-related failure to deliver salaries on time into clients' bank accounts before Easter 2002 made national headlines. A computer failure delayed the payments of salaries from 20 000 employers to their employees, and tens of millions of pounds did not arrive in the employees' accounts on time. Matters were made worse when Barclays did not inform its clients about the systems failure until days after the fault had been identified – it appeared that Barclays did not have any plans to deal with an event of this nature. *The Times* asked why emergency teams had not been put to work to solve the problem and why proper backup systems had not been in place: 'With proper backup systems, calamities such as this should be avoidable, or at the least, easily remedied.'

WATCHDOGS

In addition, the financial services firms are subject to the watchful eye of the UK regulatory authorities, notably the Financial Services Authority (FSA) which has extended its regime to cover the entire spectrum of financial services.

With specific reference to September 11 and the ability of the financial services firms to relatively quickly restore their systems, Guy Warren, head of UK banking practice at Unisys, explains the reasons: 'The financial services community was badly affected by the event of September 11 in New York, but was able to restore IT services relatively quickly and effectively to allow their businesses to continue trading. Other organizations in the same building were not so fortunate and have lost vital and valuable IT information for ever. So why the difference?

'Well, it is no coincidence. The financial services community consists of regulated bodies which can only perform their business with a licence. Part of

getting and keeping that licence (to look after your money) requires that they demonstrate every year that their IT systems are suitable. This means that they are audited internally and externally each year to ensure that their systems are of a suitable quality (minimizing downtime), are secure against backing and fraud and – importantly on September 11 – are proof against disasters, including fire, flooding, natural disasters and terrorist attacks. The better of the financial institutions perform "fire drills" to practise recovering from given scenarios, whether it is loss of data or loss of a facility. Modern storage systems (e.g. EMC) are very capable indeed, allowing data to be mirrored in real time to two locations 100 km apart so that both sites are effectively live and able to support the business. Archiving and backup solutions (e.g. Storagetek) are very sophisticated and allow retrieval of data from minutes, days, weeks, months or years ago to enable the audit trail to track down suspect or illegal action. All of this is required to run an IT department in a regulated company. It comes with a high price tag, which much of the time feels like an expensive overhead, until the day you need it.'

Guy Warren pointed out that backup recovery systems are expensive but essential to run a regulated company, and practising the recovery of data or facilities is an important preparation for disaster.

COMPLIANCE

With a strict regulatory system in place, financial services should above all ensure that their compliance procedures cover as many eventualities as possible. The strict regulatory regime in the UK makes it incumbent upon firms to install and maintain systems that are disaster-proof and able to run with as little downtime as possible. In the case of banks, the banking code stipulates that information should be revealed in certain circumstances and that banks' data are stored for many years.

Contrary to widespread belief, the law does not require banks to keep records as a general rule, but there are specific requirements relating to the retention of records for money-laundering prevention or tax purposes. Banks also need to retain records of dormant accounts until the funds are claimed. E-mails should be retained, although many companies would rather delete them, especially since it has become commonplace for e-mails to be admitted in evidence in the courts, as was seen in the Microsoft Antitrust Trial. A company in the United States, Electronic Evidence Discovery, employs some 50 people to dig out e-mails required for various purposes.

UK laws and regulations covering financial services as well as other companies include the following.

The Companies Act 1985

Under this law, companies have an obligation to keep their accounting records. If records are held electronically, they should be adequately safeguarded.

Regulation of Investigative Powers Act 2000

This law applies to communications services providers and stipulates that law-enforcement authorities should have a right of and access to interception of records, including requests to decrypt information held.

Computer Misuse Act 1990

This Act targets unauthorized access to or modification of computer material and makes certain categories of intrusion and alterations of data held on the Internet illegal. More specifically, the Act makes it an offence if an unauthorized person causes a computer to perform any function with Intent to secure access to any program or data held in any computer, if the access he or she intends to secure is unauthorized, and if he or she knows at the time that this is the case.

Copyright, Design and Patents Act 1988

This Act contains provisions regarding the use of illegal software. In the US, retention of data is mandated by the Inland Revenue and local and state laws.

The Data Protection Act 1998

Organisations such as credit agencies holding personal records on file should be aware of the principles of the Data Protection Act in the storage of data. The Act relates to the rules for disclosure of individuals' personal data held by an organization. One of the principles of the Act is that data should not be stored for longer than necessary. Information relating to a person's credit record, for instance, should not be kept for longer than six years by credit agencies.

EU directives

Other regulatory provisions on the statute book or in the pipeline include a series of EU directives in the e-commerce field, including the e-commerce directive No. 00/31/EC. The directive was passed in June 2000 and covers information society

services provided by electronic equipment, both business to business (B2B) and business to consumer (B2C), including services provided free of charge and interactive online shopping. Sectors covered include online financial services and online professional services (lawyers, accountants, etc.).

A new directive on distance selling of financial services has also been agreed by the EU Council of Ministers, but in 2001 was not yet on the statute book. The Distance Selling of Financial Services directive deals with the marketing of financial products, such as credit cards and pension plans, via the Internet, phone or fax as well as direct mail. The directive bans inertia selling to consumers. Under an opt-in rule, companies would also no longer automatically be able to use unsolicited e-mail to market their products.

MISUSE OF FINANCIAL SYSTEMS

Despite all the regulatory safeguards, there were suspicions that the September 11 terrorists had taken advantage of the financial system prior to the attacks by transferring huge sums of money for their military operations from one country to another. This was thoroughly examined by the authorities, including the Financial Services Authority in the UK, and a number of accounts held by suspects were frozen. Laws on money laundering were strengthened.

The Turnbull Report (UK) 1999

The UK Turnbull Report on the Combined Code of Corporate Governance tightens the corporate net as far as business risk management is concerned. The report is not limited to financial companies but addresses all companies in the UK, particularly listed companies. A guide to the code has been published by the Institute of Chartered Accountants in England and Wales, with the blessing of the London Stock Exchange. The guidelines indicate that a company's internal control systems should:

- be embedded within its operations and not be treated as a separate exercise
- be able to respond to changing risks within and outside the company, and enable each company to apply it in an appropriate manner related to its key risks.

Companies' control systems should ensure the safeguarding of shareholders' investments and company assets, and an annual review of such control systems should be carried out. The focus should be on risks to the business, and the responsibility for risk control should be vested in the board that is ultimately responsible for internal controls.

VULNERABILITY

The financial services industry is particularly vulnerable to attacks generated by terrorist and other hostile entities. Financial service companies usually maintain a high profile as a sector and tend to concentrate in city centres in high-rise buildings clustered together. The devastation caused by terrorist attacks is therefore all the more total, and the cost in terms of loss of human life, equipment and buildings enormous. The targeting of financial centres above all manifested itself in the attacks in the City of London and Docklands and against the WTC in New York.

UK bombings

Disasters through terrorist attacks are not unfamiliar in the UK. The bombings in the City and Docklands in the 1990s caused many firms to tighten up their backup procedures.

Multiple strike terrorist attacks – September 11

In the US, the financial services firms hit by the multiple strikes on September 11 were among the elite. With a presence in the two collapsed towers were Morgan Stanley, Lehman Brothers, Cantor Fitzgerald, Dun & Bradstreet, Keefe Bruyette & Woods and many foreign finance houses. Although not its main location, NYSE also had offices on the site. In the surrounding blocks in the complex were JP Morgan Chase, Deutsche Bank, Charles Schwab, CSFB, Salomon Smith Barney, American Express Bank, Standard Chartered Bank and others. Goldman Sachs and Merrill Lynch had offices in blocks adjoining Ground Zero.

Hardest hit were Cantor Fitzgerald, Fred Alger Management Inc., Sandler O'Neill & Partners and Keefe Bruyette & Woods. Between them the firms lost almost a third of the total number of people who died in the attack.

With the two towers collapsing, computer systems were lost. The SEC whose office dealt with cases under investigation, lost data on cases relating to insider trading. Keefe Bruyette & Woods lost all its physical files, apart from the appalling loss of 67 of its 220 employees.

But when it came to backup, the major financial services firms had their house in order, with firms immediately posting reassurances on their Websites that clients' records were safe. The biggest problem turned out to be associated with the loss of employees, a factor that had not been sufficiently taken into account in disaster recovery plans which had hitherto been centred on single terrorist attacks and other less extensive events.

Information service provider Reuters' data system on the 12th floor of the North Tower, serving 3000 clients, was completely destroyed and many of its customers lost key IT infrastructure. Reuters responded immediately to the crisis

by setting up overnight a secure private virtual network for clients and providing temporary mobile phones to clients who had had their terrestrial connections disrupted. The rescuers team in Geneva worked through the night to provide thousands of clients with access to an online replacement market data system, allowing them to do business the day following the attacks. Most clients had been reconnected when the main markets reopened the following Monday.

Keefe Bruyette & Woods, which lost more than a third of its staff, including many traders and analysts, reportedly managed to show an increase in profits (undisclosed) for 2001 and even moved up in the 2001 M&A rankings.

Cisco helped Cantor Fitzgerald get back onto its feet by rewiring its emergency offices in New Jersey, without charge. Six months later, Cantor had regained its dominant Wall Street position as a bond-brokerage firm, despite losing some of its business, and was making progress helped by eSpeed, the electronic trading arm which is 52 per cent held by Cantor.

Six months after the attacks offsite backup systems had expanded and some of the dislocated companies were beginning to return, although according to online broker Tenantwise.com, only 17 per cent of the executives displaced had returned to the area. Companies that had returned or planned to come back included the Bank of New York and Merrill Lynch, Dow Jones and Deloitte Touche Tomatsu. Other firms, including Keefe Bruyette & Woods, Lehman Brothers and Morgan Stanley, had permanently relocated.

TECHNOLOGY LEADERS

The pioneering spirit and high spending power of the financial community, as well as the mission-critical nature of stored data, the need to stay ahead of the competition and pressures for transparency and availability of information from regulatory bodies, have combined to place the financial firms at the forefront of technology, with state-of-the-art IT systems and sophisticated remote backup and restoration solutions. As a result, the members of the financial services community are better equipped than most to withstand outside attacks, but unfortunately this also makes them an attractive target for infrastructure attacks by terrorist and internal threats by subversive staff, not to mention the opportunistic outsider beguiled by the prospect of stealing untold millions.

DEALER ROOM RECOVERY SERVICE

One of the specialized recovery services available to the financial services industry is a fully equipped dealer room recovery facility, such as that offered by Compaq. The dealer room recovery centre consists of a fully functional dealing room and

back office facility. The rooms are fully equipped with Reuters (SelectFeed Plus), Telerate Knight Ridder, ICV, Bloomberg, Bridge data information feeds, voice recording, dealing controllers and Reuters Triach. Personal trader workstations are on every desk. These are available as a stand-alone or as an integrated solution.

CONCLUSION

Financial services have at all times been highly enthusiastic when it comes to new technology and have spent huge sums on pioneering the development and implementation of the latest technology in backup and storage, high-speed, wide-reaching networks and sophisticated applications. The industry is particularly dependent on electronic storage of mission-critical data, information and numerical records, and at the same time is tightly regulated. Financial services therefore need to have their IT systems in place and up and running on a continuous basis. All these factors have combined to place the financial services right out in front when it comes to IT backup and restoration systems, and as such the sector is more resistant to disasters than most. Unfortunately, these companies are also prime targets for catastrophic events such as terrorist attack, due to their high profile and tendency to cluster together in financial districts.

10

The backup and storage industry players and their products/services

INTRODUCTION

This chapter gives details of some of the disaster recovery/backup solutions vendors and their product lines. Some vendors are household names, others are specialists in products of particular interest from a technology point of view.

INDUSTRY TRENDS – VENDOR ALLIANCES

Normally competitors, the big IT companies have recently shown signs of collaborating in their increasing use of partnerships and alliances in marketing their systems and in their growing acceptance of interoperability standards for components and equipment.

Alliances and co-operation within various IT segments are increasingly making headlines. The new joint ventures and collaborative agreements are designed to meet stiff competition in the home market and abroad. In March 2002 for instance, Hitachi and Mitsubishi Electric Corp. announced the merger of key segments of their semiconductor businesses. Toshiba and Matsushita Electric Industrial set up a joint venture in 2001, for their flat-panel screens for notebook computers. In April 2002 IBM announced a joint venture with Hitachi (majority-owned by Hitachi), under which IBM would transfer its hard drive business to Hitachi for the two companies to jointly develop advanced storage systems for major corporations.

SEPTEMBER 11 – VENDOR ASSISTANCE

But even in a world where competitive advantage counts for everything, the human face of business shone through following the September 11 attacks in New York. The scale of IT damage from the terrorist attacks was considerable. Out of 104 IT locations, 23 were seriously impacted or inoperable. One firm was reported to have its offices in one tower and its backup system in the other. Others suffered extensive losses. The SEC reported the loss of data on insider trading cases and other investigations. Keefe Bruyette & Woods lost physical files. Law firms reported extensive destruction of clients' records.

In an extraordinary display of support and co-operation, the big IT vendors came to the rescue of their clients. Within hours of the disaster, IT suppliers EMC, IBM, Veritas, Sun, HP, Compaq, Oracle and Microsoft formed an alliance to assist their clients. Others, such as Comdisco, bought by SunGard on November 15, 2001, offered premises and facilities to clients. Reuters set up a secure private virtual network for clients and established an instant replacement market system.

As a result, although the financial services community in New York was badly affected by September 11, with the support of their suppliers, they were able to restore their IT systems fairly rapidly and continue trading.

MAJOR PLAYERS

Below is an outline of some of the major players in the backup and storage industry and their products/services.

IBM

IBM is one of the IT pioneers, spanning the entire range of IT hardware and software solutions. Lately, the company has developed an open business model, allowing networks to be built according to customer specifications. IBM's open storage solutions include integrated modular technologies, embracing disk, tape and storage networks, and optical disk storage media. The company has recently (June 2002) launched NAS, SAN and SCSI over IP (iSCSI) products and is supporting the setting up of an iSCSI standard. It has also marketed the 200-I, a storage box allowing LAN users to pool storage. Its new Total Storage Proven Solution relies on configurations pre-tested for interoperability and incorporates products from numerous vendors, building solutions with the latest technology storage platforms. With some IBM clients having hundreds of servers, all requiring storage, IBM is promoting the concept of server consolidation.

In January 2002 IBM was pronounced the leader in contributing to 'Intelligent enterprises' (by *Intelligent Enterprise* published by CPM media). Such enterprises employ strategic IT applications solutions for the purpose of turning data into intelligence. Intelligent enterprises use data gathering to create competitive advantage and thus achieve greater returns on their IT investments. IBM was named as industry leader due to its strength in key technologies and leadership in hardware platforms, open systems and storage. Also selected among the 'top dozen' were, inter alia, Microsoft, Siebel Systems, Veritas and Intel.

Tivoli

Tivoli, formed by former IBM employees in 1989 and bought by IBM in 1996 for US$ 743 million, is a prominent name in the disaster recovery solutions field. Its systems management software helps companies manage storage, security, availability and performance. Tivoli is one of IBM's key software group brands.

Cisco

Cisco Systems is a world leader in networking via the Internet. Its technologies include advanced routing and switching, optical networking, wireless and storage networking, security, broadband and content networking. The company was formed in 1984 by a group of computer scientists from Stanford. Cisco's solutions are the basis for most large commercial networks and also for SMEs.

Its networking solutions are based on a cost-effective infrastructure spanning data centres, MAN and WAN. It operates an open standards-based architecture (AVVID), which gives customers universal access to storage solutions and products. Joint storage solutions with partners include storage over metro optical, storage over WAN, and network-attached storage.

Dell

Dell is boosting its presence in Europe in its aim to expand its network server business. An increased number of technical consultants will advise clients on large storage installations. This expansion follows Dell's October 2001 agreement with EMC of Massachusetts, developer of storage solutions. In terms of network server sales, Dell is currently number one in the US, with an 18 per cent share of US network server shipments (according to IDC at the end of 2001). Compaq is the leader in Europe, the number two storage market, with Dell holding only 10 per cent. Worldwide, Compaq holds a 26.4 per cent share of network server shipments, compared with 19.29 per cent held by Dell.

Computer Associates

Computer Associates International Inc. (CA) is a leading software company. Founded in 1976, CA serves 99 per cent of the Fortune 500 companies in more than 100 countries. The company became the first to meet the high industry standards of the ISO9002 quality certification.

CA's products and techniques are divided into three categories: process management (for seamless management of businesses processes), information management (for the management of business-critical information) and infrastructure management (for the management of core infrastructure and keeping e-business applications up and running and secure). CA markets solutions across these categories, in storage, security, enterprise management, application life cycle management, data management and application development, as well as portal and business intelligence.

Compaq

Compaq, in a takeover battle with HP, launched in 2002, its enterprise storage virtual array system priced up to US$ 300 000. This launch is also aimed at capturing a slice of EMC's market. According to a study carried out by IDC, Compaq was the market leader worldwide for major indicators of storage sales, including server-based storage revenue share and growth revenue in 2000.

Founded in 1982, Compaq provides a wide range of information technology services and software solutions. It markets enterprise and computing solutions, as well as fault-tolerant business-critical solutions and products for personal use in more than 200 countries directly or through marketing partners. Its FC-IP (fibre channel – Internet protocol) enables the implementation of global data replication networks. The SAN-based business continuance solution now marketed by Compaq allows users to implement solutions extending across cities, countries or around the world. In September 2001, Compaq linked the new technology-based SAN across three continents. Its SANworks data replication manager (DRM) solution offers customers greater flexibility in managing their business continuance systems and enables remote replication of data in real time. The SAN solution offered by Compaq is disaster tolerant, with no single point of failure.

Hewlett-Packard

Hewlett-Packard (HP), in merger talks with Compaq at the time of writing, was at the forefront of the development of digital advanced tape (DAT) technology. The company has since gone in for linear tape open (LTO) technology. The proposed merger with Compaq, if it proceeds, is likely to impact other players in the field, such as Sun Microsystems.

EMC Computer Systems

EMC is one of the leaders in providing storage systems solutions but has recently faced tough competition from IBM. It is now focusing on the growth opportunity of storage by supporting interoperability, which enables clients to use storage equipment from one supplier on servers from another.

SUN Microsystems

Sun works with Hewlett-Packard to provide storage solutions from other suppliers such as Hitachi Data Systems. Through such partnerships, the customer ends up with one supplier but a choice of products. Sun has announced a complete range of storage software and subsystems named the Storage Open Architecture. As a follow-on to its Sun Open Network environment, the new architecture is set up as a family of integrated storage management facilities.

Brocade

Brocade (Brocade Communications Systems Inc, Nasdaq: BRCD) is in a dominant market position as a provider of intelligent platforms for networking storage and is widely accepted by many companies as the preferred provider of this type of equipment. The company's networking foundation for its SAN solutions can span up to 100 km over MANs. Its product range, the Brocade SilkWorm® family of fabric switches and software, is designed to optimize data availability and storage and server resources in the enterprise. Brocade claims that its solutions simplify the implementation of storage area networks and reduce the total cost of ownership of data storage environments, together with enhanced efficiency.

The SilkWorm 3200 is the latest in a line of 2 Gbit/sec fabric switches based on the Brocade Intelligent Fabric Services Architecture. Promoting the SilkWorm 3200, Jay Kidd, Brocade Vice President of Product Marketing, outlined its strong points: 'The SilkWorm 3200 provides the industry's most cost-effective entry point available today for companies moving to storage area networks, ideally suited for small and medium business SAN requirements, and enterprise departmental solutions such as server clustering. The SilkWorm 3200 now extends the Brocade 2 Gbit/sec intelligent storage networking platform from the entry level to the enterprise, helping Brocade SAN customers to further optimize their IT resources and reduce the total cost of ownership of their storage environments.'

Brocade claims that by using its solutions, companies can simplify the implementation of storage area networks, reduce the total cost of ownership of data storage environments and improve network and application efficiency.

Brocade's latest offering is the SilkWorm 12000 Core Fabric Switch enterprise storage networking platform. It is said to be the industry's only 2 Gbit/sec modular fabric system.

In April 2001 Brocade completed the installation of a storage area network to support the operations of Halifax, one of the largest mortgage lenders in the UK. The SAN created a disaster-tolerant environment for critical financial data, with the deployment of more than 50 SilkWorm fabric switches in one multi-fabric SAN, spanning servers and storage solutions from multiple vendors. The new network was deployed in conjunction with Hitachi Data systems, one of Brocade's partners in the UK.

Storagetek

Storagetek (founded in 1969) is a world leader in virtual storage solutions for tape automation, disk subsystems and storage networking. The company has 7800 employees spread over 50 countries and 22 000 customers worldwide. Storagetek concentrates on serving the finance, insurance, telecommunications, government, e-commerce and manufacturing sectors. Revenue in 2001 was US$ 2.5 billion (50

per cent US, 50 per cent international), with 67 per cent derived from storage sales and 33 per cent from storage services. US$ 244 million was spent on R&D in 2001.

Storagetek is well known in the industry for providing high-performance, flexible storage solutions with maximization of existing storage and the ability to add new storage easily. A producer of 'silos', the company has concentrated on the mainframe environment, and often the entry-level storage users find its products too costly. It has now moved into open systems. Its proprietary tapes include the 9840, a high-performance tape with a data transfer rate of 10 MB uncompressed. The high-performance, high-capacity tape T9940 has a native data capacity of 60 GB and native transfer rates of 110 MB/sec. They are available as fibre channel drives.

In the face of predictions that tape has come to the end of its run, Storagetek is valiantly defending the product. It provides reliable, uncorrupted backup, at a reasonable price, and is suitable for large-scale use such as government technology operations.

Another product, SN6000, virtualizes tape storage, obviating the need for configuring every host every time a new tape drive is added. The SN 6000 eliminates unnecessary downtime and reduces administrative overheads. The SN6000 provides storage for a whole array of different servers. Pat Margin, President Chairman and CEO of Storagetek, explains: 'If you have 200 different servers, some built by Unix, some by Sun, some IBM, some HP and some NT servers, the SN6000 will provide a storage area for all the servers so that each server treats the storage area as its own.'

He predicts: 'The demand for storage is going to continue unabated, even in a slowing economy. The manner in which we see storage will be different from what it is today. There will be more and more storage accessed remotely. There will be more storage providers. Storage will continue to be a challenge for a lot of companies which will turn to professional people to manage their storage environments. There also will be storage technologies like holograms that could get a foothold in about five years.'

In April 2002, Storagetek announced an alliance with LSI Logic Storage Systems (a subsidiary of LSI Storage Corporation), to offer an alternative to existing suppliers in the open storage market.

One of Storagetek's customers in the UK is Barclays, which over the past two years (2000–1) has introduced storage virtual tape in its data centres to support its tape data storage requirements over the next five years.

Seagate

Seagate entered the storage network market at the end of 1999 when it acquired Xiotech in a stock acquisition deal worth US$ 360 million. It is now one of the

world's largest technology companies. Starting as a provider of disk drives in 1978, its core technology is now storage technology. Its markets for storage solutions range from personal through SMEs to large enterprises. It is the world's largest manufacturer of disk drives and magnetic disks and provides the highest capacity disk drive in the world (2002) (180 GB, 3.5in drive).

Fujitsu

Fujitsu is a US$ 50 billion company, with offices in more than 30 countries. Fujitsu has shifted its emphasis from hardware products to software and services, and its storage interests cover both sectors. The group is entering into partnership to produce single storage solutions incorporating partnership products. Its products include SAN components, RAID (redundant array of independent disk) systems, optical disks, tape drives and archiving libraries.

Softek

A subsidiary of Fujitsu, Fujitsu Software Technology Corporation (Softek) is one of the world's leading software management companies, providing solutions to global companies which ensure high availability (HA) of critical data through simplification and optimization of data resources in a risk-reduced environment. The Softek software conducts storage management across different storage applications regardless of vendors and platforms. Its storage virtualization software, an infrastructure product, eliminates the boundaries between storage hardware and servers and creates open network storage pools for SAN devices from different vendors. The extra capacity is thus available wherever it is needed rather than being tied to a single server. Storage resource management is implemented through the Softek Storage Manager software, which ensures permanent availability of critical data through the provision of the relevant management capabilities.

Softek Sanview, a resource management product, maps and displays the connections of SAN-connected devices so that outages can be diagnosed and avoided. Through its Softek DR Manager, a data management product, Softek speeds up data recovery in case of disaster by identifying critical data and prioritizing data recovery.

Hitachi

Storage hardware and software solutions are sold through Hitachi Data Systems (HDS), founded in 1989 as part of Hitachi Ltd's information systems and telecommunications division. This division contributed US$ 27.8 billion, or 32 per cent of Hitachi Ltd's total revenues for the year ended March 31, 2001. Clients include more than 50 per cent of the Fortune 100 largest companies, with banking

and telecommunications sectors figuring strongly. The company's headquarters is in Silicon Valley, California. It has operations in 170 countries and is strong in the emerging economies of South-East Asia and Eastern Europe.

Hitachi offers storage solutions for complex enterprises, supported by a network of strategic alliances. The company emphasizes the need for a reduction in complexity and the cost of storage management, at a time when storage growth is unprecedented and unpredictable.

The company delineates a set of key requirements for efficient storage solutions, with easier data sharing and lower costs:

- scalability and capacity growth without disruption
- 7/24 availability
- automated performance tuning
- ability to pool and manage large quantities of data
- open-source connectivity – connect any server to any storage system through storage networks
- rapid recovery and/or restart of applications when the unforeseeable does happen
- service for planning and deployment of consolidated storage networks
- centralized management and responsive service and support to ensure maximum uptime.

Hitachi claims that its Freedom storage systems, software and services can reduce per megabyte administration costs by up to 35 per cent, with a substantial increase in ROI.

Sony

Sony is a broad-spectrum manufacturer of audio, video, communications and information technology products and is a leader in DVD technology. Sony aims to become a leading personal broadband entertainment company in the 21st century. Sony broadcast and professional data storage division (Europe) offers end-to-end storage solutions and Digital Tape Format (DTF) technology with high-capacity, fast data transfer rates. Its other dominant technology is AIT (Advanced Intelligent Tape).

With the information market being given an extra fillip through the introduction of broadband networks, Sony has announced the introduction of DTF-2, a tape storage series with a record transfer rate. The series is aimed at large corporations and has a storage capacity of up to 518 GB per cassette and a transfer rate of up to 40 MB/sec. This technology has already been used in the professional broadcasting industry. In 2003, DTF-3 tape drives will be available, with a native capacity of 550 GB and a data transfer rate of 50 MB. Another

product, the DTF-4, is scheduled to be launched two years later. This product will offer 1000 GB of native capacity. DTF is positioned as the replacement for entry-level and mid-range tape technologies such as DDS and DLT. It offers a suitable migration path for the many users of DDS.

Sony also offers tape libraries. Its DMS-B150L library system is based on the DTF format and combines capacity, throughput and rapid access, offering an incremental expansion path. The library can offer up to 250 large-format DTF cassettes, with a total capacity of 30 TB (or 77.7 TB compressed), scalable up to 128 TB. The robotics can handle an average of 360 cassette exchanges per hour. File access time is less than a minute for the large-size DTF cassette. Another library system which can be shared by multiple host computers is the DS8400 in the Peta Site range.

Veritas

Veritas, one of the top ten software companies in the world, with a turnover of US$ 1.5 billion, specializes in storage management software for disaster recovery, data protection and storage virtualization. Veritas software solutions are used by many large companies across the world, providing interoperability across different applications, servers, hardware and storage applications.

Legato Systems

Legato delivers worldwide software solutions to assist business continuance through automation with application ability and storage management solutions.

Quantum

This NYSE quoted company, founded in 1980, is a leader in network storage systems and the world's largest supplier of tape drives. Its DLT format was successful for a decade, but its automation products were limited, and a new company, ATL, jumped in and supplied autoloaders and libraries for Quantum tapes. Quantum then took over ATL and the combined company, Quantum/ATL, now offers an extensive portfolio in DLT automation. It has an office in Hampshire and headquarters in the US (California).

Comdisco

Comdisco, whose storage assets were acquired by SunGard in 2001, supplies business continuity services and web hosting services. Founded in 1969, Comdisco is now an industry leader, with more than US$ 4.5 billion in revenue and over 4000

employees, with offices in Asia, Europe and North and South America. As a full service provider, Comdisco assists in planning, creating, implementing and managing availability solutions. Services include contingency planning, data protection and restoration capabilities, as well as web hosting and recovery services.

One of Comdisco's clients, Royal & Sun Alliance, the international insurance group, advises clients on good practice, as well as on observing business continuity practices. To protect its diverse systems across the world, Sun Alliance implemented Comdisco's Work Area Recovery programme. The need for such a programme became particularly evident in the late 1990s when one of the company's largest sites was severely damaged in Manchester by a bomb.

Tandberg

Tandberg Data is a leading Norwegian manufacturer and supplier of tape information storage products. Its products are based on SLR (scalable linear recording) and DLT linear technology platforms. The affordable SLR7 tape drive for NT and Unix is a 20/40 GB solution. The new generation Super DLT (S-DLT) drive offers 110/220 GB. Tandberg also offers secondary storage products based on tape drives, libraries and autoloader. The DLT VS80 tape drive (40/80 GB) is the world's first half-height tape-drive product.

Tandberg targets the small and medium sized-markets with cost-effective products that are scalable and reliable. The company is represented in major countries around the world, including the US, the UK, France, Germany and Japan. Tandberg is traded on the Oslo Stock Exchange.

Dantz

Dantz Development, a privately held corporation headquartered in California, has been developing software since 1984. Its market for affordable backup software is primarily small and medium businesses. Its Retrospect Backup product, which automatically combines a full backup with subsequent incremental backup, results in reliable restoration and savings in terms of time and space.

NEC International

Founded in 1991, the NEC Corporation introduced the well-known Packard Bell brand and consists of the assets of Packard Bell and the NEC Corporation. From 2000, NEC became known as NEC International. The company delivers mobile, desktop and server computer solutions. Packard Bell is aimed at the consumer market. NEC's corporate structure is divided into three companies: NEC Networks, NEC Solutions and NEC Electron Devices.

INDUSTRY ASSOCIATIONS

The storage industry and disaster recovery/business continuity profession has set up a number of associations to promote its strategies and assist its members.

Storage Networking Industry Association (SNIA)

The SNIA was formed in 1997 as a non-profit trade association to promote storage networks and ensure that the networks become 'complete and trusted solutions across the IT community'. The SNIA's vision is as follows: 'The SNIA is the point of cohesion for developers of storage and networking products in addition to system integrators, application vendors and service providers as the world computer systems market embarks on the evolutionary journey called storage networking. The SNIA is uniquely committed to delivering architectures, education and services that will propel storage networking solutions into the broader market. Storage networking represents the next step of technological evolution for the networking and storage industries. It is an opportunity to fundamentally improve the effectiveness and efficiency of the storage resources employed by the IT community.'

The SNIA Europe (SNIAE)

The SNIAE is part of the SNIA and was launched in 2000 to promote the storage industry within Europe. The purpose of the SNIAE is distinct and its mission includes becoming the central point of contact for European storage networking vendors and IT industries and promoting the acceptance of storage networking solutions among vendors, developers, integrators and IT professionals, as well as delivering education and information for storage networking vendors and the IT community.

The Fibre Channel Industry Association (FCIA) Europe

The FCIA is a non-profit-making body for the promotion of fibre channel through the development of the European market, the Middle East and Africa through initiatives and member interaction. Members include software and hardware vendors, resellers, analysts and systems integrators. Founded in 1998, the association has 100 members. The organization works with standards organizations and participates in exhibitions, conferences and other events.

The Business Continuity Institute (BCI)

The BCI, set up in 1994, has over 1100 members in 32 countries and aims to promote the highest standards of professional competence and commercial ethics

in the practising of business continuity services by its members. Its mission is to promote the art and science of business continuity management. Its aims include the definition of professional competencies expected of business continuity professionals and the provision of an internationally recognized certification scheme for the profession.

The Disaster Recovery Institute International

The US-based Disaster Recovery Institute International is primarily an educational organization with the aim of providing a body of professional knowledge in business continuity planning/disaster recovery. Certification of qualified individuals is available for MBCP (Master Business Continuity Professional), CBCP (Certified Business Continuity Professional) and ABCP (Associate Business Continuity Planner). The common knowledge base of the Institute is claimed to serve as the industry's best practices standard, and training courses are held for planners worldwide.

The Computing Services and Software Association (CSSA)

The mission statement of the CSSA is as follows:

- To accelerate industry growth and prosperity.
- To present our industry's agenda to government and the private sector.
- To raise media awareness of the importance of our industry.
- To build our list of industry contacts and personal expertise.

The association lobbied the Chancellor of the Exchequer for concessions for the IT industry in the 2002 Budget.

CONCLUSION

Vendors of backup and storage solutions range from giants such as Compaq and IBM to the more specialized suppliers such as Tandberg. The backup and storage sector is feeling the recessionary pinch but is doing better than other segments of the IT industry. To retain market share, vendors are adopting open systems, interoperability and common standards, and are consolidating their position through alliances and partnerships. The vendors benefit from various associations representing their interests and promoting the industry in general.

11

Summary of conclusions

The following summarizes the conclusions throughout this FT Executive Briefing.

CHAPTER 1

The threats to IT systems and backup are many and unpredictable, and data losses are on the increase, despite advances in the reliability and sophistication of storage devices and the availability of security and anti-virus software. Added to this, more mission-critical information than ever is now stored on computers rather than other media. With advances in technology, the virulence of attacks is on the increase and 100 per cent reliance on even the most advanced backup system is not always sufficient to recover data. In the fight against natural disasters and attacks caused by humans, backup and recovery solutions, together with defensive strategies, should be reviewed constantly to ensure the best protection of data at all times.

CHAPTER 2

While companies' state of readiness is not 100 per cent, there has been much improvement in recent years. September 11 found a high level of readiness to cope with disaster among affected companies. Surveys also confirm that companies are in a higher state of alert when it comes to disasters than they were a few years ago. While recessionary influences have an effect on companies' ability and preparedness to invest in IT systems, backup and storage expenditure is not the first item to be slashed. Rather it tends to be given priority, due to the importance of maintaining access to critical data in adverse circumstances.

CHAPTER 3

Statistics show the varying levels of risks associated with different types of attack, with external attacks ranking high in frequency, if not necessarily in severity. But whatever the form of attack, an important weapon in ensuring the retention of backup data and mission-critical information, and consequent limitation of losses, is a thorough risk assessment of IT systems leading to a knowledge of the inherent risks associated with various types of attack, as well as implementing access control and other measures to protect systems as a first line of defence.

CHAPTER 4

Disaster recovery and business continuity plans broadly aim to cope with disasters that may or may not threaten the survival of the business and bring the business back to normal as fast as possible. The plans differ in scope, with disaster recovery

typically being more narrowly focused on IT systems, and business continuity involving functions throughout the enterprise. The plans also differ in design, revolving around the modus operandi of a particular organization, its size and its industrial/commercial sector. Whatever the format and content of a plan, an important aspect from a management point of view is to keep it alive and to update it constantly in the light of changing circumstances. Such a strategy will enable the organization to cope with disasters immediately they occur, thus minimizing their consequences.

CHAPTER 5

From traditional tape storage to LAN, SAN and WAN, the backup and storage industry has progressed rapidly in recent years. New technologies have created highly reliable backup solutions, with much increased speeds, high availability, performance and scalability. Most importantly, the new high-speed networks have enabled backup to be performed in locations sufficiently remote from the processing centres to put backup and storage out of the reach of disasters striking in one location or area, and thus safeguarding mission-critical information. Challenges facing the industry include new SAN development areas and the wireless network, which is already being planned and is beginning to appear in experimental form in the US and the UK.

CHAPTER 6

Facilities provided by independent contractors in colocation centres, server farms and other facilities for remote storage, and duplicate data centre facilities, are expanding across the globe. Some providers are offering permanent remote facilities for replicating and storing data. Servers may belong to the client or can be leased from the contractors. Other providers are ready to step in with facilities, such as mobile disaster recovery units, should a disaster occur. The advantages of colocation facilities to clients are that the centres are purpose built and permanently manned by highly skilled staff, with advanced IT systems and a high level of security, and with a range of services available, spanning from simply storing a company's servers to monitoring and managing backup and online services.

CHAPTER 7

Outsourcing, out of favour for a while, is again gaining ground in the field of IT. The consensus is that with the increasing complexity and high-tech nature of IT systems, and the consequent demands on budgets, skill levels and management

time, outsourcing/insourcing or the services of an ASP or SSP should be considered as a serious option by large and small organizations alike, taking into account the benefits such as rapid deployment, gains in management time, predictability of budgets, reduced IT downtime and improved backup and restoration facilities.

CHAPTER 8

With costs of backup and recovery solutions rising, companies are keen to find ways of predicting costs and controlling budgets, and more precise methods of estimating IT associated costs are being developed. But the effects of disasters are unpredictable, with the major ones being hugely expensive, as reflected in insurance claims at the beginning of the twenty-first century. Those organizations with proper procedures for estimating the cost of backup, with insurance in place and supported by proper disaster recovery and business continuity planning, are in the best possible position to ensure their survival should a catastrophe occur.

CHAPTER 9

Financial services have at all times been highly enthusiastic when it comes to new technology and have spent huge sums on pioneering the development and implementation of the latest technology in backup and storage, high-speed, wide-reaching networks and sophisticated applications. The industry is particularly dependent on electronic storage of mission-critical data, information and numerical records, and at the same time is tightly regulated. Financial services therefore need to have their IT systems in place and up and running on a continuous basis. All these factors have combined to place the financial services right out in front when it comes to IT backup and restoration systems, and as such, the sector is more resistant to disasters than most. Unfortunately, these companies are also prime targets for catastrophic events such as terrorist attack, due to their high profile and tendency to cluster together in financial districts.

CHAPTER 10

Vendors of backup and storage solutions range from giants such as Compaq and IBM to the more specialized suppliers such as Tandberg. The backup and storage sector is feeling the recessionary pinch but is doing better than other segments of the IT industry. To retain market share, vendors are adopting open systems, interoperability and common standards, and are consolidating their position through alliances and partnerships. The vendors benefit from various associations representing their interests and promoting the industry in general.

OVERALL CONCLUSION

Both software and hardware technologies have developed rapidly in recent years. On the face of it, new IT solutions are highly complex and costly, but viewed as a new wave of technology, ultimately give higher availability, scalability and greater utilization of storage media. As a result, the increased capacity, which is being created in the wake of the information and data explosion, is able to meet the demands for increased storage space. With interoperability between products emerging, the various solutions can be combined into a single manageable system, which ensures that the products of different vendors can be incorporated to obtain the best possible solution. Techniques such as virtualization and clustering eliminate bottlenecks and minimize the risk of failure.

The new technologies bring in high availability and minimization of downtime, which has cost enterprises so dearly over the years. Better protection of backed-up data and systems in the form of remote locations, duplicate backup systems, colocation centres, more advanced tape formats and mirroring and snapshot technologies all help towards the objective of ensuring full restoration of data within a minimum timeframe. Automatic backup solutions have freed up staff and fostered a more reliable backup culture, which is becoming less dependent on the whims of error-prone or uncontrolled staff.

Spurred on by the catastrophic events of September 11, disaster recovery and business continuity planning as precautionary techniques are gaining ground and are becoming important elements in corporate survival strategies throughout industry. As a result, companies, especially larger ones, are becoming better equipped to deal with attacks, whether internal or external, and are able to feel more confident about being able to withstand the myriad disasters that may strike at any time in the future.

Glossary

ADSL	Asymmetrical digital subscriber line. Technology providing high-speed data transfer lines. Can be several times faster than a modem connection and allows video and audio to be transferred.
AIT	Advanced intelligent tape technology.
ASP	Application service provider. A company that provides software applications to clients remotely on a subscription or rental basis.
Bandwidth	Rate of transfer of data via a communications network, expressed in bits/second, Kbit/second, etc.
BIA	Business impact analysis, business impact assessment. Analysis identifying the impact of the loss of company resources. A review of current operations with a focus on business processes and functions to determine the effect that a business disruption would have on normal business operations. Impacts are measured in either quantitative or qualitative terms. Used in the recovery planning/business continuity process.
Bits/Bytes	A bit is a binary digit (1 or 0). A byte consists of eight bits (decimal value between 0 and 255).
Broadband	High-speed transfer channels.
Browser	Software or viewing pages on the net.
Business continuity plan	A document that defines recovery responsibilities and resources necessary to respond to a disruption in business operations.
Business continuity software	An application program developed to assist an organization in writing a comprehensive business continuity plan.
Business disruption	Any event whether anticipated (i.e. public service strike) or unanticipated (i.e. blackout) which disrupts the normal course of business operations at a corporate location.
Coaxial cable	Insulated copper wire shielded against radio frequency interference by an aluminium layer.
Cold site	A geographically separate alternative facility that is void of any resources of equipment except air conditioning and raised flooring. Equipment and resources must be

	installed in such a facility to duplicate the critical and important processing environment and/or business functions of an organization.
DAT	Digital audio tape.
DDS	Digital data storage tape format.
DMZ	In its original meaning: demilitarized zone. SI-Security defines a DMZ as 'a network added between a protected network and an external network in order to provide an additional layer of security'.
DTF	Digital tape format.
E-mail	Electronic mail sent via the Internet.
Encryption	The scrambling or encoding of messages for security purposes.
End-to-end encryption	The encryption of information at its origin and decryption at its intended destination without any intermediate decryption.
Extranet	Refers to an Intranet accessible to people outside an organization or group. Accessible through a valid username and password.
FCIA-E	Fibre Channel Industry Association Europe.
Fibre	Fibre optic cables consisting of a bundle of glass threads as thin as a human hair, carrying data as laser-generated light beams. A single fibre can carry traffic at several terabits per second.
GPU	Graphics processing unit.
HA	High availability (e.g. in an SAN environment using cluster technology software).
HBA	Host bus adapter.
Homepage	The front page of a Website.
HTML	Hypertext Mark-up Language. Used to format a web page's content.
I/O	Input and output, i.e. information going into or coming out of a program, computer or other IT device.
ISDN	Integrated Services Digital Network. Data moving across existing telephone lines, with speeds of up to 128 Kbps. Up to ten PCs can be connected to an ISDN line using an LAN.

ISP	Internet service provider. Supplies users with connectivity to the Internet.
LAN	Local area network. Computing equipment in close proximity to each other connected to a server which houses software that can be accessed by the users.
LTO	Linear tape open (open format tape technology).
MAN	Metropolitan area network.
MSP	Managed service provider.
NAS	Network-attached storage.
Offsite storage location	A secure location remote from the primary location at which backup hardware, software, data files, documents, equipment or supplies are stored.
Outsourcing	The contracting out of data processing functions to an independent third party.
Recovery window	The time for restoring critical business operations following a disaster.
Risk assessment	The process of identifying and minimizing the exposures to certain threats which an organization may experience.
Risk management	The discipline which ensures that an organization does not assume an unacceptable level of risk.
ROI	Return on investment. Used to calculate the return on IT investment.
SAN	Storage area network.
Satellite communication	Data communications via satellite. For a geographically dispersed organization, this may be a viable alternative to ground-based communications in the event of a business disruption.
SCSI protocol	Used for FC-SAN.
SNIA	Storage Networking Industry Association.
SONET	Synchronous Optical Network.
SSP	Storage service provider.
System outage	An unplanned disruption in system availability as a result of computer hardware or software problems or operational problems.
TCO	Total cost of ownership. A model for calculating the costs of providing applications to users.

Terabyte	A terabyte is about a million megabytes, or exactly 1024 × 1024 × 1024 × 1024 bytes.
WAN	Wide area network, with its parts geographically dispersed (different cities or countries, continents). Public carriers are used in most WANS. Some have their own satellite stations or microwave towers.
Warm site	An alternative processing location, which is only partially equipped (as distinct from hot site, which is fully equipped).
WASP	Wireless application service provider. An ASP specializing in remote management of wireless applications for mobile phones and laptop computers.

Some of the definitions have been supplied by courtesy of Wells Fargo & Co.