Business Continuity Management

Business Continuity Management

How to protect your company from danger

MICHAEL GALLAGHER

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 2003

ISBN 0 273 66351 8

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

Michael Gallagher is Head of Management Services in Radio Telefis Éireann (RTÉ), the Irish national broadcasting organization. In this role he has been responsible for initiating and implementing RTÉ's business continuity management programme and developing the continuity plans that also take account of RTÉ's public service obligations in relation to the handling of major or national disasters. As Head of Information Technology at RTÉ for almost 20 years he was also responsible for establishing the organization's IT disaster recovery and resilience plans. Prior to joining RTÉ he worked as a management consultant with Price Waterhouse & Company – now PwC.

He has written extensively on IT policy and management topics and his books on the use of computers in the human resource function were regarded as definitive texts in the area.

He is a founder member and Vice-Chair of the Irish Branch of the Emergency Planning Society and is actively involved in Survive – the international business continuity organization. He is also a member of the Business Continuity Institute, a Fellow of the Chartered Institute of Management Accountants and of the Irish Computer Society.

Michael can be contacted at:

'Clonyn'
27 Greenville Road
Blackrock
Co. Dublin
Ireland

E-mail: gallagml@iol.ie

Contents

Acknowledgements

This book is based on the practical experience of initiating and managing a business continuity management (BCM) programme in RTÉ, the national broadcasting organization in Ireland.

My involvement in BCM arose from my responsibility for the Y2K project in RTÉ and the realization that there needed to be a BCM programme that was more all-embracing than the IT disaster recovery plans that had been in existence for many years. The Y2K project also considered the wider context and the public service responsibilities that are attached to a national broadcaster. Extensive measures were put in place to ensure that the public was kept informed of any significant implications of the possible fall-out from the Y2K bug. Following on from this, BCM became a high-profile and critical activity within RTÉ.

I want to thank the Director General and the Executive Board for their support of BCM in the organization. In particular I want to acknowledge the contribution of the BCM Working Group, of my colleague Helena Walsh and that of Denis Woods, Renaissance Contingency Services, to the development of BCM in the organization and to enabling me to commit some of that experience to paper.

I am also grateful for the support of my fellow officers of Survive Ireland and of the Republic of Ireland Branch of the Emergency Planning Society.

Finally I wish to express my appreciation of the support and encouragement of my wife Anne, and of David, Marie, Stephen and Helen, during the time, and the many weekends in particular, that I devoted to the writing of this book.

Executive summary

Twenty-eight per cent of UK businesses do not have a formal business recovery plan.

Thirty-seven per cent of the businesses that do have a disaster recovery plan have never tested it.

Commercial Claims Survey, Deloitte & Touche, 2001

Business continuity management (BCM) has recently achieved a higher profile on boardroom agendas. Board members and senior executives need to understand something about the nature and scope of BCM. They need to be in a position to evaluate and enhance the status of the activity within their organizations. This book examines the nature of BCM and looks at its relationship with other activities such as risk management, insurance and the emergency services.

Business continuity management is not just about recovery from a disaster such as one caused by fire or flood or the failure of IT systems. It can be about the collapse of a key supplier or customer, about fraud, unethical operations, and about reputation management.

- Are you satisfied with risk management and business continuity management in your organization?
- Are you sure that your organization could manage through a disaster better than your competitors? If it can't then what would the impact on the business be? Would it survive?
- Are there plans in place to ensure the safety of your employees, your customers and the general public? If not, what are the legal implications and would your organization be irreparably damaged as a consequence?
- Has anyone in your organization considered how to handle trauma or the contact with next of kin following a disaster?
- Is there a plan to deal with the media if a disaster strikes, or would it be a free-for-all with several different stories or versions emerging?

Regulatory requirements impact on business continuity arrangements. The criticality of e-business and IT services, and the real threats that are there, require that the electronic environment be adequately protected in terms of security policies and procedures, built-in resilience and effective recovery arrangements. These areas have become so significant that computer security cannot stand apart from the BCM and risk management functions. They must form part of an integrated approach if an enterprise is to have effective protection and response mechanisms.

- IT security policies are essential, but are you doing what you say you are doing?

For BCM to work it must be driven from the top. It is about creating a continuity culture in the organization. This can be at least as important as producing the actual plans.

BCM is an ongoing process. It may be more difficult to maintain the plans than to create them initially. Plans must be exercised or tested. This is not easy and may be neglected.

There is a need for greater liaison between BCM and the emergency services. This is frequently neglected. There are mutual benefits in establishing a good working relationship between both parties.

The term 'business' in BCM should not restrict its applicability. It is something that virtually every organization should address, regardless of sector or size.

Don't relax because you have a good plan to recover your IT facilities and systems quickly. The IT business continuity plan is only an element, however important, of your overall business continuity management requirement.

Introduction

Gartner estimates that two out of five enterprises that experience a disaster will go out of business within five years.

Enterprises can improve those odds – but only if they take the necessary measures before and after the disaster.

Aftermath: Disaster Recovery, Gartner, September 2001

Professionals involved in the promotion of business continuity management (BCM) have for years been in a position to quote a variety of examples and statistics that have emphasised the need for proper planning and management in this area.

There have been various examples.

- A single bomb in St Mary's Axe in London in April 1992 caused damage amounting to approximately £1.5 billion and forced 40 companies to relocate to alternative premises. The dramatic video, which showed the impact of the bomb and the way in which Commercial Union Insurance Company responded to the disaster, proved to be a very effective way of gaining senior management approval and commitment to a BCM programme.
- The power problems in Auckland, New Zealand in early 1998 highlighted the extremely serious consequences of difficulties with the electricity supply, the need for resilience and diversity in supply, and how situations can go from bad to worse. In a period of less than a month four power lines that supplied New Zealand's financial heart – the Auckland Central Business District – failed. This area also contained the country's main container port, major hotels, telecommunications companies, hospitals and educational establishments. When the fourth line went down the situation was extremely serious and the estimated time to restore a basic service was one week. As it turned out there were other problems and it was a further six weeks before power was restored fully, using temporary lines.
- The California power crisis in 2001 also emphasized the problems caused by an unreliable supply of electricity.
- The disastrous fires close to Sydney in 1994, and then more recently in the Christmas and New Year period of 2001/2002, were also used to emphasize certain BCM messages. The film and photographic coverage was dramatic, and the side effects, such as the level of pollution in Sydney, were also frightening.

Despite these examples it could still be difficult to sell the idea of BCM. However, selling it to the board and senior executives of a company has become easier since the tragic events of September 11 2001 in the United States.

The horrific attack on the World Trade Center (WTC) placed the spotlight on BCM in a major way. The terrible devastation seen over and over again on our TV screens ensured that organizations immediately considered how they would survive in equivalent circumstances. The catastrophe was so big that the likelihood of it recurring may be slight, but it got a lot of managers thinking and certainly put BCM much higher up the executive agenda.

Disasters do not need to be anywhere near as large to cause major problems for an organization. Sometimes the impact can be terminal.

How would your organization cope with any one of the following types of incident?

- A major fire at head office or at a large operational unit.
- Severe flooding of your main facility or major damage to your computer centre caused by burst water pipes. Would the consequences be worse if it happened over a holiday weekend where systems automation facilities ensured that computer staff were not working?
- Spillage of a toxic substance, which meant that access to a key facility was prohibited by the authorities for a number of days.
- A major computer virus attack.
- If your organization was responsible for causing a major environmental pollution problem, how would management handle the media and minimize the impact on the organization's reputation?

SEPTEMBER 11

In the immediate aftermath of the New York disaster it is interesting to note how organizations coped and how effective and relevant their contingency plans were.

- *Some plans failed because they assumed that they would only ever be subjected to a single-building hit.* The wider nature of the disaster had not been considered. This is typical of many business continuity plans.
- *Some organizations found that their plans were much too detailed and accordingly not as effective as anticipated.* A critical success factor in good business continuity planning is to get the balance right between too much and too little detail. This is particularly the case where senior and operational management are not as familiar with the plan as they should be. Obviously if the plan is not tested regularly this familiarity will be absent.

It is also a problem when the plan has been prepared by groups other than the managers who are directly involved in the organization. A simple call-out list of key personnel who know the business can be more effective than a very detailed plan, which is difficult to keep updated and is allowed to gather dust on the shelf.

- *Some plans were not immediately available.* Copies were not always held in the homes of key personnel and managers had difficulty getting access to them. How many plans are meticulously prepared and then all copies are stored at the centre where the problem can arise?
- *It is understood that in at least one organization key members of the emergency response team were unable to handle the traumatic after-effects of the disaster and were not effective in their role.* The composition of the emergency response team is critical. These must be people who can remain relatively detached from the impact of an incident and be effective leaders during the recovery process. They are not necessarily the most senior executives in the organization.
- *Plans were not up to date.* An out-of-date plan is worse than not having a plan. As corporations experience significant organizational change – whether this means expansion, contraction or a refocusing on activities resulting in rationalization – it is very easy for the plan to become largely irrelevant quite quickly. The easiest environment in which to keep a plan up to date is one where the organization is relatively stagnant – not very typical in today's business world.
- *Generally operations took significantly longer to recover than had been envisaged in the plans.* The extent of the disaster, and in some cases the loss of key personnel, impacted on this.
- *Some plans had not been sufficiently tested; this was especially the case regarding tests that would have involved staff other than IT personnel.*
  - When was your organization's contingency plan last tested?
  - What type of test was it?
  - Were all systems interfaces tested? This can be critical.
  - Was the test confined to IT operations?
- *Some organizations did not have adequate alternative serviced office space available to continue operations quickly.* This may have been influenced by the geographical extent of the problem and the fact that so many corporations were seeking facilities at the same time.
  - Where is your back-up facility located?
  - Where would staff work?
  - Would transport, communications and other services be available?

  Generally, plans were based more on the protection and recovery of physical assets and computer systems than on people issues.

- *Back-up facility providers may not have been able to cater effectively for so many calls for help.*
  - Are you aware of the customer profile of your alternative/recovery site provider?
  - How many of its customers could be affected by the same incident?
  - What ratio of customers to facilities is used and is this adequate?
- *In some cases organizations discovered that their emergency operations centre for directing crisis management activities was unavailable.* Other premises had to be found. There were difficulties in getting key staff to alternative locations because of transport difficulties, and the failure of telecommunications systems added to the problem.
- *Vital paper records were lost.* Sometimes insufficient attention is given to safeguarding an organization's vital paper records. If a document is digitized it is likely to become part of the conventional IT back-up and recovery plans. Otherwise, unless there is a definite policy and procedure to ensure that copies of important documents are made and stored at an alternative location, vital documents are at risk.
- *On the positive side, there were some very good stories.* Third-party recovery services performed well. Organizations with good plans managed well. Generally, corporations with recovery service agreements were reasonably well spread over the major service providers and apparently all customer calls for assistance were facilitated – even if some of the recovery locations provided were not the ones originally contracted for and with which recovery staff had become familiar. However, to a large extent this justified the considerable investment by organizations in contracting for this type of service.

GEOGRAPHICAL CONCENTRATION

The concentration of so many organizations, including their back-up operations, within the relatively concentrated area of the WTC has encouraged many organizations and regulatory bodies to reconsider the increased risk attributable to geographical concentration.

In many cities the financial services business tends to be concentrated in certain parts of the city. London is a good example, where so many financial businesses and in some cases their back-up facilities are concentrated in the City and in Canary Wharf. In the event of an incident, or incidents, affecting both locations, including unaffected but cordoned-off areas, many firms could be in trouble. They could be unable to operate critical business units as both their primary and back-up sites became unusable or inaccessible.

Despite the way in which IT developments can facilitate the decentralization of business functions and activities, there has been a reluctance to decentralize. The apparent benefits of concentration in terms of cost – for example, the savings on travel and subsistence payments and on minimizing duplicated functions – have been to the fore.

Since September 11 some large organizations have looked again at the process of decentralization and of reducing the concentration of staff in individual locations. Technologies such as video-conferencing that facilitate the dispersal of staff have been given a further boost. E-work also falls into this category. The provision of effective remote access to IT systems is now seen as a priority by some organizations. With a reasonable level of investment, the capability to enable staff to work from home and to be able to switch quickly to access IT facilities at an alternative location in the event of a crisis is highly desirable. A by-product of providing such facilities is the ease with which employees can be kept fully informed of how a crisis is being dealt with via a confined website.

BCM IS A PRIORITY

Before September 11, the need for comprehensive business continuity plans was being stressed by external auditors – and internal auditors – and this has now become stronger.

The insurance industry was badly hit by the tragic events. In addition to rises in premiums, insurers are increasingly seeking evidence not just of the existence of an appropriate plan but confirmation that there is a process that has full management support and that plans have been adequately tested.

Good management demands that BCM is a priority. It is a requirement of good corporate governance that there is a BCM programme in place. This has been emphasized by the Turnbull Report, and board members are increasingly aware of their liability. This is the source of much of the pressure to have proper business continuity plans, as managing risk has been explicitly highlighted as a key board responsibility.

Despite these pressures there can be a tendency to pay lip service to BCM or to have a token BCM project. Responsibility may be given to someone without sufficient authority and without full executive support.

When the project is mooted, or when the work starts, there are always the familiar excuses:

- It will never happen to us.
- I'm sure that we could cope.
- You can't plan for the unforeseen.

- There are so many potential problems that it is impossible to have an effective plan.
- If we don't have a disaster we've wasted money.
- Isn't that why we have insurance?
- We are used to things going wrong.
- It really doesn't matter because in an emergency everyone will rally round and get things sorted out.
- I don't have the time – there are more important things to do.
- I could do all this work without any help from you – just give me the time!

HOW THIS BRIEFING MAY HELP

Every organization is different, and this is reflected in the different approaches that are taken to BCM. There is no single best way to approach it, and accordingly this book takes an approach that is not over-prescriptive. It is hoped that this book will help to increase the level of awareness as to what BCM entails and on how to approach it. It is intended for managers who want to know more about BCM and for people who may be charged with establishing and implementing BCM in an organization.

The objectives of this book are:

- to examine what BCM is;
- to consider the need for BCM;
- to describe the approach and the organization climate required to make BCM a success.

A list of useful sources of information is included in Appendix 3. These include books, journals and, in particular, relevant contacts and their websites.

1

What is business continuity management (BCM)?

Business continuity management is the act of anticipating incidents which will affect mission-critical functions and processes for the organization and ensuring that it responds to any incident in a planned and rehearsed manner.

This is the definition used by the Business Continuity Institute (BCI). There are other definitions of BCM. Some of these emphasize the combination of management disciplines and activities that help to ensure the continuous operation of the essential business functions under all circumstances.

The BCI definition emphasizes three key elements:

- '*It is the act of anticipating incidents* …' The organization must examine the risks and threats to which it is exposed and consider how best to deal with them should an incident occur. The choice of the word 'incident' rather than 'disaster' is important. The term 'disaster' immediately conjures up pictures of an explosion, fire or serious flooding. 'Incident' includes these occurrences but also embraces power failure, telecommunications failure, fraud, product contamination, pollution of the environment, failure of a key supplier and other events that do not sit comfortably under the generally accepted meaning of disaster. It may even include the inappropriate comments of indiscreet senior executives at public functions!
- '… *which affect mission-critical functions and processes* …' BCM is not about plans and procedures for the everyday things that go wrong. It is concerned with significant incidents that have a considerable impact on the core activities of the organization. It is far too easy to divert effort into documenting procedures for the failure of day-to-day operational processes. While these procedures must exist, BCM must emphasise the *big* picture.
- '… *ensuring that it responds to any incident in a planned and rehearsed manner*' This element of the definition encompasses the planning, meaningful involvement of appropriate personnel, acceptance and ownership of the plan, and thorough testing which are all essential prerequisites of an appropriate response.

Sometimes when describing BCM to a group of managers it is best to try to relate it to their business in a personal way. A statement such as the following can have greater impact. 'BCM is about ensuring that if your organization experiences a disaster or other serious incident you have already considered that possibility. You will have taken steps to reduce the risk of this happening and to minimize the impact if it does happen. You will have a plan in place with which all key managers are familiar, which has been tested, and which will enable your organization to continue to function as close to normal as possible with the least disruption possible.'

This also emphasizes that BCM is not simply a matter of having a plan. A proactive aspect of BCM is ensuring that measures are introduced to reduce the

likelihood of problems arising, and to inject elements of resilience and contingency into the operations – which is all part of establishing the appropriate BCM culture.

In selling and gaining management acceptance of the need for BCM, it can be very effective to pose questions relating to the impact of a serious incident on the areas for which managers are individually responsible.

- If the main office facility is unusable and inaccessible following an explosion last night:
  - Where can the staff be based?
  - How quickly?
  - How will computer facilities be provided?
  - How quickly will there be a telephone service?
  - What impact will the situation have on revenue and customer support?
  - What vital records will have been lost?
- If the main production facility is suddenly flooded:
  - Would the health and safety procedures be satisfactory?
  - How quickly could key customers be supplied?
- If a fire destroyed the computer centre last night:
  - Would up-to-date copies of all necessary data and systems be available?
  - Are the most recent back-ups stored at an off-site location?
  - What arrangements are in place for the use of a back-up site with adequate accommodation?
  - How quickly could data communications facilities be restored?
  - How quickly would alternative computers, with current versions of software, be up and running?
- If the electricity utility has a problem with supplying adequate power, what are the implications for the business?
  - Are key electronically controlled processes protected against power surges and intermittent failures?
  - If the main power supply cables are severed, how quickly can power be restored? Should there be an alternative supply via a separate route?

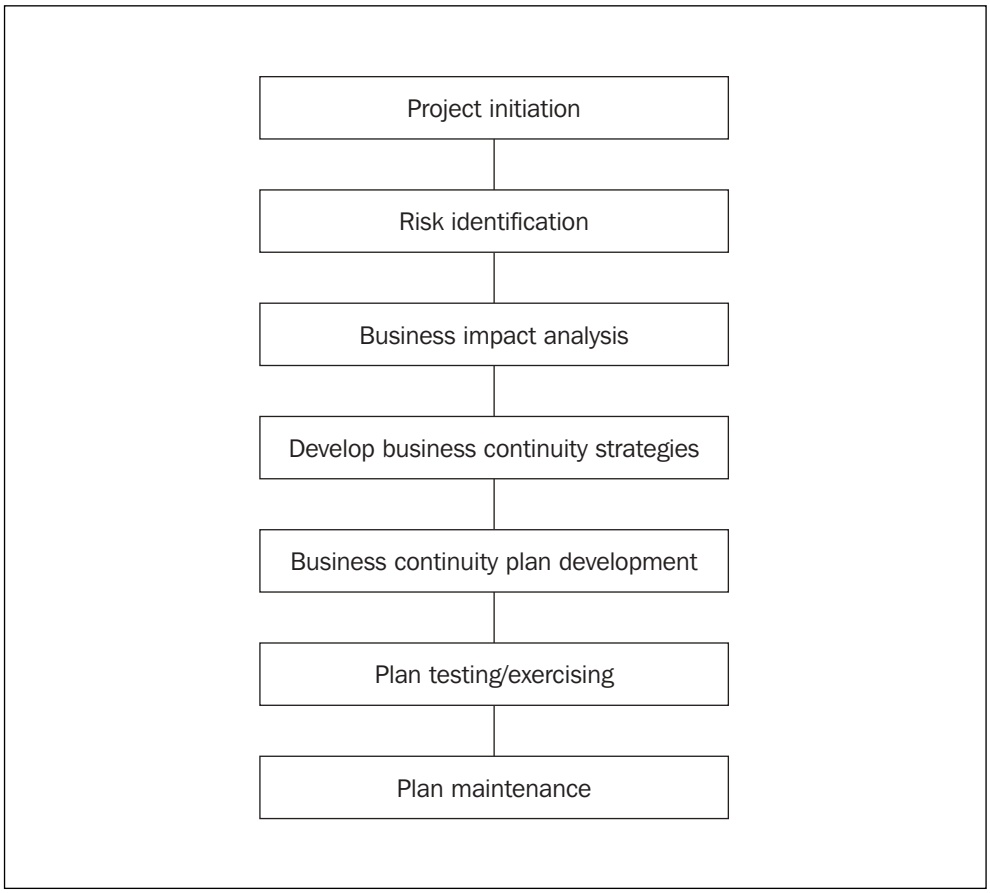
Use recent incidents, or 'near misses', to get management engaged. It is generally much more effective to take as an example an incident that happened within the organization, or a local incident, or one within a company in the same industry with which management will be familiar.

Examples such as:

- The fire which started in a desktop fan left on over the weekend in the legal department and which was discovered by a security guard on a regular round. Fortunately the fire was still at an early stage. What would have happened if the security guard had taken a different route and the fire had had a chance to become established? It would have been particularly damaging in a building containing lots of paper and adjacent to the accounting department.
- The fire in the staff kitchen, located next to the boardroom and the senior executive suite and used to prepare snack meals, which was extinguished quickly by a staff member who had just completed a fire safety course. Would other staff have been as effective?
- The overflowing toilet from which water started to leak through the ceiling of the computer centre late on Friday night. The centre is usually unattended at weekends but fortunately a computer operator came in early on Saturday morning and limited the damage.

The principal phases in BCM are shown in Fig. 1.1.

Fig. 1.1 **The principal phases in BCM**



THE EVOLUTION OF BCM

Business continuity management is the outcome of a process that started in the early 1970s as computer disaster recovery planning (DRP) and then moved through an era where the emphasis was on business continuity planning rather than on management.

In the 1970s the DRP activity was driven by the computer manager. In realizing that the concentration of systems and data in itself created new risks, computer operations management introduced formal procedures governing issues such as back-up and recovery, access restrictions, physical security, resilience measures such as alternative power supply, and change control.

In those days, if a major incident or disaster happened, the downtime that could be tolerated was measured in days rather than hours. Unsurprisingly, the cost of back-up computers sitting idle in an alternative location waiting for a disaster to happen was prohibitive.

However, organizations such as banks were in a more vulnerable position and invested considerable resources in installing and testing computers at alternative sites. Back-up tapes or disks were increasingly stored at protected locations well away from the computer centre.

The 1980s saw the growth of commercial recovery sites offering services, often on a shared basis. This was the start of the sophisticated recovery centres that operate today.

However, the emphasis was still only on IT. The disaster recovery plans documented the actions required to safeguard and restore computer operations. These covered computer processing, computer applications, telecommunications services and data after a disruptive event. The objectives were to prevent or at least minimize the impact that such an event would have on the business. They were more concerned with, for example, restoring a company's financial systems to an operational state than with worrying about whether there would be accommodation available to allow the staff of the finance department actually to use the systems.

The 1990s witnessed significant change in the IT environment and in the move from DRP to business continuity planning (BCP). Throughout this decade, and into the 2000s, there were significant changes in the IT approach to DRP/BCP and in what constituted acceptable downtime. The emphasis moved from being mainly on IT to an approach that considered all aspects of an organization's business and relationships.

Now BCP has become BCM with the emphasis on management – not just planning. This encompasses the emphasis on risk management and the measures to be taken to reduce risk. BCM is no longer regarded as a project – it is now a programme, emphasizing that it is a continuous process rather than a task with a defined end-date.

After September 11 BCM has assumed a new importance. Board members now realize that the very survival of the enterprise may depend on it. The increased recognition of BCM means that a greater budget allocation may be available to it. More significantly, the message preached by business continuity practitioners for years that business continuity principles should be an integrated part of the business planning process may be heard. This applies to capital projects, new processes and applications. BCM – and risk management – considerations should be addressed in the business requirements phase of projects rather than as an add-on when completed. At that stage the add-ons become expensive.

IMPACT OF Y2K ON BCM

The hype, concerns, remedial action and contingency plans that surrounded the year 2000 (Y2K) had significant implications for BCM.

In the first place, it was the fear and uncertainty concerning the implications of the year 2000 changeover that caused many organizations to think of BCM for the first time. In addition:

- it increased awareness of business interruption issues;
- it resulted in a better understanding of critical processes and vulnerabilities;
- it improved co-operation and collaboration between public and private sectors on emergency management issues.

The work that was done to ensure that systems addressed the date change correctly led to significantly better control over systems. Systems documentation was improved, and some organizations established a proper inventory of their systems and data for the first time.

Most organizations had never previously realized the degree to which equipment and processes were dependent on a computer chip to function. The uncertainty surrounding the implications for embedded systems also resulted in significantly better records and understanding in this area.

The concern to ensure that corporate governance requirements were met also resulted in an avalanche of correspondence to suppliers and customers looking for assurances as to compliance. In particular the concerns about how utilities – power, gas, water, transport and communications – and financial institutions would cope gave rise to a range of contingency measures in many organizations.

To a large extent, before September 11, it was Y2K that provided the greatest boost to BCM. Many of those responsible for the Y2K project were then given the task of building on the work done and of broadening it out into full-scale corporate business continuity planning and management.

The preparations made for Y2K have subsequently proved to be of value in a number of areas, including:

- when different types of disasters have occurred subsequently – in the case of the events of September 11 a number of companies have attributed the quality of their response to the work done in the late 1990s;
- in providing comprehensive information more quickly in merger and acquisition situations;
- in the detailed preparatory work that was required before the change to the euro in most member states of the European Union (EU).

RELATIONSHIP WITH RISK MANAGEMENT

Risk management should be a key consideration in every business decision.

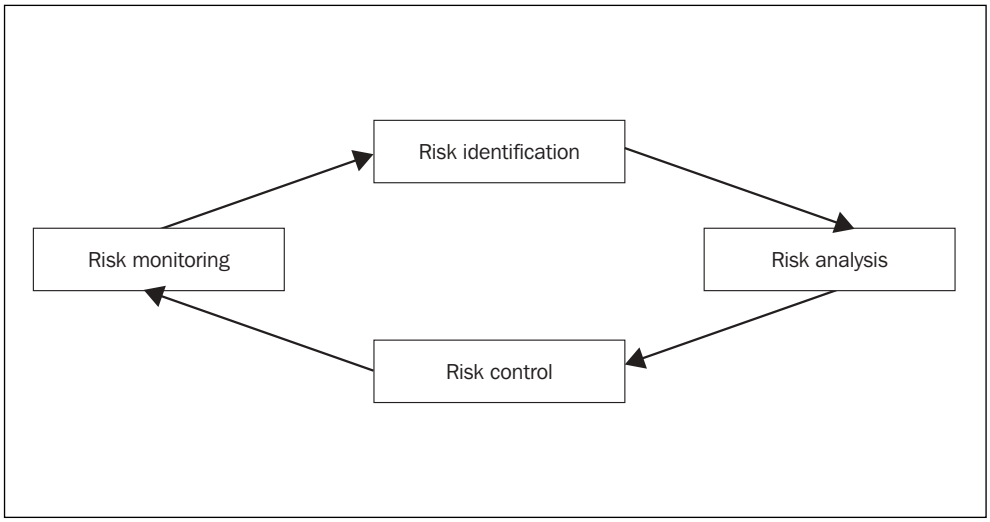
BCM is closely linked to risk management. In many organizations BCM is part of an overall risk management function. This is particularly the case in financial organizations where risk management is well established, features very high on the corporate agenda, and is usually represented at board level. While the Turnbull Committee has placed a lot of emphasis on risk, there are other factors that impact on the regulatory environment within which financial organizations operate. The international banking regulations established through the Bank of International Settlements in Basle, Switzerland, have imposed increasingly sophisticated and extensive requirements for risk management within the banking system. The Basle Committee's 2001 proposals ('new Capital Accord') are a major overhaul of the 1988 Capital Accord. The accord will apply to all major banks in the G10 countries from 2004 and it is likely that regulators in many other countries will adopt it. In the EU, the European Commission has stated its intention to apply the new Capital Accord to all credit institutions and investment businesses. The implications are regarded as far-reaching and will require significant investment by financial institutions in order to comply. There are onerous requirements which will impact on risk management and business continuity activities.

Risk management is the process of identifying risks, evaluating their potential consequences and determining the most effective methods of controlling them or of responding to them. The aim is to reduce the frequency of risk events occurring, whenever this is possible, and to minimize the severity of their consequences if they do occur.

Risk management should be very much a part of every manager's day-to-day responsibilities. It is not simply an 'add-on'. It is integral to strategic management, project management and operational management.

To manage risk effectively, risks need to be systematically identified, analyzed, controlled and monitored. This process is referred to as the risk management cycle (see Fig. 1.2).

Fig. 1.2 The risk management cycle



Risk classification

There are various ways of classifying risks. Categories include market risks, credit risks and operational risks. Market risks can embrace such areas as the impact of world economic climate changes, financial market fluctuations, changes in interest rates and in foreign exchange rates. Credit risk basically relates to the possibility of a debt to a business not being honoured. Obviously in financial trading there are also different types of business transactions not necessarily related to lending which are subject to credit risk.

The main class of risk that impacts on BCM is operational risk. The term derives from risks seen as relating to the activity of the business, but in reality it is a term that includes all types of business risks except market or credit risks.

Another approach to classification is one that distinguishes between strategic and operational risks. Strategic risks are the ones that concern the board and management strategists. While operational risks are still an issue at board level, they tend to be managed at a lower level.

Strategic risks include:

- actions by governments – these can have worldwide implications, may determine the regulatory and legislative environment, and can involve the introduction of taxation changes and other economy management measures;
- changing customer requirements – such as fashion changes;
- changes in competitive environment – new entrants, takeovers/mergers;
- new technology – providing both threats and opportunities – or technology obsolescence;
- substitute products;
- wrong marketing strategy.

Examples of operational risks include:

- *External risks:*
  - interruption of supplies (product or raw material) – key supplier goes out of business, industrial action, transport difficulties, international disputes;
  - quality of supplies – quality control problems, environmental or weather conditions.
- *Internal risks:*
  - fire;
  - flood;
  - explosion;
  - computer/systems malfunction;
  - equipment breakdown;
  - pollution;
  - industrial action – disputes;
  - fraud or losses in foreign exchange dealing;
  - sabotage;
  - design mistake;
  - loss of key people.
- *Distribution risks:*
  - transport problems;
  - product counterfeiting;
  - product tampering.
- *Customers:*
  - key customer goes out of business;
  - key customer switches to alternative supplier.

BSI guide

The British Standards Institute (BSI) has produced a guide to how organizations can establish and manage their strategic risks. This document is applicable to organizations worldwide in both the private and public sectors. It outlines a management framework for identifying threats, determining the risks, implementing and maintaining control measures, and for reporting on the process.

The guide includes the following self-assessment benchmark questionnaire, which will enable you to get a feel for where your organization is positioned in relation to risk control.

BSI benchmark questionnaire

	Question	Score
	Each question can score in the range 0 to 3.	
1	Have you identified the strategic risks to the organization?	_____
	Score 0 if there is no process for risk identification and the organization has not identified its strategic risks. *Score 3 if the organization has established a formal system for risk identification and regularly reviews its strategic risks.*	
2	Have you assessed the likelihood and consequences of the significant risks being realized?	_____
	Score 0 if the business threats are not fully evaluated, assessed and ranked for action as appropriate. *Score 3 if the organization has a fully developed system that evaluates the risks so they can be prioritized.*	
3	Have you assessed those risks that could:	
	(a) damage your reputation?	_____
	(b) adversely affect your market position?	_____
	(c) result in production and/or service failing?	_____
	Score 0 for each 'no'. *Score 1 for each 'yes'.*	
4	Have you established management controls to deal with the risks?	_____
	Score 0 if there are no internal control arrangements for managing the risks. *Score 3 if there are established control systems implemented and maintained for internal control of the risks.*	
5	Are the control measures embedded in the culture of the organization?	_____
	Score 0 if the organization has not established a positive culture within the organization to mitigate the risk. *Score 3 if the internal control measures are well embedded in the culture of the organization.*	

6 Have you established a contingency plan to deal with disasters? _____

Score 0 if there is no contingency plan.
Score 3 if there is a well-established plan that is tested and reviewed regularly.

7 Have you established continuity management arrangements in the event of a disaster? _____

Score 0 if there are no continuity arrangements.
Score 3 if there are arrangements to ensure that the organization can quickly become operational again in the event of an emergency or product recall, etc.

8 Do you regularly audit the management control arrangements? _____

Score 0 if there is no audit system in place.
Score 3 if there is a formal system in operation and it is effective in establishing areas of improvement.

9 Do you regularly review the arrangements with respect to their adequacy? _____

Score 0 if the organization never reviews its arrangements for strategic risks.
Score 3 if the organization carries out a thorough review of its current arrangements and re-examines the scope to establish whether it is sound in the emerging marketplace.

10 Do you report annually on your risk control measures? _____

Score 0 if the organization does not make a report on any issue other than finance.
Score 1 if there is a report covering issues such as occupational health and safety and environmental matters.
Score 3 if there is an annual report statement on all risk control measures as required by Turnbull.

Total score _____

If your total score is:

10 or less	Your organization has hardly made a start on the effective management of its strategic risks and needs to move forward quickly on this front.
11 to 20	Your organization has made a start but needs to do much more.
More than 20	Your organization has addressed many of the aspects of strategic risk management and is on the way to effective control of those risks that are of strategic importance.

RELATIONSHIP WITH THE EMERGENCY SERVICES

In many organizations there has been a tendency to ignore the emergency services, or to fail to develop a satisfactory working relationship with them and understanding of them. Many plans finish at the 'factory gate'. While there will most likely be contact with key suppliers of power and voice and data communications facilities, there is often a gap when it comes to the emergency services.

Plans cannot ignore the roles of, and relationships with, the police, fire and ambulance services. Sometimes the gap arises because there is no established mechanism to liaise easily with all of these services. This can lead to confusion as to roles in the event of an emergency. This issue is examined in Chapter 9 – Role of the emergency services.

Case study 1.1

Enron – risk management failure on a massive scale

Enron was the sixth largest energy company by market capitalization in the world, with revenues of $101 billion and assets of $47.3 billion in 2000. On 2 December 2001 Enron Corporation filed for bankruptcy protection from its creditors in the largest financial failure ever in the United States. In addition, it brought about the virtual demise of its auditors, Andersen.

Shareholders saw the Enron share price drop from a high of $90 in August 2000 to less than 50 cents in November 2001. Many of Enron's 21,000 employees in the United States and throughout the world found themselves not only without a job but with part of their pension fund invested in Enron.

Enron was formed by the merger of Houston Natural Gas and InterNorth of Omaha, Nebraska, in 1985. This was the year that the US Federal Energy Regulatory Commission issued an order that required pipeline owners to provide open access to pipeline capacity. This, and other developments, encouraged the growth of a market in short-term gas supply contracts and eventually led to a true spot market for natural gas. Enron went on to dominate this marketplace.

Enron got involved in complex off-balance-sheet vehicles to access capital and to hedge risk. It also became involved in other industries, and by the late 1990s it was heavily into the broadband industry that was destined to support the 'New Economy'. By 2000 Enron Online had become established as a leading web-based service that offered traders in energy and other markets information, transaction services and trading tools. The company was also trying to become a market-maker and price-risk-management provider in bandwidth trading. It envisaged playing the same dominant role in this business that it had done when the natural gas industry was deregulated. It even had plans to offer new distribution channels to the lucrative entertainment industry.

In 2001 the complicated off-balance-sheet transactions became a cause of concern to financial analysts. The dotcom bubble was bursting and there were troubles for the global telecommunications industry. Enron's share price started to tumble.

In November 2001 Enron restated its earnings for the years 1997 to 2001. It admitted that 'certain off-balance-sheet entities should have been included in Enron's consolidated financial statements'. Including them meant that its declared debt burden increased by hundreds of millions of dollars. The company stated that the original 'financial statements for these periods and the audit reports for the year-end financial statements from 1979 through 2000 should not be relied upon'. By the end of the month the shares, which had been as high as $90 in the previous year, were now trading between 45 and 25 cents.

Within days Enron filed for Chapter 11 bankruptcy protection.

A combination of aggressive accounting and off-balance-sheet deals had allowed Enron to create a virtual company with virtual profits. It boosted profits by booking income immediately on contracts that would take up to ten years to complete. These and other questionable financial practices apparently were not seriously questioned by the auditors.

Internally, Enron's risk managers questioned some of these practices and profit forecasts. Their views were disregarded by an aggressive management.

2

Why do I need BCM?

The Turnbull Committee Guidance for Directors on Internal Controls sets out an overall framework of best practice for business based on an assessment and control of their significant risks. For many companies business continuity management will address some of these key risks and help them to achieve compliance.

Nigel Turnbull, Chairman, ICAEW Committee on the Guidance for Directors on Internal Controls

There are many reasons why every organization should have an active business continuity management programme. In some cases the initiative comes from pressure to respond to the recommendations and demands of the auditors or insurers. Sometimes, the driving force is the concern of non-executive directors who are conscious of their responsibilities under the requirements for good corporate governance.

Regardless of these pressures, BCM should be regarded as an integral element of good management. It is foolhardy for management not to consider and plan for business continuity and minimize the disruption that would be caused to the business. But BCM is about more than this. It is concerned with:

- safeguarding share value and shareholder interests;
- demonstrating good management;
- protecting employment;
- managing and protecting reputation and brand value.

Many organizations today are demanding that their first-tier, and in many cases second-tier, suppliers have documented disaster recovery and business continuity plans in place.

IMPACT OF TURNBULL

In 1999, the working party established by the Institute of Chartered Accountants in England and Wales (ICAEW), which was chaired by Nigel Turnbull, produced its report on Internal Controls. It provided guidance about the adoption of a risk-based approach to establishing a system of internal control and reviewing its effectiveness. The Turnbull guidance is linked, via the Combined Code on Corporate Governance, to the Listing Rule disclosure requirements of the London Stock Exchange. Consequently, non-compliance with the Turnbull guidance would result in an embarrassing disclosure in a company's annual report. This could attract the attention of the press, financial analysts and commentators, shareholder activists and institutional investors.

Apart from the implications for public quoted companies, The Turnbull guidance is regarded as having a much broader application. It makes good business sense to manage risk effectively and to embed internal control in the business processes by which a company pursues its objectives. Organizations have been encouraged to treat Turnbull as the opportunity to improve not only the management of risk, but also the business as a whole. The implementation of the guidance is not a one-off exercise. The expectation is that the practices are embedded in the operations of the organization and become part of the culture.

Accountants, external and internal auditors, business consultants, and directors and senior executives of companies have been significantly exposed to these guidelines. They are very aware of the possible implications of failure to adhere to them.

This has given a considerable boost to both risk management and business continuity.

IMPACT OF THE FOREIGN CORRUPT PRACTICES ACT

In the United States the Foreign Corrupt Practices Act (FCPA) of 1977 is often quoted as a driver of BCM. Some regard it as having done more to increase awareness of the need for contingency planning than any other factor.

At first sight, the BCM connection with such a piece of legislation is not at all obvious. The legislation came into being in the post-Watergate era and was designed to eliminate bribery. It allowed for the prosecution of companies that used bribes to get business advantage in foreign markets. It made it illegal to destroy corporate documents in order to cover up a crime.

It is a requirement of the FCPA that 'companies make and keep books, records and accounts which, in reasonable detail, accurately and fairly reflect the transactions and disposition of the assets'.

Under the legislation, corporate officers are subject to large fines and terms in prison for failure adequately to protect their company's assets. The Act allows for both criminal and civil prosecution for violation.

The record-keeping provisions of the legislation are significant. They have been adopted by the Securities and Exchange Commission (SEC) and are now applicable to all publicly held companies in the United States.

The FCPA requires that companies must have an organizational structure, control procedures and systems that:

- safeguard their assets;
- check the accuracy and reliability of accounting records;
- promote operational efficiency;
- encourage adherence to prescribed policies.

This places an obligation on management to ensure that it concerns itself with the effectiveness of all relevant controls. Management is obliged to exercise 'standards of care'.

This is where contingency planning and BCM come in.

Initially, the FCPA also gave a boost to what was then known as computer disaster recovery planning. Because of the significant investment in developing or acquiring computer systems, there was a need to regard the software as a significant asset. It needed to be treated as an asset in the same way as corporations were accustomed to treating physical assets like buildings and plant and equipment. The investment in data and the creation of databases, which were vital to the business, meant that data should also be treated as an asset. This gave a major impetus to writing up the plans, but more significantly to investment in computer resilience, off-site storage, and in particular to the market for facilities such as portable computer rooms and hot sites.

NASD PROPOSALS

The National Association of Securities Dealers (NASD) in the United States was established by legislation in 1938. It is responsible for regulating the US securities industry and the NASDAQ Stock Market. Its jurisdiction extends to over 5,400 firms and over 676,000 securities industry professionals.

In spring 2002, it proposed that all of its members operate viable business continuity plans as quickly and efficiently as possible.

The specific proposal is as follows.

Business continuity plans

(a) Members of the Association must create and maintain a written business continuity plan identifying procedures to be followed in the event of an emergency or significant business disruption. The business continuity plan must be made available upon request to NASD staff.

(b) Members must conduct a yearly review of their business continuity plan to determine whether any modifications are necessary in light of changes to the member's operations, structure, business or location.

(c) The requirements for a business continuity plan are flexible and may be tailored to the size and needs of a member. Each plan, however, must, at a minimum, address:

- data back-up and recovery (hard copy and electronic);
- all mission-critical systems;

- financial and operational assessments;
- alternative communications between customers and the firm;
- alternative communications between the firm and its employees;
- business constituent, bank and counter-party impact;
- regulatory reporting;
- communications with regulators.

(d) 'Mission-critical system' means any system that is necessary, depending on the nature of a member's business, to ensure prompt and accurate processing of securities transactions, including order taking, entry, execution, comparison, allocation, clearance and settlement of securities transactions, the maintenance of customer accounts, access to customer accounts and the delivery of funds and securities.

(e) 'Financial and operation assessment' means a procedure created by a firm to test and determine the firm's capability to conduct business.

The proposal also requires members to file with the NASD up-to-date key information that would be of particular importance during significant business disruptions, including:

- emergency contact information for key staff;
- identification of a designated contact person;
- location of books and records (including back-up locations);
- clearance and settlement information;
- identification of key banking relationships;
- alternative communication plans for investors.

In the aftermath of September 11 this is a timely exhortation and reflects the general movement by regulatory bodies for appropriate business continuity plans.

In addition, the Expedited Funds Availability Act specifically requires federally chartered financial institutions to have a demonstrable business continuity plan to ensure prompt availability of funds.

FSA

In the UK, the Financial Services Authority (FSA) sees BCM as part of good risk management. It expects all authorized financial institutions to consider the need for a risk-based BCM framework including an appropriate business continuity plan.

The FSA Handbook states:

A firm should have in place appropriate arrangements, having regard to the nature, scale and complexity of the business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness.

The FSA's policy governing outsourcing requires firms to have formal service level agreements (SLAs) with their outsourcing providers where the contract is material. Outsourcing BCM processes such as arrangements for the use of disaster recovery centres come within the range of 'material contracts'. The SLAs should contain a range of performance criteria such as:

- availability and assurances in relation to syndication arrangements;
- the nature and frequency of testing;
- maintenance of facilities;
- the adequacy, resilience and diversity built into the power supply;
- equivalent assurances in relation to voice and data communications facilities.

Following September 11, the FSA commenced a total review of BCM in the sector and produced working papers as part of a consultative process aimed at placing greater emphasis on ensuring continuity. It also recognized that the WTC experience indicated that a major factor in the ability of firms to recover quickly was the extent to which they could communicate effectively. The FSA, in conjunction with the Bank of England, therefore assembled a database of 24-hour contact details for the key personnel in the major firms and financial infrastructure providers in the UK. This is now held centrally, and procedures are in place to ensure that it is updated regularly.

HIPAA

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 has significant implications for BCM, including computer security. Just as with the Foreign Corrupt Practices Act, the connection with BCM is not immediately apparent.

HIPAA was introduced to address two issues in particular:

- to improve continuity of health insurance coverage for individuals who change or lose jobs;

- to establish standards for healthcare information, transactions and data elements – this mandates the creation and adoption of standards that can be applied to any electronic transmission of specified transactions.

HIPAA calls on all relevant organizations to adopt procedures that will guard data integrity, confidentiality and availability.

Healthcare oganizations must implement the following:

- Contingency plans that include:
  - applications and data criticality analysis;
  - data back-up plans;
  - disaster recovery plans;
  - emergency mode operation plans;
  - testing and revision.
- Security incident procedures.
- Security management process.

HIPAA compliance requires that healthcare organizations, their partners and subcontractors 'maintain reasonable and appropriate administrative, technical, and physical safeguards to ensure integrity and confidentiality of information, protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorised uses or disclosures of the information, and ensure compliance with such safeguards by the officer and employees of such parties'.

The cost of compliance is still a major issue in the United States.

Healthcare has come to rely significantly on technology, which comes in an increasingly diverse and complex array of systems and facilities. These often come in a variety of guises and platforms, and because of their specialized nature are not generally within the field of responsibility of IT management – the people who to a large extent were responsible for the evolution of BCM and to whom disaster recovery and restoration of facilities is second nature.

There is also a growing dependence on telecommunications technology, which links disparate healthcare facilities as well as offering alternative delivery methods such as telemedicine and internet-based services.

In this industry, equipment failure or incidents such as power loss can be a matter of life or death. Patient care organizations are particularly vulnerable, and incidents that are not properly allowed for, or protected against, will impact considerably on the reputation of the organization.

There is no other industry where the burden of responsibility is so onerous. Even so, there are many who feel that the issues of contingency planning and disaster recovery still need to be addressed more fully throughout the industry.

HIPAA will be a major influence in this process.

PRIVACY

In addition to requirements already referred to, there is an increasing body of legislation dealing with privacy and information security. While compliance is more a direct issue for others in an organization, business continuity personnel must be aware of the obligations that are imposed on an organization and of the negative publicity that would arise in the event of a conviction. This interest must also extend to issues such as ensuring that there are appropriate procedures and arrangements in place for the safe disposal of trash.

While there may be sophisticated protection in place for computer systems and data, the careless disposal of printed drafts could cause significant embarrassment. Financial institutions discard loan applications that contain personal information perhaps including income, credit card details and particulars of other loans. Lawyers and medical practitioners routinely discard sensitive information that they are obliged to protect. HR departments continually dispose of material from personnel files that may include not only remuneration information but medical records or even details of disciplinary issues.

The requirements of HIPAA in the United States have already been referred to. Equivalent legislation impacting on the financial services industry came into effect with the Gramm-Leach-Bliley Act (GLB), with a compliance date of 1 July 2001. A key provision of this law is that institutions must diligently protect customers' privacy. In addition to the more traditional financial institutions, this legislation also applies to organizations such as:

- car dealers that finance and lease vehicles;
- retail stores that finance consumer goods or issue their own credit cards;
- estate agents.

This legislation calls for customer information to be protected through proper security systems and procedures in eight specific areas. One of these areas is the secure disposal of records, documents, or other media formats.

DATA PROTECTION – EUROPE

In the EU, data protection legislation has been in place in most member states since the 1980s. The European Data Protection Directive (95/46/EC) was adopted in 1995 and has resulted in legislation being updated in many countries. This is geared to protect the privacy of personal data related to living individuals. It imposes strict rules in respect of the obtaining, processing, management, accuracy, security, disclosure and transfer of personal data.

The legislation has focused on:

- the security requirements in relation to the safeguarding of personal data;
- extending the coverage to manual data as well as processed data;
- the transfer of data outside the EU.

In relation to security, the following is typical of the requirements defined by legislation: 'Appropriate security measures shall be taken against unauthorized access to, or unauthorized alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.'

Previously, data protection legislation applied only to 'processed data'. Personal data that is processed manually is now covered by the legislation. There are transitional arrangements in place, but by October 2007 all relevant processing of manual data must comply with the specified data protection obligations. The inclusion of manual data is, however, subject to the qualification that manual data is covered only if the data forms part of, or is intended to form part of, a 'relevant filing system'. This is defined as: 'Any set of information relating to individuals to the extent that the set is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.'

The Directive 'prohibits the transfer of data to a third country which does not have adequate protection in place'. The European Commission can, and does, issue a 'whitelist' of countries whose data protection laws are deemed to be adequate. Transfers to companies in the United States can take place if the recipient company has signed up to the 'safe harbour principles' which is a privacy standard approved by the EU.

REGULATION AND BUSINESS CONTINUITY

All of the regulatory and legislative requirements described have underlined the requirement for appropriate business continuity practices. It is also important that the business continuity function in an organization is actively involved in ensuring that all of the requirements imposed are adequately addressed.

Case study 2.1

Eli Lilly and Prozac.com website subscribers

This case study tells how a company inadvertently released the e-mail addresses of 668 users of the medication Prozac.

Eli Lilly is an Indiana-based pharmaceutical company that manufactures, markets and sells drugs, including the antidepressant medication Prozac. As part of its marketing effort,

Eli Lilly operated a website, prozac.com, which the company promoted as 'Your Guide to Evaluating and Recovering from Depression'.

In March 2000, the company offered through prozac.com a service called 'Medi-Messenger' which enabled its subscribers to receive individualized e-mail reminders from Eli Lilly concerning their Prozac medication and other matters. On 27 June 2001 the company sent an e-mail to subscribers to the service informing them that it was discontinuing the prozac.com reminder programme. This e-mail unfortunately disclosed all of the subscribers' e-mail addresses to each individual subscriber by including all of their addresses in the 'To:' entry of the message. The company was made aware of the problem when it received complaints from several customers.

The Federal Trade Commission (FTC) in Washington DC became involved over allegedly false or misleading representations, made through Eli Lilly's privacy policies and during the sign-up process for Medi-Messenger. The Commission's complaint alleged that Eli Lilly claimed that it employed measures, and took steps appropriate under the circumstances, to maintain and protect the privacy of personal information obtained from or about consumers through its website, when in fact it had not employed such measures and had not taken such steps. It was of the opinion that Eli Lilly failed to provide appropriate training for its employees regarding consumer privacy and information security, and failed to provide appropriate oversight and assistance for the employee who sent out the e-mail.

The FTC mandated the company to take certain corrective steps.

This case highlights how easy it is for privacy entitlements to be breached accidentally. In this case it could have damaged the trust in and reputation of the company involved. Eli Lilly responded well to the incident. It apologized to the consumers, and quickly put measures in place to prevent a reoccurrence. The FTC regarded the responsiveness and the company's efforts to improve corporate privacy policies as a model for others to follow.

Absolute data security is virtually impossible to achieve. The American Civil Liberties Union (ACLU), the leading defender of individual rights in the United States and a strong supporter of strict confidentiality of personal data, played a significant role in highlighting and pursuing the Eli Lilly case with the FTC. It is ironic that in spring 2002 a relatively simple search of the ACLU website caused it some embarrassment by disclosing personal details of customers of its online store.

Disclosure of sensitive data, whether by accident or otherwise, is a major risk of modern business.

REPUTATION

> *Trust and reputation can vanish overnight.*
>
> Alan Greenspan, Chairman, US Federal Reserve

Dr Greenspan was referring to the Enron bankruptcy, where its main energy trading business failed because people lost trust in the group.

Trust and reputation in many ways equate to brand. There are many examples of reputation loss in BCM literature. These examples, and now more recent ones, feature at business continuity conferences and workshops. Two frequently quoted examples are Perrier and Ratners.

Perrier

The French company was the market leader in bottled water, with sales of around 1.2 billion bottles a year. It was expanding its market on an annual basis, and was geared up to increase production substantially when disaster struck.

This was not a fire, an explosion or a hurricane. In 1990, minute traces of benzene were discovered in some of the Perrier product. This was a major problem – especially for a company that emphasized the purity and quality of its water.

The company recalled some 160 million bottles and totally mishandled the publicity surrounding the scare.

- The following year production was at less than half the capacity of the plant and the bottom had fallen out of the market.
- Perrier domination of the quality water market was at an end.
- Other water companies took advantage of the situation and the marketplace is now totally changed.
- The Perrier share price plummeted, and in 1992 the company was acquired for a knockdown price, the equivalent of £1.6 billion or £1 per unit (bottle) of production capacity.

Ratners

This chain of jewellery shops was one of the most successful in the UK. It was built up over 40 years to be the country's leading high-street retail jeweller. This was largely through the efforts of Gerald Ratner who pursued a low-price, high-volume policy. In April 1991 Ratner addressed a group of business leaders at the annual conference of the Institute of Directors. He was then asked how his company could sell its product so cheaply. Jokingly, he said that essentially the product was rubbish – 'total crap'.

- The press got hold of this nugget, the story gathered momentum, and it was seen as a case of a retailer having disdain for his customers.
- The company was almost out of business within a year.
- In November 1992, Ratner resigned from the company.

This was all because of an ill-considered response by a senior executive to a simple question.

Attributes

Trust, reputation and brands are built up over years and perhaps generations. The creation of these attributes and assets will have been established through product quality, customer service and massive marketing spend. They may become household names such as:

- Coca-Cola
- Kellogg's
- McDonald's
- Microsoft
- Intel.

If handled correctly a crisis can actually enhance the reputation of an organization. Consider the case of Johnson & Johnson and the Tylenol contamination crisis in the 1980s. The company responded with quick corrective action that reflected a sincere concern for public safety. It exemplified the three Cs of the right response – concern, compassion and commitment. In reputation surveys, Johnson & Johnson continues to feature prominently at the top of the list. Compare that with the total mishandling of the Ford/Firestone tyre problem in the summer of 2000.

In some cases, brands may be the most valuable of a corporation's assets. They must be protected and BCM has a role in that protection.

Case study 2.2

Ford/Firestone tyre recall

In mid-2000 problems were identified with certain types of Firestone tyres, and in particular their use on Ford's top-selling, and highly profitable, Explorer SUV (sports-utility vehicle). This allegedly resulted in over 100 deaths, cost both companies billions of dollars, and severely damaged their reputations.

In the light of worries about possible safety defects in Firestone tyres, Sears, Roebuck & Co. stopped selling three brands – the same ones used on Ford's popular Explorer SUV. This put pressure on Ford to take action in the United States – it had already begun replacing the tyres on the vehicles sold in various other countries. Motorists had reported that the tread had a tendency to peel off, especially in warmer climates, causing accidents, injuries and deaths.

Ford and Bridgestone/Firestone responded by saying that the tyres were safe and blamed improper maintenance for most of the problems. This was despite the fact that thousands of tyres had been replaced in places as far apart as South America, Saudi Arabia and Malaysia. Even though complaints had been made as early as 1998, Ford and Firestone only got around to recalling and replacing the tyres in August 2000.

In August, Ford started to recall 6.5 million Firestone tyres even though Bridgestone/ Firestone, its business partner for almost a century, continued to insist that there were no problems with the tyres. Ford maintained that it was the problems with Firestone's tyre design and

manufacturing that caused more than 100 deaths linked to tyre failure. Bridgestone/Firestone then acknowledged that there were design and manufacturing problems but insisted that the design of the Ford Explorer contributed to the deaths. It published data showing that Explorer had five to ten times as many tyre failure claims as Ford Ranger pick-up trucks with the same tyres. It asked federal officials to investigate the safety of the Explorer's steering system. On the other hand Ford claimed that the problems did not arise with Explorers fitted with Goodyear tyres.

In May 2001, Ford planned to recall a further 10 million to 13 million tyres. Bridgestone/Firestone countered by saying that it would no longer sell tyres to Ford and that it no longer had trust in its relationship with the car maker. It blamed Ford's failure to acknowledge its responsibility as the reason for terminating the business relationship.

The replacement of the tyres cost Ford over $2 billion and its stock price took a hammering. Over the three-month period to September 2000 Bridgestone/Firestone saw its stock price drop by almost 50 per cent. From the perspective of the public both sides were to blame. Firestone tyres on other vehicles appeared to pose no significant risk. Explorers with other manufacturers' tyres appeared to be as safe as other SUVs. Regardless of the rights and wrongs, the public's confidence in both companies had been shaken.

The companies had failed to follow the correct strategy and fell into the trap that many groups fall into when things start to go wrong. The first response was one of denial. Having first denied that there was a problem they then tried to shift the blame.

They blamed each other and failed to realize that the problem belonged to both of them. This strategy alienated the public who felt that the recall and replacement programme was happening only because the companies got caught.

Our reputation is the most precious asset we manage. After last year's Firestone tyre recall, everyone at Ford Motor Co. has a very clear idea of the downside risks to reputation, and what they can do to you.

William Clay Ford Jr., Chairman, Ford Motor Co.

BCM IS NOT JUST FOR LARGE ORGANIZATIONS

Because a lot of the emphasis in the business continuity press, and in business continuity material generally, relates to large organizations and to the financial services industry, there is a feeling that it is not a matter of concern to the smaller business.

The financial services industry, generally, is ahead of most sectors when it comes to BCM. Because of the nature of the industry, its dependence on computer systems and operations – many of which are large scale and centralized – and the vast sums of money involved, BCM can be seen as a very expensive activity.

In particular, the promotion of computer disaster recovery planning has traditionally emphasized approaches to resilience and recovery that are geared to larger organizations. For the suppliers this is where the market and profit margins

are. The average small business would be tempted to say that this relates to a totally different league and level of operation, and accordingly from its perspective is irrelevant.

This is not the case. Research has shown that the small business community – the small to medium-sized enterprise (SME) or small to medium-sized business (SMB) – has been very slow to address the BCM issue and is very vulnerable. To a large extent a 'disaster' will have more far-reaching implications for this community than for the larger business. SMEs should be conscious that a computer virus, or an internet connection failure such as a problem at an ISP, could have very serious implications which could ultimately impact on business survival. It does not have to be a high-profile disaster or a terrorist attack.

BCM is vital for the smaller business. Increasingly, small businesses are under pressure from their customers and business partners to do business online. They may be dependent on key customers who insist on a high level of online availability or of interconnection with their systems. These customers may also refuse to do business unless they are satisfied that adequate business continuity plans are in place that address all critical processes and vulnerabilities.

Gartner estimates that only 35 per cent of SMBs have a comprehensive disaster recovery plan in place. They estimate, with a probability rating of 0.7, that this figure will grow to 50 per cent by 2007. Gartner also says that fewer than 10 per cent of SMBs have crisis management, business recovery and business resumption plans in place (*Preparing for a Disaster: Affordable SMB Actions*, March 2002). This is totally inappropriate in the trading environment in which such SMBs operate and which will become increasingly demanding.

Small businesses should remember that their biggest threats do not come from high-profile incidents such as earthquakes or terrorist bombs. It is the dozens of relatively minor issues such as prolonged power outages or computer network failures that may cause the problems. The vast majority of problems are caused by people or process failures. This is where the effort and investment should be concentrated.

Because of size, the process is simpler and the cost will be proportionally less than for larger organizations. The consequences of not having a plan are, however, likely to be disastrous.

ARE YOU READY?

- Do you have an active BCM programme in place in your organization?
- Is there a BCM mission statement?
- Is there a person appointed with overall responsibility for managing the programme?
- Has a risk management/BCM culture been established?

- Has a risk analysis or business impact analysis been done and has management endorsed the priorities and criticality which that process has defined?
- Is there an emergency/crisis management team?
- If there is a serious incident, are you aware of your role?
- Do key executives know their roles in a crisis?
- Are you familiar with the basics of the business continuity plan?
- Have key executives got a copy of the plan at a location where it would be quickly accessible?
- Is the plan tested regularly – when was the last time?
- Was it a realistic and worthwhile test?
- Does the plan deal with how to handle the media?
- Does the plan deal with people issues – communication with next of kin and trauma counselling?
- What is the link between insurance arrangements and contingency planning?
- Are you confident that your organization conforms to corporate governance requirements and any relevant regulatory requirements related to BCM?
- Are you aware of the arrangements for moving to alternative sites?
- Are you confident that the plans for IT resilience and contingency are adequate?
- Have the plans and processes been audited/appraised by external experts?

3

But we have insurance

Risk management and business continuity management are now embedded in the insurance purchase process. Insurers are now demanding good BCM practices.

Insurance is central to BCM – but it is not always given the attention that it deserves. There are at least three aspects of insurance that need to be considered in relation to BCM:

- Management may take the view 'we have insurance – why do we need to concern ourselves with BCM?'
- It is very important to work closely with those responsible for insurance cover in the organization and to understand exactly what is covered.
- The insurance scene has changed dramatically since the events of September 11, and unless you can convince your insurers that your organization has addressed the issues of business continuity it may be difficult – and certainly expensive – to get insurance cover.

WE HAVE INSURANCE

Some organizations take the simplistic line that just because there is an annual budget for insurance, risk is looked after and that there is no further need to worry. This they feel leaves them immune from threats and disasters, and anyway, these things happen to companies that are not insured.

They may also feel that by insuring their operations they will be immune from large disaster costs because the insurance will look after them. This is not totally correct:

- Insurance companies will look for the disaster avoidance and recovery plans and actions, and if they are deficient this will certainly impact on any settlement.
- If there is a claim, subsequent premiums will most likely increase.
- There are several types of coverage, and there is a need to be sure of precisely what is covered and in what circumstances.

This may be a minority view, but it does indicate the difficulties that those responsible for the implementation of business continuity have to face.

Insurance is a necessary part of the total business protection and recovery plan – but it is only a part.

- It may provide finance in the event of a problem arising. This money may not be instantly available and sometimes there can be a substantial delay before the cheque arrives.

- It will not keep customers supplied or guarantee that market share will be recovered.
- It will not protect the organization's reputation and image.
- Insurance for loss of profits, or for increased cost of working, will cover only a defined period – which in practice may prove to be inadequate.
- Proving loss of profits can be very difficult. The outcome may be based on historical performance and may not take account of recent market developments.
- It may be particularly difficult to prove loss of profits in the case of a service business, with arguments to suggest that the situation may be simply a case of deferred sales.

Nevertheless, insurance should be considered part of the continuity planning where an appropriate insurance strategy will provide a lifeline in the event of a disaster.

Case study 3.1

Argos – the internet '£3 TV' offer

In September 1999, the UK catalogue retailer Argos was inundated with online orders after a software problem led to top-brand 21-inch television sets being mistakenly priced at £3. The sets should have been priced at £299.99, but were offered at the incredible bargain price when the figure was rounded up to £300 and the zeroes were dropped by mistake.

At that time the Argos site was attracting some 100,000 hits per month. By the time the company discovered the mistake, hundreds of orders had been placed with a value in excess of £1 million. One person was reported to have ordered 1,700 sets.

Argos refused to accept the orders and apologized to its customers.

This was another case of acute embarrassment. Insurance will not address embarrassment or the impact on reputation. It also highlighted the effect a simple error can have in an active online environment and the speed at which the problem grows.

UNDERSTAND THE INSURANCE COVER

It is imperative that there is a close working relationship between those working on BCM and those in the organization responsible for insurance matters. Sometimes the insurance function protects its patch carefully, and this can lead to the two functions operating independently and ultimately to the detriment of the organization.

Often business continuity managers do not know what insurance is in place, and may simply assume that the insurance manager has considered all aspects and areas.

It tends to be only the larger companies that have a designated risk manager – although this can be industry dependent. Where there is no risk manager, insurance often comes within the remit of the finance director or chief financial officer. It can

be a responsibility that is tagged on to other more time-demanding duties of a manager within the finance function. In these situations, the risk management function may well be handled by the insurance broker. This arrangement assumes that the broker will understand the business and the nature of all the risks to be covered. The broker, or indeed the person in the organization charged with responsibility for insurance, may not understand the business or the technology. This can result in an insurance policy, or policies, that are not comprehensive enough or that are sufficiently ambiguous to leave the organization inadequately covered.

In larger organizations those responsible for insurance can be too remote from the operation. This type of situation can lead to confusion. Individual business units or subsidiary companies may expect that the corporate insurance function has looked after everything, while the corporate centre may expect the individual units to have looked after their own special requirements.

Everyone concerned should be fully consulted and aware of what is covered – and how it is covered.

The following types of questions need clear answers:

- What is the nature of the cover provided?
- Is it restricted to physical assets such as buildings and plant and equipment?
- What is the property valuation used – does it cover actual cash value or new for old?
- What is the nature of the cover in relation to IT and e-business?
- In the case of computers, in the event of a serious outage does it allow for increased cost of working and is this adequate?
- Does it cater for loss of business/profits and how has this been determined?
- Does it cover restoration of data? Is this adequate – in particular if valuable archive data needs to be reconstituted?
- How adequate is the business interruption insurance generally? Does it cover:
  - planned future business growth;
  - the impact on all of the elements of the business;
  - the contractual arrangements with key customers and suppliers;
  - the implications arising from the possible loss of physical access to the business?

If a disaster occurs, company personnel should be familiar with the procedures for contacting and dealing with the insurer. They should be clear about the steps to be taken to ensure that:

- the property is protected against further loss;
- appropriate salvage and restoration processes are implemented;

- the necessary actions are taken to ensure that the claims process is brought to a successful conclusion.

Insurers recommend that the following actions be taken as quickly as possible after a loss occurs:

- Ensure that the area involved is made safe.
- Report the incident/claim immediately.
- Restore fire protection.
- Protect undamaged property from loss.
- Take photographs of the damage.
- Consult with all relevant parties, including external advisers, to get an initial estimate of the extent of the damage, the likely timescale to recover operations, and the cost.
- Identify the immediate measures required to resume operations.
- Maintain safety and security of the site.
- Plan for the repair and restoration work.
- Request authorization from the insurer before proceeding with any significant repair work or any major purchases.

The whole process will be helped considerably by keeping detailed records and maintaining a close and trusted working relationship with the insurance providers from the start.

IMPACT OF SEPTEMBER 11

The events at the World Trade Center (WTC) and in Washington on that terrible day have had an enormous impact on the insurance industry throughout the world. To understand this, it helps to compare the cost to insurance companies of these events with the previous worst cases.

Most insurance industry sources estimate that the cost will be in the region of $50 billion, with some predictions that it may move into the $70 billion to $80 billion range. Over 3,000 lives were lost in New York, including at least 350 members of the emergency services and many IT professionals and others responsible for recovery efforts. Thirty million square feet of commercial office space was lost, of which less than half was in the two 110-storey towers of the WTC. Approximately 100,000 workers were displaced.

Before this the biggest ‘man-made’ disaster in terms of insurance cost was the Piper Alpha tragedy, which resulted in 167 deaths and cost $3 billion. In July 1988, a massive leakage of gas caused an explosion on the Piper Alpha oil rig in

the North Sea, north-east of Aberdeen in Scotland. This resulted in a fire that completely destroyed the platform.

Until recently the most expensive events for the insurance industry have been 'natural' disasters. Despite the extent and notoriety of these events they are still considerably less significant, in insurance terms, than September 11.

These were the main events:

- Hurricane Andrew in south Florida in August 1992 cost $20 billion. An indication of the scale of this disaster can be gauged from some statistics. The hurricane resulted in:
  - 38 deaths;
  - 700,000 people evacuated from the area;
  - 22,000 federal troops deployed in the largest US military rescue operation ever;
  - 175,000 left homeless;
  - 25,000 homes destroyed;
  - 7,800 businesses affected;
  - a $10 billion clean-up bill.
- Northridge earthquake in California in January 1994 cost $16 billion. This moderate but very damaging quake shook the densely populated San Fernando Valley in northern Los Angeles. It struck a modern urban environment, generally designed for seismic resistance, but it still resulted in:
  - 57 deaths;
  - 1,500 severe injuries;
  - 12,000 buildings damaged;
  - damage to the major freeway serving Los Angeles, as well as to 11 major roads in downtown LA and 170 bridges.

Because it happened in the early hours of a Monday morning, and on a holiday, its potential effects were reduced.

- The winter storms called Lothar and Martin in Europe in December 1999 cost $8 billion. High winds over a wide area, and a large amount of additional damage caused by heavy rain, were the hallmark of these storms. Lothar hit an area that stretched from the north-west coast of France to Paris, Switzerland and Germany, resulting in 80 deaths. Martin caused significant damage in areas such as southern Italy which were unaccustomed to such high winds. Further damage was inflicted by severe flooding and avalanches in the Alps.
- Typhoon Mireille in Japan in September 1991 cost $7 billion. This damaging storm led to the largest insurance loss in Japan. It resulted in:
  - 52 deaths;

  - 780 injuries;
  - 10,000 homes being flooded;
  - six million homes affected by power outages;
  - $3 billion damage to crops.
- Daria, the storm in Europe in January 1990, caused 95 deaths and cost $6 billion.
- Hurricane Hugo in the United States and Puerto Rico in September 1989 caused 86 deaths and cost $6 billion.

The losses arising from the events of September 11 are not just American losses – they are international. The financial loss will work its way through the insurance and reinsurance industry worldwide. Mergers and acquisitions have been commonplace in the insurance industry over recent years, and this means that most insurers and reinsurers are now large multinational businesses operating on a global basis.

The losses have already had a significant impact on insurance premiums – not just commercial but domestic and personal premiums too.

In addition to more expensive insurance, underwriters are now seeking evidence of how the practices of pro-active risk management and sound BCM have improved the quality of an organization's risks.

RELEVANCE TO BCM

In the recent past it may have been possible to obtain a reduction in insurance premium in the 5–10 per cent range by being able to demonstrate an active and effective business continuity programme. Such a reduction has been used as a factor, however minor, in justifying BCM in the past. This is no longer the case.

The issue now is: I may not get insurance cover at all unless I can convince the insurer that there is a BCM programme in place and that steps have been taken to manage and reduce risk.

Negligence on the part of the insured may lead to a reduced payment in the event of a claim. Does the failure to have a demonstrable and tested business continuity programme amount to negligence? It probably does.

In summary, the insurance scene has changed dramatically, and will continue to change, with significant implications for organizations and increasing emphasis on risk reduction measures and business continuity plans.

- Large companies are now setting up their own insurance companies – if the scale and distribution is right, this can result in lower costs and keep the money in the business.

- Insurance is now more expensive – premiums are increasing for all categories of risk.
- Open-ended cover is not as easily obtained as it used to be.
- Insurers insist that organizations manage their risks more actively and that there is an active BCM programme in place.
- Certain assets cannot be insured – goodwill, brand and reputation.
- Insurance is reactive – while it has its place, the whole process must be more proactive and BCM may be the key.

4

Good BCM – not token BCM

BCM is not just about the production of a plan. It is about installing a risk and business continuity management culture or mindset throughout the organization.

BCM – A SIMPLE PROCESS

Although BCM has developed its own terminology and mystique and can be surrounded by a variety of methodologies and software products, it is essentially a simple, commonsense process. It is important for the success of BCM that business continuity professionals speak the same language as their management colleagues and do not create barriers through the inappropriate use of terminology.

BCM is concerned with a few key concepts:

- realistic evaluation and management of risks;
- an understanding of what the business consequences would be if key facilities, processes, activities or people were lost;
- an appropriate strategy to limit damage and recover from an incident as effectively as possible.

There is, however, no such thing as a universally applicable approach to BCM. This is why the input of an experienced BCM professional is so significant to the success of a BCM programme.

The BCM process itself can be more important than the actual 'plan'.

- Plans will vary, as can be seen from the size and table of contents of different plans.
- Management awareness and the establishment of a business continuity culture in the organization can be as significant as an actual written plan.
- Key managers who have been through the BCM 'indoctrination' process and who know the processes at an operational level are invaluable and in an emergency may only need to refer to the plan for contact details.

These observations may seem to indicate that there is no need for a 'plan'. This is not the intention, which is to emphasize the importance of the process and of the establishment of the BCM culture.

The plan must fit comfortably with the culture and management style of the organization. For example, the type of plan that suits a financial institution would be totally inappropriate in a radio or television broadcasting organization.

The importance of the process and culture, rather than the nature of the actual plan, is not always appreciated by auditors or consultants. Very often the procedure is to

look for the big book and tick the boxes on the questionnaire based on this document. Quite often the box ticking is based on the table of contents rather than the book itself! This has given rise to the tactic of 'show them the size of the plan', and regardless of its unsuitability the boxes are ticked and no further questions are asked.

Do not measure your success in BCM by the size of the plans.

An irrelevant or out-of-date plan is worse than no plan

A distinction is drawn between a BCM programme that is alive and vibrant and one tolerated as an overhead that is not seen as contributing to the bottom line. Perhaps it is regarded as an activity that is there to keep the auditors and insurance people happy.

Unfortunately the sight of a detailed multi-volume plan with an attractive cover may be enough to ensure that the questioning authorities are satisfied. A detailed plan on an office bookshelf may look impressive but the chances are that it does not reflect the current situation and is largely irrelevant. Experience has shown that frequently plans are not updated following the introduction of new processes or systems, or the significant modification of existing ones. If the plan is not changed to reflect staffing and organizational changes at least twice a year, the responsibility and contact details in the plan will be poor.

There may be considerable technical detail in the plan that to the external or casual observer is too complex to evaluate and may indeed be of limited value. A bad plan, an out-of-date plan, or a plan that is so detailed that in an emergency it will be ignored by the crisis team, is often worse than having no plan at all. It can give rise to complacency and a false sense of security.

In a disaster situation such a plan could seriously impede progress towards recovery.

The single greatest influence that determines the state or condition of the plan, or of the whole BCM process, is the degree of active commitment to it by top management. The plan that has been inspired and promoted by a committed board sponsor is much more likely to be effective. However, this enthusiasm and commitment must be ongoing. If the original sponsor is no longer involved, someone must take over the reins, assume responsibility and pursue it with the same vigour.

The plan that is reluctantly undertaken because of pressure from the auditors or insurers is likely to be the one that is left to gather dust. A token effort may have been made to satisfy their basic requirements, and once achieved the personnel involved may move on to other things. There is unlikely to be a satisfactory sense of ownership of a plan that is conceived in this manner.

Sometimes these plans are simply copies of plans from other organizations – introduced by an external 'adviser', or obtained from a sister company within the

group. The plan may have been designed for a very different set of circumstances and may not relate well to the real requirements. In other cases a software package may have been used to generate the plan. Some packages are based on templates that can allow the quick production of a plan. It may be a substantial volume and may look impressive, but it will be useless unless sufficient work and thought has gone into the process.

Weekend disasters are easier to cope with

A good plan will have considered the implications of various types of incident at different points in time. For example:

- failure of the computer-based accounting system may have a much more significant impact at the end of an accounting period;
- the loss of a computer will be more serious if it occurs on the day the weekly payroll is due to be processed, or on the day that the electronic transfer of funds to employees' bank accounts should be done;
- problems with the automated production process will be very serious on a Thursday night for perishable products due to be delivered the following morning to the weekend retail trade;
- a serious incident at a major electricity generating plant is much more disruptive at a time of peak demand;
- failure of television broadcast transmission equipment just before the start of coverage of a major sporting event is much more serious than a problem that occurs in the morning off-peak viewing period;
- in an e-commerce type of environment where worldwide transactions are being processed there is no 'good time'.

Disasters don't often conveniently happen after the close of business on Friday, giving the weekend to get organized for Monday morning. However, the explosion at St Mary's Axe in London in 1992 did occur at the weekend, as did the bombing in Bishopsgate – in the financial heart of London – in April 1993. In both these cases the timing may have helped to alleviate the effect of having contingency plans that were less than perfect.

The Bishopsgate bomb exploded at 10.30 am on a Saturday which meant that there were almost 48 hours before business was due to resume. The timing may have allowed some organizations to survive better than if the explosion had occurred during the working week. Another aspect to the incident is that the City is almost deserted at the weekend. If the explosion had happened during the week a wider exclusion cordon would have been necessary. Accordingly, apart from the probable significant loss of life, many other organizations would have suffered from denial of access to their premises – one of the most disruptive of disaster scenarios.

Informal arrangements don't work

In the past some organizations depended on reciprocal arrangements with other organizations and 'best endeavour' type agreements with critical suppliers. These types of arrangements operated mainly for computer and telecommunications services.

The days of largely informal arrangements between companies to help each other in the event of a disaster are long gone. Apart from the possibility of the other organization also being affected by the disaster, the difficulties of ensuring compatibility between both operating environments are significant. This might have worked in the days of batch computing or for computer applications such as payroll, but it is irrelevant now.

Supplier goodwill may also have worked in an era when the technology lifespan was much longer. There was also the possibility that equivalent technology models were still coming off the production line three or four years after acquisition by the company. The rate of technology change and the extent to which just-in-time production operates means that this is no longer a viable option. No matter how significant an organization is to a supplier, it is not sufficient to rely on informal arrangements. The supplier will help out as much as possible, but if the 'disaster' also impacts on a number of its customers, the supplier will have difficulties in sharing skilled personnel and replacement equipment among all.

The only real option is to have formal contractual arrangements – service level agreements (SLAs) – with critical suppliers.

IS BCM EXPENSIVE?

The quick answer to this question is no. But BCM can be, and sometimes is, used to attempt to justify expenditure and this must be guarded against.

In reality, many components of BCM cost very little in terms of capital investment.

Generally, the most significant and important aspect of BCM is the establishment of a BCM or risk management culture in the organization. This culture then influences all key business decisions. For example, the case for new capital investment must include consideration of issues such as resilience and contingency. The cost of catering for adequate resilience and contingency should be regarded as an essential element of the cost justification of a project.

Do not entertain the attitude, 'the project is viable and justifies the investment but now I have to build in features to satisfy the BCM people and this should not be charged to the project'.

If these considerations are addressed from the start of a project, it will be much more cost-effective than trying to implement them or retrofit at a later stage.

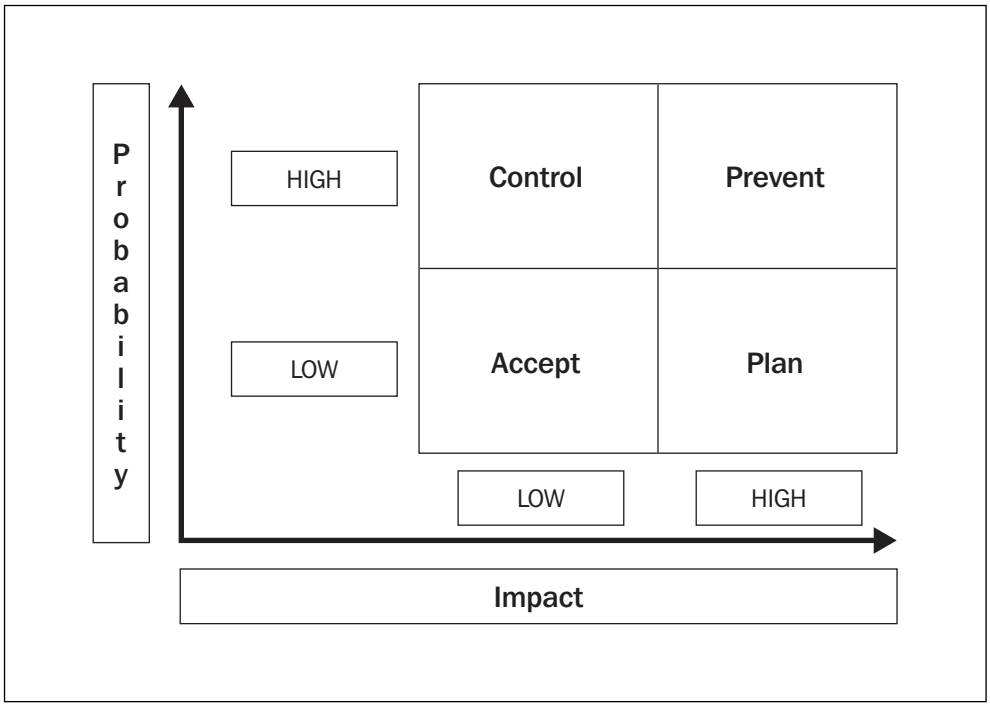
With BCM, the important thing is to identify the risks and the measures that can be taken to reduce those risks to an acceptable level. Then having costed the

options, the situation should be presented to the board or the relevant decision-making authority. It is then their responsibility to make an informed decision. That decision may be to proceed and in doing so accept that there is a level of risk that must be lived with. This is an executive decision – but one that has been made following consideration of the relevant BCM and risk factors.

Any investment is required mainly in people's time and in training/awareness. This is necessary to ensure that people consider business continuity in all of their business thinking, to allow them to envisage disruptive scenarios, and to develop and implement the appropriate action plans. One of the pitfalls is to invest in the wrong processes or activities. This is where the benefits of business impact analysis (BIA) come in. The BIA process will identify and rank the business processes, criticalities and dependencies. On this basis investment can be determined, justified and prioritized.

Figure 4.1 indicates that decisions in relation to risk should be based on the assessment of the probability of the risk becoming a reality, and of the impact that it would have on the enterprise.

Fig. 4.1 Risk matrix



BCM IS POSITIVE AND INCLUSIVE

There has been a major change in emphasis from focusing on things going wrong to the more positive aspects of business continuity. This is one of the main differences between BCM and the earlier emphasis on disaster recovery planning,

but many people still regard BCM and its practitioners as being solely concerned with the steps required to recover from a disaster.

The word 'business' in BCM has tended to give the impression that it relates only to commercial operations. The prominent role which the financial services sector has played in the profession may also have encouraged this perception.

BCM is applicable to every organization in both the public and private sectors. It is now accepted as important in areas such as:

- government departments
- public utilities
- local authorities
- education
- healthcare
- voluntary bodies, charities, sporting bodies, etc.

In selling the concept of BCM, emphasis must be on the positive aspects and on how it can contribute to the organization. It will then have a better chance of being endorsed and promoted by management.

CO-OPERATION

The broadcasting industry was seriously affected by the destruction of the World Trade Center because most New York television stations had their main transmitters on the towers. Only two stations were in a position to stay on air immediately after the disaster happened because they had back-up transmitters at the Empire State Building. It was almost two weeks before most NY City radio and television stations were back on air – and then with weaker signals. The amount of advertising revenue lost has been estimated at $1 billion.

The broadcasters then formed a coalition to consider how their requirements for greater resilience in the transmission process could be achieved. They wanted to find a cost-effective way of staying on air, and became involved in arrangements to share each other's facilities in the event of an emergency.

In the past there was a significant degree of co-operation between companies in relation to helping one another in the event of serious computer problems. This was fostered by trade associations and computer user groups. For a variety of reasons this became impractical and now companies tend to work independently and confidentially on their business continuity arrangements. This is evident from the reluctance of many organizations to present real case-study experiences at business continuity conferences.

There is considerable scope for more openness in this area – without necessarily disclosing trade secrets. It is now anticipated that there will be a greater exchange of ideas in business sectors. There are also undoubted benefits to be gained from a more communal approach to working with local infrastructure providers and emergency services in developing strategies and plans.

Discussing your business continuity plans with colleagues in the same industry, and indeed with your competitors, can be smart business.

PEOPLE ISSUES

Until recently, many plans have virtually ignored the fact that a disaster could result in significant loss of life. In the case of the more traditional threats such as fire or flood, the presumption was that there would be time to evacuate the premises or area. Some loss of key personnel may have been considered and this may have resulted in recommendations regarding succession planning and back-up for key staff. There may also have been a recommendation that senior executives or specialists should not all travel together.

Terrorist attacks now show that people can be lost – not just buildings, computers, plant and equipment and stock.

Recent events have also concentrated attention on the traumatic impact of disasters. The psychological impact of trauma can be very serious – in some cases more serious and prolonged than physical injury. Trauma can occur not simply in the case of people who have been directly involved in the incident. It can affect work colleagues in other locations, personnel in the emergency services, staff involved in managing and working on the response to the incident, local residents, and, of course, friends and next of kin of the dead and injured.

As seen in the aftermath of September 11 feelings of guilt can also be traumatic. The causes of guilt may range from concern that some health and safety precautions were not adequate; that there could have been more evacuation drills; the implications of having swapped a shift, called in sick, left early or arrived late; to having been on holiday on the day.

Reference is made elsewhere to the importance of ensuring that people involved in crisis management will operate effectively in times of crisis. Trauma can render even the most effective executive powerless.

In a recovery situation, certain staff will be required to make a massive commitment in terms of time and energy. Adrenalin may keep them going for a period, but eventually the situation will catch up with them and their contribution will suffer. Many plans do not adequately allow for relief for recovery personnel.

In post-incident reviews this can be one of the key findings – too much was expected of too few.

COMPREHENSIVE APPROACH

Ensure that every aspect and all eventualities are considered in the process. One factor that contributes to this is the allocation of valuable and experienced personnel to the programme. This will help to avoid the 'if only' scenario.

If only:

- we had known that the combination of very heavy rain, very high tides and an easterly wind had caused severe flooding in this area before;
- we had taken the computer back-up tapes off-site;
- we had known where the water shut-off point in the building was;
- we had found time for proper fire drills;
- we had realized the importance of the documents held in the company secretary's department;
- we had invited the local fire service to develop a pre-fire plan for our site;
- we had ensured that we had the source code of the computer-based process control system before the supplier went out of business – or at least had it deposited in an escrow account;
- we had followed up on our policy of not overloading electrical circuits;
- we had signed up for more frequent updates of the computer virus protection software.

COMMON WEAKNESSES IN BUSINESS CONTINUITY PLANNING

- Inadequate senior management support.
- Insufficient financial support to implement essential contingency arrangements.
- Failure to take a holistic approach.
- Lack of clear understanding of the responsibilities for the initiation, development, implementation and ongoing management/maintenance of the plans and the process.
- Inappropriate ownership – process controlled and 'owned' by specialist group rather than by line management.
- Failure to involve all relevant parties – such as internal audit.

- Plan stops at site gate – it does not consider external factors adequately.
- Inadequate contact with, and understanding of, the role of the emergency services.
- Poor risk analysis/business impact analysis.
- Insufficient training of all concerned.
- Insufficient or inadequate testing/exercising.
- Balance not right between clear action plans and detailed operational plans.
- Inappropriate mechanism for keeping the plans current – documentation out of date.
- Plans do not reflect latest organizational, systems, process or technological changes.
- Plans not held in a place where they are readily accessible when required.

5

How do I get started?

In preparing for battle I have always found that plans are useless, but planning is indispensable.

Dwight D. Eisenhower

The first step must be to get the necessary commitment at board level.

The BCM sponsor will emerge from this process and a business continuity manager must then be identified and appointed. This position must be full-time if BCM is to be taken seriously. This means that while the person may have responsibilities in associated areas such as risk management or computer security policy, BCM is not something to be given to someone who has another executive role where BCM is regarded as an add-on. Neither should it be given to someone simply for the sake of giving that person something to do.

A sample job specification for a business continuity manager is included in Appendix 2. A suitable person in-house could quickly learn the business continuity skills required – even if some external assistance is needed for a time.

At this stage the awareness programme must start. Managers and staff should be made aware of the significance of BCM to the organization and of the commitment to it. This may be done through communications from the CEO, presentations to groups, the company newsletter and the intranet. BCM must be sold positively and everyone should be convinced that it is essential. This is also important from the perspective of getting the right people involved from every area of the business – if they do not know what BCM, is why would they want to get involved?

The decision as to the extent, if any, that external help is required to get the process under way must be made at this stage.

All directors/heads of function should be asked to nominate appropriate representatives from their areas to represent those areas on the BCM working group. These representatives should be chosen for their knowledge of their areas/functions and their commitment to the concept.

BCM WORKING GROUP

The establishment of a working group is very helpful in making BCM a success. The group should represent all the parties involved. These areas or functions may include:

- insurance
- security
- damage and salvage assessment

- public relations
- human resources
- information technology – hardware, software, networks (LAN, WAN), PC support/help desk
- voice communications
- building services/infrastructure/property/office services
- transport
- finance
- procurement
- legal
- internal audit
- customer service
- sales and marketing
- production and distribution.

Meetings should take place at regular intervals, usually monthly, and ideally should last for no more than one hour.

The purposes of the group and the meetings are:

- to ensure that every area is aware of what is happening at organization level and in other divisions;
- to provide a means of ensuring that no aspects of the organization are missed in the planning;
- to report progress;
- to review timescales, targets and the appropriateness of the approach being followed.

This group should be chaired by the business continuity manager.

The notes on these meetings will be important in keeping the executive sponsor, auditors, and all other interested parties informed on progress.

BUSINESS IMPACT ANALYSIS

Business impact analysis (BIA) and risk analysis are closely related activities and a certain amount of this will probably have already been done by the time the programme actually starts.

BIA is an analysis carried out at a reasonably macro level which identifies the impacts of losing business functions or resources. There are various ways of approaching BIA. It can be approached quite informally, or a more formal

approach can be taken which involves the use of detailed forms or questionnaires. The approach depends on the nature of the organization – size, structure, local or international, etc. In some cases the impacts and priorities will be obvious to all without any significant exercise.

The BIA process requires interviews with senior managers – thus also increasing awareness of it and its profile. In all cases it is a question of ascertaining and quantifying the impact of losses and then ranking them in order of importance. Forms are often used in order to standardize the approach. The type of forms can range from those with a small number of headings, which act as a type of agenda at meetings, to ones with considerably more detail. Typical headings are:

- nature of function;
- impact of problems from different perspectives – image/reputation, costs involved, loss of future business, etc.
- impact of problems at different times of the day, week, month and year;
- what, if any, resilience could be provided now – easily and quickly?
- recovery – how long would it take to recover, what are the priorities for resumption, what will the backlog be, what would the additional cost of working be, what does the insurance cover?
- what workarounds are available and how would they operate?
- what are the continuity and recovery requirements – accommodation, computer systems, etc?

BIA is an exercise about the ability to home in on the things that are important rather than the 'hobby-horses' of particular managers. Managers will have different perspectives ranging from 'there is no problem here so it doesn't concern me' to 'my function is the most critical in the business, and I need many levels of resilience built in, ready-to-roll recovery arrangements at an alternative site, etc'.

Business impact analysis – suggested report format

- Introduction
- Executive summary
- Background to study
- Current state assessment
- Threats and vulnerabilities
- Critical business functions/operations
- Business impacts – operational and financial
- Potential strategies

- Recommendations
- Conclusion
- Appendices

USE OF CONSULTANTS

There is no point in trying to pass off the responsibility for BCM to external consultants. BCM must be regarded as a management responsibility and owned by management. There are, however, roles that experienced consultants can play and which, if used appropriately, can greatly enhance the programme.

Consultants can bring a new perspective to the process. Their experience in equivalent businesses or industries may mean that by adapting an existing methodology or approach, which they have used already, they can speed up the process considerably.

Consultants can also help to ensure that the project gets better support and involvement from both senior and operational management. The consultancy budget may help the project to get more attention from senior management.

The contribution of the consultant will be worthwhile only if the involvement is properly thought through and managed – which is no different to the requirements for the successful engagement of consultancy in any other area of business activity.

The keys to success are:

- overall responsibility for and direction of the project must remain with management;
- consultants should be used to help in achieving the goal – they should not be allowed to take over the project; this is particularly the case with BCM since it has no definite end and is a continuing process – it could be a consultant's dream in terms of a never-ending assignment;
- the consultants' role should be very clearly defined and communicated to all involved with the activity;
- definite timescales, deliverables and fees should be agreed before commencement.

Types of consultants

There are a few different types of consultants operating in the BCM area. They range from the 'one-man-band' through to the specialist departments of the major international consultancy firms.

Because of the nature of the BCM business and the value that can be added to the activity by suitably experienced 'outsiders', the use of the smaller specialist

consultancy company, with vastly experienced personnel, can be very effective. This type of company, while offering significant experience, can be in a position to offer a more flexible type of service and significantly better value than the larger operations. Often what is required is someone to help set out the framework for the process, to give it a kick-start, and to assist on an occasional basis to check how things are going. A consultant may also be useful where there are issues relating to crossover or blurred interfaces between departments, and also to provide an occasional healthcheck over a period of years.

In some cases the larger firms cannot provide the same degree of continuity of personnel over the longer term. There are also cases where very bright, but relatively inexperienced, trainee consultants are hired, trained in the firm's BCM methodology and software tools, and then released to clients. This type of situation can lead to the production of a very impressive looking plan. This plan can be effective but in some cases will also reflect the inexperience of the consultant.

Some of the companies that provide a variety of business continuity services, such as hot sites and serviced work areas, also provide consultancy services. Companies that specialize in the provision of disaster-tolerant computer hardware, storage and software are also involved in consultancy. Consultants from these sources specialize in advice that is often related to their main line of business, but can also provide independent advice that is not product related.

There are also some consultancy firms that feel that BCM is simply another project, and that assigning a good project manager is the most significant requirement. This is not always the case, and it can be an unsatisfactory approach.

Which type is best?

There is no simple answer as to which type of consultant is best. The answer depends on a number of factors such as:

- the role envisaged for the consultant;
- the status or maturity of business continuity within the organization;
- the nature of the organization – some firms of consultants may specialize in particular industries, and if the company is a multinational one with plants around the world it may be necessary to work with one of the international consultancies;
- where business continuity sits in the organization structure – e.g. as part of a corporate-wide risk management activity or as something that is being advocated or sponsored by the internal audit function;
- the relationship already established with a major consulting firm – they will know the organization, and while a specialist department will be involved they will benefit from the background knowledge already available;

- the possibility of extending the brief of consultants who have already been involved in working with the organization in areas such as IT resilience and disaster recovery planning.

Generally, it is better to work with firms that specialize in the area. Firms specializing in business continuity are in a better position to provide a good service than firms offering a broad range of services that may range from auditing through to multi-faceted consultancy.

The latter type of firm may not have the in-depth practical experience, and this can result in:

- spending too long coming to terms with the organization and the issues;
- engaging key staff in unnecessarily long meetings trying to understand the issues – managers soon get fed up and lose interest in the project;
- proposing solutions that can err on the side of protecting the consulting firm from possible blame or liability, resulting in significant implementation and compliance costs for the organization;
- the use of methodologies that are time-consuming and that emphasize considerable detail rather than getting to the point.

The most effective business continuity consultants are not necessarily those who continue to make impressive presentations to senior management. Rather, they are those who ensure that the objectives are achieved and that the client's management is adequately supported at all stages of the project and so able to liaise effectively with the board. Those who make impressive presentations may be more concerned with ensuring that they are indispensable to the project, thus ensuring further work.

Areas for consultancy

Consultants may be useful at every stage of the BCM programme. There are a number of areas or activities that can benefit from the use of consultancy.

First, the client must ask what the reasons are for involving a consultant.

- Is it someone to initiate the project?
- Is it to help make the case for BCM and to help to sell the concept to the board?
- Is it to run the project because there is no suitable person available with sufficient time?
- Is it to supplement the available internal resources in order to achieve a desirable implementation timescale?
- Is it to have an experienced professional available to the project? Someone to work with throughout the project as an adviser, sounding board and facilitator?
- Is it to provide technical expertise in certain areas such as IT resilience, back-up and recovery?

- Is it to avoid having to send staff on expensive courses? To train staff by having them work alongside the consultant and benefit from knowledge transfer in this way?
- Is it to evaluate the relevance and effectiveness of existing plans?
- Is it to assist with the exercising, or testing, of the plans and to provide an independent assessment of the value of the exercise?

Selecting consultants

Once it is decided to use consultancy services, and the requirement has been clearly defined, the process of selecting the most appropriate supplier must take into account a number of factors.

- Have the terms of engagement and the deliverables been clearly defined?
- Is there a fixed price for the expected deliverables? Arrangements based on time and materials should be avoided if at all possible. An exception arises where the contract is to provide a number of days of expertise rather than defined deliverables.
- Do the proposals from consultants provide details of the phases, tasks, milestones and associated costs for the project?
- How independent are the consultants? Have they got alliances with vendors in the business continuity marketplace – e.g. providers of computer hot sites? Such alliances may have advantages, but may also impinge on independent advice. It is important to be aware of any such alliances before making a commitment.

Some of these factors relate to the consulting organization itself, but the key issues concern the people who will be doing the work. Regardless of the size and reputation of the firm, ultimately it comes down to the actual personnel who will be assigned to the project. The presentation to management may have been done by a senior manager or partner who made a major impression, but this person may have a relatively minor role in the assignment.

It is important to establish a number of facts about the people who will carry out the assignment.

Qualifications

- Who is/are the consultant(s) who will do the work?
- What are their qualifications?
- What is their track record?
- What organizations have they worked for?
- Have they produced business continuity plans?

- Did they do a good job and can these clients be approached for references?
- Have they verifiable expertise in the industry or activity in which they will be involved?
- Are they members of a professional body, such as the Business Continuity Institute, Disaster Recovery Institute International or Emergency Planning Society?
- How good are their interpersonal skills? How well will they get on with our people?

QUESTIONS FOR THE CIO OR IT DIRECTOR

General

- Do you have an IT business continuity plan/disaster recovery plan?
- Is business continuity/disaster recovery an agenda item for IT management meetings?
- When was the plan last updated?
- When was the plan tested with a realistic exercise?
- Are all contact details up to date?
- Have key managers got copies at home?
- Are responsibilities clearly defined for plan maintenance, training and testing?
- Is there one particular person, with deputies, who has responsibility for managing activities in the event of a disaster?
- Are all staff members fully briefed on their responsibilities in this regard?
- Have the priorities as defined in the plan been agreed at executive level in the organization?
- Have user departments been involved in drawing up and testing the plan?
- Are user department processes taken into account in testing?
- To what extent are IT plans part of and consistent with the overall BCM process in the organization?

Technology

- Do the plan and the back-up arrangements adequately cater for the technology in use – models, releases, versions, etc.?
- How quickly can IT operations be restored in the case of different disaster scenarios?

- How adequate are the LAN and WAN resilience and back-up arrangements?
- What is the resilience/recovery strategy – built-in redundancy, multiple nodes, clustering, mirroring, multiple sites, hot site, cold site, etc.?
- What SLAs are in place with third-party suppliers?
- Do these SLAs provide for automatic and immediate switch over to alternative computers – if not, what is the expected time lag?
- What type of agreements are in place with data communications suppliers?
- Do alternative arrangements cater for disasters that might impact on a region and not just the site – such as power or telecoms failure?
- Have the plans been verified or evaluated by independent third parties?
- Is a UPS (uninterruptible power supply) facility in use – can it cater for the critical load and is there a formal maintenance arrangement in place?
- Are back-up generators installed – are they serviced and tested regularly?

6

Preparing the plan

When a crisis occurs is not the time to do the planning.

If business continuity plans are too detailed they will be useless and ignored in a crisis.

People go on courses or buy books and expect to find a format or template that they can use to produce a business continuity plan (BCP) quickly. While there are many formats, and software is available to provide assistance, there is no silver bullet. There is no single format that suits all organizations. The process of creating awareness and establishing a BCM culture in the organization takes time and in many respects can be more important than the actual documentation of the plan.

What is most appropriate for your organization depends on a number of factors, and in some cases the plan will be little more than a list of key contacts. The process of awareness creation, discussion of the various resilience and recovery options available, and of who is responsible for what in the event of an emergency, will have created an environment in which the organization is more prepared for a crisis. Managers who have been through this process, and who have an in-depth knowledge of the business and work processes, will instinctively know what to do – such as get on site and contact the right people.

This is not to say that there should not be a more extensive written plan. It is particularly relevant where there is a significant staff turnover or there is the possibility that key, knowledgeable staff may not be available. There are also some areas where it is essential to have detailed plans and procedures. One such area is IT, where the basic plan must be supported by comprehensive documentation on back-up and recovery procedures, alternative network switching arrangements, alternative off-site location arrangements, etc.

Despite the reservations expressed, a sample table of contents for a corporate ('ABC') BCP and the typical content of the departmental arrangements that should support such a plan are included below. Also included is an outline table of contents prepared by the Contingency Planning Exchange (CPE) and Project Impact of the Federal Emergency Management Agency (FEMA), both of the United States.

SIMPLICITY CAN BE THE KEY

People are expected to be familiar with the plan and to use it in an emergency. What happens if a manager is informed at 4.00 am that the main production facility is flooded or that the office block is on fire? If the plan is a detailed, multi-volume one it will be ignored as the emphasis will be on getting to the site fast and getting things done.

Plans that are too detailed can be worse than not having any plan. In an emergency the result can be that some people attempt to follow the plan while others ignore it. A complex plan will also be hard to keep updated. Apart from the amount of work involved, it will become a nuisance for plan-holders to have to come to terms with masses of replacement pages.

Detailed plans may also be over-prescriptive. In an emergency, decisions must be made. Managers need flexibility to act as events unfold. A good plan will keep instructions to a minimum, and they will be expressed as simple action points.

Very few staff need the complete plan. Give individuals only the sections that are relevant to them.

Consider the essential elements of a plan. There is no reason why they cannot be described briefly and still communicate the message effectively:

- Plan invocation – when and by whom.
- Roles and responsibilities of the crisis management team.
- Contact details for crisis management and recovery teams, senior management, emergency services and other organizations who will be involved in recovery, as well as for key staff, customers and suppliers.
- The business processes to be recovered – priorities, how, where and timescales.
- Recovery steps.
- Communications with the media, staff and business partners.
- Arrangements for testing and updating the plan.

An overly complex plan will not survive.

ABC BUSINESS CONTINUITY PLAN

Introduction

Plan overview

- Scope of plan
- Structure of plan
- Plan synopsis
  - If an incident occurs
  - What is a disaster?
  - ABC policy statement – overview of strategy

- Plan co-ordination
  - Business recovery objectives and priorities
  - Definition of responsibilities
- Premises, plant and facilities
  - Services/facilities co-ordinators
  - Initial assembly points
  - Command/control centre
  - Standby sites/arrangements

Emergency response plan

- Introduction
  - Background
  - When to invoke the plan
  - Roles and responsibilities
  - How to use the plan
- Notification and activities
  - Staff notification procedures
  - Contact lists/telephone numbers
- Incident response
  - Incident response team and role

    Incident response procedure – key first priority and interim recovery options

    Internal contacts

    External contacts
  - Activity log
- Recovery support teams
  - Damage assessment
  - Human resources
  - Safety and environment
  - Legal, property and insurance
  - Purchasing/general services
  - Public affairs (public relations)

Computer security/virus attack plan

- Summary of policy, responsibilities and authority
- Incident response procedure
- Internal contacts
- External contacts

IT/systems plan

- Overview of plan
- Incident response procedure
- Internal contacts

Telecommunications plan

- Overview of plan
- Incident response procedure
- Internal contacts

Business area plans

- HQ production (HQP)
  - HQP overview
  - HQP incident response
  - HQP staff contacts
  - Recovery tasks
  - Resource requirements
  - Vital records, materials, equipment and IT services
- HQ warehouse (HQW)
  - HQW overview … etc. as for HQP (and equivalent for business areas below)
- HQ transport and distribution (HQT&D)
- Sales and marketing
- Finance
- Executive/corporate services
- Human resources
- Region A facility …
- Other business units …

Plan administration

- Version control/plan maintenance – change log
- Distribution/list of plan holders/security
- Plan testing procedure and history

DEPARTMENTAL PLANS

Introduction

- Describes where the plan fits into the overall process.
- Names and contact details of the BC co-ordinator and deputy BC co-ordinator
- Outlines the role of the departmental BC co-ordinator (DBCC).

In the event of an incident that is classified as serious (or as a disaster), the DBCC will be contacted immediately. It is the responsibility of the DBCC to contact the department manager and the key members of the departmental team and to respond to the incident in the manner described in the department's BCP. This presumes that the DBCC and deputy DBCC are thoroughly familiar with the BCP.

The DBCC is responsible for ensuring that the department's BCP is kept up to date, and that all critical functions are continued in the event of disruption.

Description

- Brief summary of the plan for the department. This refers to the nature of the business recovery team and lists the critical business functions.

Plan activation

- Actions to be taken and by whom.
- Actions during first 72 hours – business function, day, evening, team member, action, comments.
- Actions after 72 hours.

Contacts

- Key staff – name, address, phone (home and mobile), deputy details.

Alternative operations

- Processing vital functions manually.
- Move to alternative location.

Computer-based vital records

- Business function, file/record name, reconstruct last 24 hours.

Non-computer-based vital records

- Business function, file/record name, reconstruction.

External contacts

- Contact details of key customers and suppliers.

CPE/FEMA BUSINESS CONTINUITY PLAN

1. Introduction

1.1 Scope

Specify what business activities this plan will address. Include the plan's boundaries and exclusions. The boundaries will place limits on what the plan will cover and the exclusions are the things a plan will not address.

1.2 Objectives

State the goals of the plan in terms of key functions and timeframes. Describe all of your work functions and prioritize them in order of their impact. Identify the maximum amount of time that one of your activities could go unperformed before significantly impacting your customers and the overall business.

1.3 Assumptions

List conditions that are assumed to be true when planning.

1.4 Strategies

Provide an overview of the recovery strategies that are in place that will help your business get back up and running after a serious emergency. Examples include copies of critical files kept off-site, the ability to work from home, and the back-up of your required computer programs and files.

2. Emergency response plan

2.1 Evacuation procedures

Outline how personnel should vacate the building in an orderly and safe manner. Include designated emergency assembly areas for staff temporarily to congregate immediately after leaving the building.

2.2 Notification procedures

Describe the emergency communication process once an emergency situation is discovered. The procedures must identify who should be immediately contacted and by whom.

3. Continuity plan

3.1 Roles and responsibilities

Identify the key responsibilities for employees throughout the recovery process. Tasks should specify roles and responsibilities for each person. Tasks should be assigned to primary and alternative team members. Procedures should be explicit so members can readily perform the functions if necessary.

3.2 Plan invocation

Describe the criteria and process for implementing the plan. This process should include procedures for activating alternative processing sites and support personnel and services. Include how vital records will be recovered from off-site storage locations.

3.3 Continuity requirements

Outline the required resources and logistics to support the continuity workflow process. Identify the resources needed to continue business functions within the required timeframes, and provide an inventory of the requirements for your recovery solution.

3.4 Function procedures

Describe the steps required to recover your work functions. For example, how will work change now that you are no longer processing as normal?

4. Restoration plan

4.1 Roles and responsibilities

Identify the key responsibilities to be performed throughout the restoration process. The restoration process includes how files and equipment are restored or replaced. It also includes how your original office space will be restored or replaced. The assistance of your building management office, landlord and insurance company is vital.

4.2 Plan invocation

Describe the criteria and process for implementing the restoration plan. This process should include procedures for support personnel, services, and considerations for returning to the home site or a replacement site.

4.3 Restoration requirements

Outline the requirements and resources needed to support the return to the home site or move to the replacement site. Identify the personnel who will be involved in preparing a comprehensive damage assessment. Be prepared to identify what is salvageable and what should be replaced, using your insurance agent's recommendations.

4.4 Migration procedures to primary site

Identify a plan and schedule to move employees to the home or replacement site. Other procedures include deactivation of the back-up site.

5. Maintenance plan

5.1 Quality assurance programme

Describe the method for keeping the business continuity programme current and consistent with business strategies and objectives. Included in this programme should be a process to update the business continuity plan and distribute and record the changes.

5.2 Exercise programme

Outline the ongoing process to validate and strengthen the business continuity programme. The exercise programme is a high-level description of exercise or test plans which include development, implementation, critique and documentation process. An exercise plan is a detailed collection of objectives, tasks, roles and responsibilities to guide the exercise participants through a single exercise.

Appendices

I. Emergency contact directories

- Business continuity team structure and contact listing

- Employee call tree and contact listing
- 24-hour contact list of emergency services (fire, police, hospital, power, water and sewer utilities, local emergency management agency, local American Red Cross office, FEMA, etc.)
- Customer and vendor contact lists

II. Checklists

- Team tasks
- Continuity requirements
- Damage assessment

III. Reference documents

- External agreements
- Service level agreements
- Risk assessment/risk analysis document
- Business impact analysis
- Floor plans

Source: Contingency Planning Exchange and FEMA website (www.fema.gov)

CRISIS COMMAND AND CONTROL CENTRE

Location

- Location should be predetermined – it should not be a question of seeking a venue when disaster strikes.
- The usual approach is to think in terms of conference rooms in headquarters. These may be destroyed or inaccessible in the event of an incident. A number of options should be considered – training centres, hotel or other third-party facilities, another company site or the back-up recovery site.
- Should it be a single room or a multiple-room facility?

The location and nature of the centre will be influenced by the type of functions to be carried out there. Initially these will be:

- gathering facts;
- evaluating the situation;
- assessment of the options available;
- determining the actions to be taken;
- issuing instructions;
- communicating with staff;
- communicating with the media;
- monitoring progress.

Resources required

- Office furniture and supplies.
- Computer equipment – PCs, printers, LAN, access to e-mail and internet.
- Power – including uninterruptible power supply (UPS) units and back-up generator(s).
- Communications facilities – with as much resilience and diversity as possible; telephones – landlines, satellite and cell-phones, fax.
- Television and radio receivers – aerial, cable and satellite connection, VCR recorders, video/digital cameras.
- Documentation, including copies of:
  - business continuity plans;
  - policies and procedures, including incident response procedures, evacuation arrangements;
  - crisis management and business resumption arrangements, telephone directories;
  - contact lists (internal and external).

DON'T DO OTHER PEOPLE'S PLANS

In managing the BCM process, it is essential to ensure that departmental managers concentrate on their own plans rather than stray into someone else's area of responsibility. It is easy for staff to start planning for situations that involve another department.

Examples of this are:

- Accounts payable examining activities that are the responsibility of the purchasing department – designing procedures for the raising of purchase orders in a situation where the computer-based purchasing system is unavailable.
- The HR department concerning itself unduly with the technical detail of the back-up and recovery of the HR system, which is the business of the IT department.

It is the responsibility of the business continuity manager to ensure that effort is not wasted in this way, and that it does not become a source of inter-departmental friction. This can be done through a BCM working group, where departmental representatives are kept informed of the BCM activities and progress in all areas, and where the boundaries are clearly marked out.

Departmental plans should be owned by the department.

VITAL RECORDS – NON-COMPUTER

Despite the huge dependence on IT systems and databases, and the extent to which computer networks, document imaging and e-mail facilities reduce paperwork, paper files still have a large part to play in providing vital records.

This important source of critical information must be considered when developing business continuity plans. If paper records are destroyed or become inaccessible, information that is critical to the survival of the organization may be lost.

The nature of these records will vary from organization to organization, and within businesses from department to department. It is important that the process of developing departmental plans has taken account of all such records as they can easily be overlooked. Sometimes there is so much emphasis on computer-based systems, including imaging and document management systems, that critical material stored in filing cabinets can be left out. The obvious areas are legal and contract departments. Other areas such as finance and HR may also have significant paper records that need to be safeguarded.

Are your personnel files adequately protected against fire?

COMMUNICATIONS AND PUBLIC RELATIONS

Dealing with the media

To manage the media in the event of a disaster every organization should have a clear, well understood and well-rehearsed media policy, media plan and media spokesperson.

Remember:

- You will get no thanks for getting it right, but if you get it wrong the world will know about it.
- Provide all assistance possible – be proactive.
- Do not issue 'no comment' statements.
- Tell the truth and issue clear and accurate information.
- Communicate via a single authoritative and credible spokesperson.
- Have a back-up spokesperson.
- Provide regular updates – delays lead to rumour and misinformation and silence can imply guilt.
- There should be no discrepancy between the message to the media and the message to employees – consistency is essential.

- Provide information that emphasizes commitment to the public good rather than simply looking after the organization's interest – e.g. assurances about work done to ensure minimum impact on the environment, public health risks or product safety.

Do not:

- answer a question if you are not sure of the answer;
- discuss injuries or deaths until next of kin have been notified;
- make 'off-the-record' statements;
- try to minimize the problem.

Staff considerations

Most plans are devised on the basis that the loss or interruption is asset-based – people are a secondary consideration. Recent events – September 11 and the anthrax scares – have increased the focus on people issues.

Plans now increasingly emphasize:

- employee safety, including evacuation procedures and drills;
- effective communication with staff if there is a crisis;
- being able to manage in the absence of key personnel.

Effective communication arrangements must be in place to keep staff informed of all developments, and to ensure that the rumour machine does not take over. The communications machinery is required to update all employees on the status of the incident, on what the strategy is, on how the incident is being managed, and to reassure staff that the organization is in control.

The following strategies and processes will help to achieve the objectives:

- There must be a single voice and a single message.
- Ensure that the message is communicated clearly to all staff. They should be aware of the forum or medium through which the information will be conveyed – websites, intranet, e-mail, newspaper notices, etc.
- Ensure that staff who are away from their home base have a means of keeping in touch with the situation.
- Senior management should be highly visible – even if they are not directly involved in the detailed recovery operation.
- Ensure that staff know that their interests are being looked after – foster a sense of community care and of working together towards a goal that will benefit everyone.

If there are fatalities or injuries, the HR team will be involved. This team is responsible for notification of next of kin, liaison with the medical authorities, and providing status updates on all affected personnel.

The HR team will be required to provide information on:

- the total number of fatalities;
- the total number of personnel injured and the nature of their injuries;
- the disposition of the injured;
- the status of next-of-kin notifications.

There are also various staff welfare activities, including travel and catering arrangements, which the HR team will be responsible for during a crisis. It then concentrates on its roles in relation to stress and trauma counselling and rehabilitation programmes.

Sample public relations policy

Where an emergency has been declared, all communication with the media, other external interested parties and communications and with staff in relation to the incident must be via the director of communications.

The following protocol must be strictly observed.

External communication

All external communication is channelled through the director of communications who, in conjunction with senior management and the emergency management team, will decide what, if any, statements should be made.

'No comment' is an unacceptable response.

You must explain that you cannot elaborate since all statements are made through the director of communication's office as a matter of company policy.

Never disclose any information, simply state that you can promise a timely response from an appropriate person.

Take note of the enquirer's name, their organization, contact details and any deadline for a response.

Pass all details to the communications department as soon as possible.

If nobody from the department is available to deal with you within the enquirer's deadline, contact the business continuity manager or the emergency response manager.

The communications department will call the enquirer to ascertain the nature of the enquiry and decide on the appropriate response.

Internal communication

The business continuity manager/emergency response manager will handle internal communication directly concerned with the operation.

The director of communications, in consultation with senior management and the emergency response team, will direct all corporate internal communication. A comprehensive statement should be communicated to all staff as early as possible, and there must be relevant updates issued as the situation develops.

Immediate contact with key customers and suppliers

The director of communications will prepare a statement, a copy of which will be given to key customers and suppliers. The chief executive will authorize its release and distribution.

It will contain:

- a brief statement about the incident;
- an emphasis on the BCM process;
- an estimate of expected developments and timescales.

RESTORATION PROGRAMME

Restoration is an intrinsic part of a business recovery strategy. It can be difficult to consider this aspect in detail until an incident happens and damage arises. However, if some thought is given to the implications and actions, it will make the process much more effective should the occasion arise. Planning will ensure that effective action is taken and this will assist in getting back to an operational situation more quickly.

The immediate reaction to a disaster such as one caused by fire, storm or flood may be to assume that everything that has been damaged should be dumped or replaced. This is not always the case. Experts should be engaged to assess the damage and to determine what should be done and what can be saved. At the same time, appropriate action should be taken to ensure that no further damage occurs and to prevent deterioration.

The result of this exercise is a plan that indicates what can be salvaged and repaired and what should be replaced.

Following a fire that caused considerable damage to an engineering installation, there was a delay of a number of days before salvage experts were brought on board. During this period the damage had worsened through corrosion. It was estimated that the cost had almost doubled. This

led to protracted negotiations with the insurer, and the insured having to suffer the cost of its negligence.

Water-saturated documents – a common outcome of disasters – may appear to be past saving, but it is remarkable how specialists are able to recover them. Rapid freezing will at least prevent further deterioration, but can be costly. When four county court houses in California were severely damaged by fire in 1995, 124,000 files were freeze-dried and restored. The reported cost was $50 per document.

The BCP should include the contact details of specialist recovery/salvage companies. A relationship should be established with them at the planning stage, and they should become acquainted with the nature of the organization, the different locations and any special features or requirements.

It may be appropriate to pay the company a retainer so their services can be obtained quickly if required. This would be particularly relevant in an incident that affects a number of businesses in the same area – flooding being an example.

FEATURES OF A GOOD PLAN

- Simple – easy to understand.
- Strategic – looks at issues from a strategic viewpoint, does not get bogged down in detail.
- Practical – developed by operational management who know the business intimately and are familiar with the options that are feasible in an emergency.
- Probability – takes account of the probability of the plan being activated, and gears procedures and cost-effective resilience and avoidance solutions appropriately.
- Flexible – it is not overly prescriptive but is flexible enough to be adopted in a variety of incidents/disasters.
- Maintenance – it is easy to maintain; a plan that is too complex is difficult to maintain, and soon becomes out of date and virtually useless.

7

Ensuring ongoing success

The hard part of BCM is not creating the plan – it is keeping it up to date.

The rate of change and the ever-increasing technological sophistication of the business environment, in both the public and private sectors, provide significant challenges in the area of BCM. Keeping a plan updated and relevant is one of the most difficult tasks facing the business continuity manager.

Among the factors that create these challenges are:

- regular reorganizations and reshaping;
- transformation and rationalization processes;
- mergers and acquisitions;
- faster rates of technological change;
- increased sophistication in information and communications technologies;
- increased dependence on just-in-time arrangements;
- greater levels of outsourcing;
- more flexible working practices;
- staff turnover and early retirement arrangements, which result in knowledge loss;
- hot-desking and virtual office arrangements.

UPDATING AND AUDITING THE PLAN

We have a plan so we are safe – but an out-of-date plan can be worse than no plan.

Having produced the plan it can very quickly become irrelevant. Keeping business continuity plans up to date is a major problem. This will be achieved only is there is proper ownership of the plan by those responsible for the daily operation and management of the business unit, department or business process. Clarity in regard to ownership is essential to success.

Many line managers consider BCM to be someone else's responsibility – 'isn't that why we have a business continuity manager?'. Business management is obviously focused on business strategy, planning, operations and day-to-day issues, and it can be very tempting to put BCM on the back boiler.

It is a major task of business continuity managers to ensure that the organization does not fall into this trap. They must ensure that the overall framework is kept up to date and that departmental plans and the other constituents of the plan reflect the business operation.

If BCP is regarded as part of a manager's job specification and becomes a KPI (key performance indicator) in the annual evaluation and appraisal process, it will be more successful. Progress on testing and maintenance is then largely an issue for line management.

Some organizations review plans at specific times – often yearly. While periodic reviews are useful they are not necessarily the best approach. The updating process may be more appropriately triggered by changes in the nature of the organization's business, the introduction of new systems, changes in geographic location, or equivalent factors, rather than purely by changes in the calendar.

It should also be possible to link the updating of the plan to the project approval and management system and to the change-control procedures within the organization.

Audit

It is worthwhile subjecting the BCM activity to occasional scrutiny by someone who is independent of the process. This can be done either internally or externally. It provides an objective assessment of the BCM process for the board. The nature of the audit will depend on the maturity of BCM in the business. An effective audit will either highlight deficiencies and indicate where there is scope for improvement, or confirm for the board that the process is effective. In commissioning an audit, it may be useful for the terms of reference to indicate that it is not essential for the resulting report to have a list of recommendations. If appropriate it should simply endorse what is being done.

Some audits can result in a list of textbook-type recommendations which may be impractical or inappropriate in the circumstances. For example – 'Disasters seldom occur on schedule. Use random, unannounced, tests of varying scales and scenarios'.

Objectives of a BCM audit

- Assess the status of BCM in the organization as regards business impacts, priorities, dependencies, sensitivities and resilience.
- Assess the currency of existing plans and confirm that there is a clear sense of ownership.
- Confirm that key staff are fully aware of their roles in an emergency.
- Review the documentation available – the plans and recovery procedures.
- Encourage training and exercising activities.
- Support the implementation of infrastructure and other developments, which may support the BCM process.

EXERCISING THE PLAN

Even a failed disaster recovery test is useful.

The importance of testing/exercising the BCP must be emphasized. Unless a plan is exercised it cannot be said to be viable and workable. There may be significant faults in it, and if it has not been tried out the plan on the shelf will provide a false sense of security which may only become apparent if it has to be implemented in a crisis.

Just as maintaining the plan is a considerable task, exercising it is not a small matter. Some plans are never exercised because of the perceived amount of work involved. There are different approaches to the task. These range from a simple call-out check through to a comprehensive large-scale exercise involving considerable personnel, financial and other resources.

Types of exercises

Walk-through

This type of test is conducted in a workshop environment using a structured approach. It is a relatively inexpensive and very feasible type of test. It considers a particular scenario and, involving all of the interested parties, establishes in a desktop setting how the plan caters for the situation.

It should identify:

- the extent to which personnel understand their roles and what is expected of them in the situation;
- if any assumptions made in the plan are false;
- if the plan as constructed fits in logically with the recovery process.

It also provides a good training exercise for both business and support services personnel.

Component or rolling testing

The most effective way of ensuring that the plans are complete and feasible is to do a full test. It is not easy, or inexpensive, but if the plan is broken down into its various components or modules, each element can be tested independently. If this is done in accordance with a schedule where all of the components are tested over a given period and again at fixed intervals, a 'rolling' approach to testing is achieved.

Component testing is often a necessary precursor to a full test. By testing modules, any amendments can be made before spending the time and money on a full test which otherwise might have had to be abandoned. Examples of component testing are:

- testing that off-site computer data can be restored effectively;
- conducting an out-of-hours telephone contact exercise for key staff and other parties;
- trying out alternative business processes – 'workarounds'.

Full BCP test

Large-scale tests are obviously the only type of exercise that can provide real assurance that the plan works. This type of exercise is not easy. It calls for considerable planning, preparation, commitment and finance. It also introduces its own risks. Consequently, this type of exercise is not undertaken lightly.

Exercises of this nature require commitment and involvement from board level down. It is by far the most effective way of increasing the BCM profile, but it can also be seen as a major diversion of time, effort and money. This is the type of operation that may require many months of planning. It must be driven by the business, and might not be done again unless there are major changes to the business operation. Because of the amount of pre-planning involved, the element of surprise will be missing, so some will say that it does not reflect reality. Surprise testing is talked about a lot in business continuity circles but in reality it is rarely done. This is because of the considerable inconvenience that it would cause. The degree of annoyance it could create might also be counterproductive to the BCM cause.

The approach to exercising

In all cases it is important to approach the exercise with a documented plan.

This indicates:

- the objective of the exercise;
- the parties and resources involved;
- the expected results;
- the times at which various targets should be achieved.

To be useful, the exercise activities and the results should be thoroughly documented. A report should be produced quickly after the exercise, identifying

all difficulties and failures as well as achievements. It should also include any recommendations to improve the plan.

It is worthwhile to involve independent observers throughout the process – from the initial planning phase onwards. The observers can be external experts and, in particular, internal audit personnel.

It is a matter for each organization to determine which approach to exercising is most appropriate. In many cases tabletop exercises with critical component testing will suffice. In other businesses it will be essential to undertake the full exercise. Some plans, such as the IT plan, may need regular exercising. For example, in the case of a financial institution where there are alternative off-site, hot site recovery arrangements including dealing-room facilities, exercises may be needed several times a year.

Some exercises may involve business partners such as key suppliers. In other cases it may be appropriate to observe and verify the testing carried out by business partners on their own continuity plans.

TRAINING AND AWARENESS

Since BCM is a continuing process rather than a project, the nature of any training and awareness programme will vary depending on the state of maturity of the process. There can be a tendency to concentrate all of this activity at the start. Because the plans change, the business changes, and staff come and go, the training and awareness programme must continue.

Business continuity training is necessary in the following areas:

- Awareness programmes for senior management to ensure that they commit their full support to the process.
- Practical training for those involved in initiating, preparing and managing business continuity.
- General staff training to ensure that all staff are aware of their roles in a crisis.
- Specific training in the operation of the plans and procedures in a crisis – this is closely related to the testing and exercising activity.
- Specific training in areas such as crisis communications, trauma counselling and emergency management.

A comprehensive, ongoing, organization-wide training programme would consist of briefings, seminars, formal courses, workshops and the use of media such as newsletters, posters and the company intranet.

How well prepared are your receptionists?

The role of receptionists in security is very important, and in many cases they are not adequately trained to handle these situations. They are in the front line and frequently the first to be involved in many security situations such as bomb scares.

BCM MUST NOT BE AN ISOLATED FUNCTION

From the scenarios portrayed in this book it is obvious that BCM cannot be an isolated, backroom activity. The BCM culture must influence business strategies and decisions.

Increasingly it is apparent that BCM and information security – protecting the availability, confidentiality and integrity of mission-critical systems and data – are intertwined. Organizations that treat BCM and information security as stand-alone activities with separate management teams and reporting structures should examine whether this is still desirable.

Cyber attacks can be equally, if not more, destructive than other types of disaster or physical terrorist attacks. However, the response is different to the traditional response to other types of disaster. These types of attack are typically more difficult to identify, investigate and resolve. They can also have a much more widespread impact on the business.

If a business is heavily dependent on IT, the integration of the BCM and information security functions will help to minimize the risks to the business in terms of planning and preparation, diligence, enterprise-wide co-ordination and response.

The business continuity function should also have some involvement in the process of developing corporate and business plans – although if the business continuity culture is sufficiently developed, the continuity considerations will be a natural part of the development of the plans. If the business continuity manager is involved in the planning phase, it will be possible to identify the risks and describe the exposure that any planned strategies will have for business continuity: for example, in relation to outsourcing functions or processes, or a change in IT strategy.

BCM DOES NOT END

BCM is a programme not a project.

BCM is a continuing process. While most of the work may be involved in getting it off the ground, introducing risk-reduction measures, deciding on recovery strategies and creating the initial plans, the work will continue – perhaps less intensely.

Senior management cannot sit back once the initial plans have been produced. There must be ongoing commitment to, and involvement in, the process. They should insist on regular reports, and recommendations should be addressed.

The working group set up at the start of the process must continue to function. It may meet less frequently, but it provides a focus for the work at an operational level. It will also help to ensure the effective communication of business continuity issues between the different departments or units.

Case study 7.1

King's Cross Underground fire

This is an example of where lack of senior management commitment, abdication of responsibility and poor communication had serious consequences.

The fire at King's Cross Underground Station in London broke out near the end of the evening rush-hour on 18 November 1987. Thirty-one people were killed and many more were injured.

The cause of the fire was a lit match that dropped beneath the wooden escalator. Flammable debris and grease were ignited and the fire spread rapidly.

The investigation pointed to a number of failures on the part of those charged with managing risk. Recommendations that had been made following a serious platform fire in 1984 had not been acted on. The investigation concluded: 'There was not sufficient interest at the highest level in the [1984 fire] inquiries. There was no incentive for those conducting them to pursue their findings or recommendations.'

Safety professionals within the company – London Underground – were junior in status and had little authority to influence the implementation of the recommendations.

The investigation concluded that: 'the chief fire inspector found the same problems of poor housekeeping and electrical wiring in escalator machine rooms year after year. He duly reported this to his superiors but told the Court that he was powerless to require action to be taken.'

The roles and responsibilities for managing risks were unclear within London Underground. Those responsible for safety believed that these responsibilities related to staff safety rather than to passenger safety. There was little communication between departments.

The investigation also concluded that: 'Compartmental organization resulted in little exchange of information or ideas between departments, and still less cross-fertilization with outside industries and other organizations … it undoubtedly led to a dangerous, blinkered self-sufficiency which included a general unwillingness to take advice or accept criticism from outside bodies.'

8

E-business and information technology – major risks

The number of known computer viruses surpassed 75,000 in July 2002 and new viruses are appearing at the rate of 1,200 a month – 40 per day.

BACKGROUND

In many ways, BCM grew out of the original information technology disaster recovery plans. The nature of IT dictated that arrangements should be in place to get back to normal operations if a major problem occurred, such as:

- a hardware/software malfunction that caused data to be lost;
- a catastrophe, for example fire or flood, which meant a bigger task to put things right – new computer hardware and software as well as the restoration of data.

It was always considered good housekeeping, or good management, to have back-up recovery procedures in place. In current e-business and e-commerce environments, organizations are totally reliant on IT. It is scarcely possible to think of a situation where any breakdown or any delay in restoring service would be tolerated, and which did not result in considerable financial loss.

While the traditional requirements of resilience, back-up and recovery are still there, and have become even more relevant, other issues also affect BCM as it relates to IT. Information security, including protection against computer viruses, has become a major issue. The growth of e-business and the need for round-the-clock service, or service at the 'five nines' level (99.999 per cent up-time), have imposed extra requirements. The growth in the use of enterprise resource planning systems means that these are so integrated into the operations of the business that even minor glitches in availability are not tolerated. Add other key business initiatives such as supply chain management and customer relationship management (CRM), and the situation clearly demands continuous, ubiquitous access to information that is critical to the survival of the organization.

In all cases it is a question of balance between the nature and cost of the measures taken to protect the organization's systems and data, and the implications of interruption or loss of service.

Your customers using the web know about your IT problems at the same time as you do – or sooner.

Case study 8.1

Microsoft – loss of service to 10 million customers

In July 2001, Microsoft experienced a three-day outage of its instant messaging service – MSN Messenger. This affected as many as 10 million users.

Microsoft attributed the outage to 'an extremely rare set of circumstances where one of the database servers had a disk controller fail and the back-up for this controller also had an error occur'. This led to Microsoft having to restart all the MSN Messenger servers. It took a week for the problem to be fully resolved.

Murphy's Law had come into play – if something can go wrong, it will go wrong.

This was hugely embarrassing for Microsoft. It resulted in some authoritative industry watchers questioning the company's ability to handle large volumes of critical traffic. Microsoft also experienced some high-profile problems with computer viruses.

These difficulties highlighted the fact that if an organization as significant and as well prepared as Microsoft can experience such problems, no organization can be immune to difficulties with resilience and computer security.

PROTECTING IT

The greatest risks to a company's IT operation may no longer be fire, flood, power outages, or any of the range of traditional threats that IT managers have traditionally emphasized in their plans. Today, business partners, customers, employees, contractors, consultants and hackers have increased access to your IT infrastructure. Unsolicited or malicious acts can result in major disruption to critical IT services.

An organization is also now more dependent for continuity of its IT operation on services outside its control. These include its internet service providers (ISPs) and telecom carriers.

Planning for continuity in the modern IT environment must address vulnerability attack, hackers, viruses and spam, as well as ISP and telecom line failures.

Some important BCM issues are:

- BCM concerns should be addressed at the start of IT projects – both infrastructure and systems projects.
- Computer configurations and network design should avoid single points of failure – or at least identify them, understand the consequences and document the contingency arrangements.
- All significant patches and upgrades to hardware and software should be applied promptly.
- IT should be represented on the corporate BCM steering group or committees.

Case study 8.2

KPNQwest, on the verge of collapse, advises customers to make contingency arrangements

In mid-2002 the provider of Europe's largest data network was bankrupt and advised its 100,000 customers across the continent to put contingency plans in place with other service providers. This emphasized the difficulties that can arise from over-dependence on a single supplier for critical services.

KPNQwest was launched in November 1998 as a joint venture between the Dutch telecoms giant KPN and the US-based Qwest. By 2002 it had some 100,000 corporate customers, and an estimated 40 per cent of European internet traffic used its fibre-optic network. It rented capacity to other telecoms service providers and many blue-chip firms used the network.

At one point it had a market value of €42 billion. However, the high cost of building its fibre-optic network, coupled with the subsequent economic downturn, ensured that the company never lived up to its early promise. Its share price, which had been as high as €90, dropped to below 50 cents and it filed for bankruptcy.

Many of the users of the bankrupt company's network, often indirectly via their prime network access supplier, then realized how dependent they were on a single supplier and network.

At the end of May 2002 the company issued a statement warning customers about the potential problems for the core business operations of thousands of its customers: 'In the interest of maintaining customers' business and network continuity, the company is advising customers that they may wish to put in place contingency plans with other providers in the event of a significant deterioration in the performance of the KPNQwest EuroRings network.'

INFORMATION SECURITY

Two out of three workers disclosed their passwords to complete strangers during a survey at Victoria Station, London.

The risks associated with information security are among the most serious facing any organization today. For companies engaged in e-business, it is a major management concern.

Security has been addressed by IT management from the earliest days of commercial computing. At first, it was concerned with issues such as access control – keeping the computer centre secure and ensuring that only authorized users had access to systems. The scenario changed with distributed computing, and has been changed utterly in the type of IT infrastructure, networks and facilities that are available today.

Now computer technology and access to data is widely distributed, not just to staff but to a wide range of third parties – contractors, consultants, temporary employees, business partners and customers. User departments now handle tasks that used to be carried out by highly trained specialists. In many cases, these people will have received minimal, if any, training in even the most basic information security procedures. This includes training in the protection of data through back-up and recovery procedures. Control of critical information can now be in the hands of a variety of people and in a variety of locations.

Initially, the threats to information security were very much from within the organization. While security breaches by insiders are still a significant issue, the major worries relate to unauthorized access by outsiders, and cyber-crime activities.

Computer security has become a much more complex and expensive function. Regardless of the effort and the technology devoted to it, total security is still only a dream. When the most security-conscious businesses still experience breaches, whether by virus attacks, website defacement, denial-of-service attacks, spoofing or simple fraud, it is only reasonable to expect that management will question the worth of the measures in place in their organization.

Most organizations encounter computer viruses every day. Daily attempts are also made to hack into countless websites. Even the home computer user on the internet is likely to be the subject of visits from interested, or just curious, invaders. Staff, consultants or suppliers may leave open modems connected to systems and computers. This effectively provides an open door for unwelcome visitors to find a way through to an important system or on to the internal network. They may even find a message 'welcoming' them to the system.

While there are various protection strategies and mechanisms available, the most important element in protection is the commitment of the organization to proper information security policies and procedures.

According to a Department of Trade and Industry survey conducted by PricewaterhouseCoopers in 2002, only 27 per cent of UK businesses had a security policy. While this proportion had doubled since a 2000 survey, the fact that almost three-quarters of UK businesses have not set out their IT security policies, and communicated them to personnel across their organizations, is cause for concern.

Is it any wonder that two out of three people were prepared to disclose their computer passwords to a stranger at a London railway station? In this context it is also no surprise that the passwords disclosed would be easily ascertained by even the most basic password-cracking software. 'Password' was the most common one disclosed. This reinforces the view that employees are an organization's weakest link.

Just like a BCP, there is no point in having an information security policy just for the sake of having one or to keep the auditors happy. There must be commitment

from the top – full appreciation of the need for such policies, they must be strictly enforced, and they must be regularly updated. Again, like BCP, information security should be a mindset and part of the culture of the organization.

The development of information security policies in an organization is a considerable task. More significant still is getting the policies accepted and communicating them throughout the organization.

There should be a formal set of computer usage policies. Every user of computer facilities in the organization should be familiar with these policies and should be obliged to comply with them.

Typically they cover:

- an outline of the organization's security policy;
- guidelines on the use of computer facilities;
- special considerations relating to the use of portable computers;
- the need to have regard for both software licensing arrangements and copyright compliance;
- measures required to protect the organization from computer viruses;
- acceptable-use policy for e-mail;
- acceptable-use policy for internet access;
- guidelines for ensuring that passwords are not easily cracked;
- policies and procedures in relation to data protection and privacy.

These are the types of policies which, if enforced, can prevent major problems occurring such as the one where a member of staff caused the company's e-mail system to collapse. In this case, an employee sent an e-mail to all the distribution lists on the company's global address list – some 20,000. To compound the problem, a number of recipients replied using the 'reply all' facility, generating tens of thousands more messages. This caused the e-mail server to crash, e-mails were lost, and the server was down for a number of days while IT staff tried to recover the situation.

TOP TEN ACTIONS FOR THE BOARD

Make sure your business:

- creates a security-aware culture by educating staff about security risks and their responsibilities;
- has a clear, up-to-date security policy to facilitate communications with staff and business partners;

- has people responsible for security with the right knowledge of good practice (e.g. BS7799) and the latest security threats – consider supplementing their skills with external security experts;
- evaluates return on investment on IT security expenditure;
- builds security requirements into the design of IT systems and outsourcing arrangements;
- keeps technical security defences (e.g. anti-virus software) up to date in the light of the latest threats;
- has procedures to ensure compliance with data protection and other relevant regulatory requirements;
- has contingency plans for dealing with a serious information security breach;
- understands the status of its insurance cover against damage as a result of information security breaches;
- tests compliance with its security policy (e.g. security audits, penetration testing of its websites).

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

Source: PwC/DTI Information Security Breaches Survey, 2002

ERP SYSTEMS

An ERP (enterprise resource planning) system is a multi-module computer application that is designed to support all the key activities of an enterprise in an integrated fashion. This includes managing the key elements of the supply chain operation – product planning, purchasing, production control, inventory control, interaction with suppliers and customers, delivery of customer service and keeping track of orders.

ERP is regarded as central to an organization's ambition to survive and prosper in today's business environment. It often replaces a myriad individual systems including 'integrated' accounting systems, and production planning and inventory control systems. Its predecessor systems were often a mix of custom-built systems and package software. Frequently they were based on a variety of computer hardware and software platforms and database management systems. Significant work went into developing and managing the interfaces between them.

The use of ERP allows for greater efficiencies in many ways. It is a more effective way of providing computer support to the business functions. It is particularly

relevant in the case of large complex businesses, or where it is necessary to rationalize and integrate systems and operations in situations where mergers and acquisitions have led to a mixed bag of systems and computer platforms. It also allows for significantly greater efficiencies in managing the total supply chain. Customers become more dependent on faster delivery of product and tighter lead times. Safety stocks can almost disappear and just-in-time philosophies dominate. In effect, ERP has the effect of making an enterprise more time-sensitive and consequently more vulnerable to the impact of time delays.

While there are undoubted benefits, ERP also poses significant challenges in the areas of information security and business continuity planning. For most businesses, the implementation of ERP is a major, complex project. As such, it is not without its risks and this in itself is a business continuity issue. There are many examples of ERP projects that have gone wrong – failed, finished well over budget, or simply failed to achieve the anticipated benefits.

Before ERP a business tended to have multiple points of failure of computer-based systems and facilities. There were potential breakdowns with individual systems and with the many interfaces between them. However, there tended to be 'workarounds' available and in some cases it was even possible to revert to manual procedures. With ERP there are fewer points of failure, but if there is a failure the impact can be significant. One of the major advantages of ERP is that it allows an organization to redesign its operations totally rather than just computerize further the existing ways of doing things. This means that there is no real alternative available if problems arise. If it takes time to recover, the implications can be serious and business may grind to a halt. Production may stop, and selling, inventory management and other key functions may find it impossible to continue. Time and production records may be unavailable and it may not even be possible to pay staff on schedule.

Because of this, business continuity issues must be addressed comprehensively at an early stage in the implementation process.

Consider business continuity at the ERP planning stage

ERP implementation is an expensive exercise. Apart from the cost of the application and the hardware and software platforms, a considerable amount of expensive input will be required from the suppliers and consultants in design, build, data-loading, implementation and training activities. Despite the expected benefits, the cost of installing such a system may lead to a temptation to trim costs by omitting expenditure required to address the business continuity issues. It may be difficult to get board approval anyway without adding further to the bill. The attitude may be 'let's get it up and running and we can address the business continuity issues in the next phase'.

Considering the vulnerability of the enterprise in the event of problems, this is false economy. If left until the 'next phase' it will probably never happen. If planned and provided for from the start, the costs are likely to be considerably less than when the facilities are provided later on.

There should be active involvement of the business continuity function from the planning stage onwards. Here are some of the benefits of this approach and the issues to be addressed in these phases of the project:

- Potential outages can be considered and thought given to what alternative processes can be designed in at the same time. These issues can be covered in a relatively small part of the overall training programme.
- Resilience can be considered more realistically where keeping the costs to a minimum is not the overriding viewpoint.
- How does the planned infrastructure meet the recovery requirements?
- Will all of the eggs be in the one basket? Should the computer facilities be split over multiple sites? If this is done, does it overcome the need to have access to a business recovery site?
- Sometimes the funding for recovery sites comes from a designated business continuity budget. This means that the project does not have to carry the costs but it results in a greater overall cost. Like any other project, the overall bill should include continuity aspects.
- If there is only a single site/computer system, how are subsequent upgrades to the systems to be tested and implemented? Moving to new releases of an ERP system with considerable new facilities can be a major issue.
- It is more likely that there will be adequate studies of the impact on the business of outages compared with the cost of providing the different types of recovery mechanisms. The recovery strategy chosen will affect the speed at which normal business operations can be resumed, and will have different costs attached.

Case study 8.3

Hershey Foods – implications of ERP problems

Hershey Foods Corporation, the leading chocolate manufacturer in the United States, experienced difficulties with the $115 million ERP it was implementing. Among other things, its ability to ship goods during the peak Hallowe'en season in 1999 was hampered.

The ERP project was a major one, designed to replace scores of legacy systems that had been running everything from inventory and order processing to human resource information systems. It was expected to impact on virtually every facet of the company's operations.

Hershey had spent up to three years implementing the system, well supported by a number of teams of consultants. There were problems as they went along.

During the busiest season of the year, customers such as Wal-Mart and Kmart had no option but to start topping up their orders with product from Hershey's competitors. Meanwhile, Hershey's warehouses were piling up with stock.

It is reported that third-quarter sales in 1999 dropped by 12.4 per cent compared with the previous year, and that earnings were down 18.6 per cent.

During the period of difficulties with the system:

- typical delivery times went from five to twelve days;
- there was a 29 per cent increase in year-to-year inventory costs;
- relationships with customers became strained;
- customers replaced usual supplies with other brands;
- rivals boosted their sales considerably.

THE INTERNET

In most cases, it is not possible for an organization to extend its corporate IT network to all its customers, suppliers and business partners. The internet provides the mechanism. What began as the world's largest pool of academic knowledge, with its relatively unfriendly user interface, has evolved into the support infrastructure for business. The internet is universal. In addition, it is both relatively easy to use and relatively cheap. It now provides the infrastructure for linking an enterprise with its business partners, its suppliers and its customers – both existing and prospective. It supports worldwide e-mail systems and allows organizations to provide access to its systems for staff from home and while travelling. It provides tremendous marketing opportunities. It offers a global marketplace to the local company, and has enabled the e-business or e-commerce revolution. It has allowed companies such as Dell, Amazon, UPS and financial institutions to exploit a whole new way of doing business.

While the internet provides business with great opportunities, there are also risks associated with using it. Nobody owns the internet, so to some extent it can be something of a free-for-all. Once connected to the internet, your computer – or server – is also accessible to every other computer connected to the net. Not everyone connected to the net and interested in your site is a potential customer. This community includes hackers, commercial rivals, cyber criminals and a range of less significant but potentially troublesome visitors.

Significant investment and commitment to security measures are required if an organization's computers, systems and data are to be protected from unwelcome visitors and interference. The most important element is an appreciation by

management of the risks involved and of the need to take appropriate action. This should lead to the development and enforcement of good security policies and procedures. It must be emphasized that without this foundation, the physical and other barriers and access mechanisms that are built will be considerably less effective.

Because of a number of well-publicized breaches of internet security, customers now expect security issues to have been addressed. If not, they will be wary of doing business with a company that does not take its security seriously. At its most obvious, this relates to concerns about credit card security.

Business continuity issues

Apart from the security issues, there are particular business continuity issues that apply to the internet/e-business environment. The traditional IT 'recovery window' is not available. E-business requires seamless, non-stop services, and a positive business continuity approach must address this. The focus must be on saving the customer or business partner from ever having to experience interruption in the service or process. The internet customer will not tolerate slow, intermittent or unreliable service. There are many alternatives available at the click of a mouse, and once lost the business will be difficult to regain.

eBay the most popular auction site on the internet, closed for more than 24 hours because it did not have adequate server redundancy, in addition to a number of software problems. The result was a reported loss of $5 million, and its market value fell 20 per cent.

In some companies, the web presence evolved rather than came about as the result of a carefully developed policy and implementation process. What started out as a toe-in-the-water approach grew incrementally – upgrade the server, add more bandwidth, get a firewall, check for viruses, etc. It is easy to understand this. Only a few years ago use of the internet was relatively undeveloped. It was exploited by enthusiastic IT personnel or by very enlightened and adventurous members of the management team who had a difficult battle with colleagues to get support for establishing a web presence. The innovative IT people involved were anxious to get things done quickly, and sometimes ignored the traditional IT good practices regarding security and resilience. The early adopters did not encounter the same level of risk – in terms of security – that exists today, and the support infrastructure did not have to be as sophisticated. As a result, business continuity planning was not part of the initial technical development phase but was thought about subsequently. When e-business became more significant, some companies rethought their approach and redesigned from scratch. Others continued to bolt on to unsatisfactory foundations, and this can result in a significant amount of incremental build and patch-up work.

A significant business continuity issue in this area relates to 'knowledge'. Because of the rate of evolution there is a real danger that the documentation of the infrastructure, systems and services will not be kept up to date. This is a particular worry because of the turnover of IT staff in this area, and the danger of losing significant knowledge and expertise when key staff leave.

The 'internet year' is regarded as the equivalent of three months. This means the supporting technology has to be frequently updated. The often neglected function of change management is particularly important in this environment. The global, non-stop nature of the internet means planned downtime for implementing hardware and software upgrades and patches is almost impossible. The infrastructure must allow for this in terms of applying and testing the upgrades on a back-up service before switching to live. A comprehensive change management plan, with good documentation and a clear definition of responsibilities, is the only viable approach.

OUTSOURCING

> *More than half of all outsourcing deals are unsuccessful. For information technology outsourcing it's even worse. Over three-quarters of IT deals fail to perform.*
>
> *Strategic Sourcing: 'The Book'*, Gartner, 2002

Many organizations have outsourced functions and operations that they deem to be non-core business activities. The objective is to concentrate on core business – on what the organization does best. This has been a feature of business since the mid-1980s and in many cases IT was the first, and sometimes the only, function to be outsourced. While there may be advantages in certain cases, not all anticipated benefits have been achieved. In some cases it is unlikely that cost savings have been met – although this may not have been the main reason behind the outsourcing of the operation.

From a business continuity perspective, there are issues to be considered – you can outsource the activity but you cannot outsource the risk.

Business continuity issues such as security, resilience and recovery need to be addressed at the earliest stage of the process. The contractual arrangements should allow for these aspects to be catered for in at least as comprehensive a manner as if handled in-house. Other important issues to be considered are what happens if the supplier goes out of business, and, probably more relevant, what happens when the contract term expires? If the result of the outsourcing arrangement proves to be problematic, because either the outsourcer goes out of

business or the arrangement just does not work, it will be very difficult to take the operation back in-house. The most likely scenarios depend on finding another supplier or, if the outsourcer has folded, the possibility that another company operating in the outsourcing business will take over the company and continue the operation. Neither of these options is hugely attractive. Once a company commits to outsourcing its IT operation it is very difficult to change suppliers at the end of the contract period. Effectively the outsourcer has the company 'over a barrel' and the situation would have to be very unsatisfactory to contemplate such an option.

The outsourcer will probably have taken on the company's IT staff. Also, by the end of the contract period, it will have amassed so much knowledge of the company's systems and operations that it would be very difficult for another company to take on the business without considerable disruption.

Where IT systems are at the very heart of the business and where they actually drive its operations, it is very difficult to outsource without exposing the business to considerable risks. However, this consideration does not always stop the drive to outsource, and management may be prepared to live with the risks.

Because of the rate of technological change and the growing dependence on e-business, the business environment now may be quite different to what it was like when the original outsourcing agreement was finalized. If the outsourcing arrangement has been in place for, say, five years, the marketplace in which the company trades is likely to have changed considerably. The company must be in a position to respond to this change with its IT systems. If the arrangement is not managed properly, this could have an impact on cost, flexibility and the ability of the organization to take advantage of the developing environment.

From the perspective of information security, the positives of outsourcing may exceed any negatives. The outsourcing company will, in most cases, be a major player in the business. It most likely will have addressed the areas of computer policies and procedures for its operation as a whole and for individual customers. It is likely to have a specialist IT security function which is up to date on the current technologies and approaches to safeguarding against security breaches. It should have current anti-virus protection, good monitoring procedures in place, and effective procedures to handle incidents.

Its approach on these issues should be investigated before any arrangement is agreed.

The main drawback of outsourcing relates to the possible confusion and lack of clarity as to responsibilities in the area of information security. The business may take the attitude that information security is not an issue for it because it is handled by the outsourcer. The outsourcer has its responsibilities, but remember that the users of the systems are still within the business. Computer users must still understand their responsibilities and obligations in relation to security, regardless of who is responsible for the provision and support of the computer facilities.

These responsibilities include using strong passwords, not disclosing passwords, not accessing risky websites and not sending e-mails with offensive content. In many companies, it is the information security department that is the primary advocate of information security and that keeps users under pressure to comply with the policies. If this function no longer exists within the company following an IT outsourcing arrangement, security may be neglected.

You can outsource the activity but you can't outsource the risk.

9

Role of the emergency services

There is an obvious need to work closely with the emergency services in preparing business continuity plans – before a disaster actually happens. It is necessary to understand their role, to understand their procedures and practices in dealing with a disaster, and to see what input they could provide to make your BCP more effective.

Despite this, many plans are prepared and exercised without any meaningful communication or involvement with these services.

One of the reasons for this is that often the business continuity personnel have no ongoing direct channel of communication with emergency services staff. While both parties are anxious to establish a working relationship, the opportunities are not always there to foster it. Both groups tend to have their own professional bodies and associations. There is relatively little interaction between the two sets of professions at this level. There is a need for both sides to look at possibilities, such as dual membership of their professional associations and forums, and of broadening the scope of training courses and conference programmes in order to promote closer links.

The business continuity person is frequently confused as to the roles and responsibilities of the different parties in the case of a disaster. Who is in charge and at what stage? Is it the police, the fire service, the ambulance service or the local authority? Who is responsible for establishing a cordon and when will it be redrawn or removed?

The objectives of this chapter are to highlight the importance of the role of the emergency services, to identify some of the key issues, to look at how the process works, and to increase the awareness of some of the areas in which assistance is available to business continuity managers.

- Establish a relationship with your local emergency planner or equivalent.
- Encourage your business continuity manager to get involved with the professional associations of emergency planning personnel and management.
- Encourage your building services, security, and health and safety personnel to become involved too.

THEY ARE THE EXPERTS

There are many similarities between business continuity management and emergency planning and management. The four phases in emergency management outlined below map very easily on to the equivalent phases in BCM.

Four phases of emergency management

1 *Hazard analysis and mitigation* – where the potential for accidents is assessed, and where appropriate steps to prevent or reduce their probability or consequences are taken

2 *Emergency planning and preparedness* – where procedures are put in place for mobilizing the available resources, and preparing these resources for an effective and co-ordinated response

3 *Response phase* – where the pre-determined procedures are brought to bear on the particular situation, until the situation is brought under control and the response objectives have been achieved

4 *Recovery phase* – when individuals, organizations and communities try to restore the pre-emergency situation or develop it, and learn lessons from what has occurred.

The response to a major incident, be it a factory fire, flooding, train or air crash, is not just determined when the incident occurs. It is most likely that the scenario will have been envisaged, exercises will have been undertaken based on the type of situation that has arisen, and the nature of the response will already have been determined.

Business continuity managers are very conscious of the difficulties involved in organizing effective tests and exercises. To the emergency services, exercises are a natural part of the job. The business world is generally unaware of the nature and extent of these exercises. These may be real or tabletop, and will frequently involve the co-ordination of all parties involved in emergency services – including the voluntary agencies and second-line reserves.

Local authorities and emergency services are always willing to provide advice to business and other organizations. This is an essential part of their objective to reduce risk, and to ensure that if an incident does occur everybody is better prepared to cope with it. For example, the Corporation of London's Security and Contingency Planning Group is available to assist businesses in the City with developing and exercising their business continuity plans.

Assistance is provided in such areas as:

- information on the major incident response arrangements within the City;
- presentations to staff and management on any aspect of business continuity;
- the development of exercises and, if appropriate, participation in those exercises.

As an independent third party, the group is also available to discuss a company's plans and arrangements in strictest confidence. For organizations based within the City boundary, there is no charge for these services.

NATIONAL EMERGENCIES

While the main concern will be with local emergencies, the events of September 11 have caused all organizations to consider to some extent the implications of a more widespread emergency.

The anthrax scares that followed September 11 showed how simple it can be to cause widespread chaos. This, whether the threat was real or a hoax, not only caused major disruption in some companies but also stretched the emergency services considerably.

Many governments were forced to reconsider their approaches to national emergency planning. The events at the World Trade Center and in Washington, and the possible scenarios that emerged such as chemical, germ or nuclear incidents, brought a new awareness of vulnerability and the lack of an effective national framework for emergency planning and response in many countries.

In the United States, the Director of the Federal Emergency Management Agency (FEMA) praised the emergency services for their heroic deeds on and after September 11, including those who risked their lives to ensure that thousands escaped from the World Trade Center. However, he was aware of the problems and communications difficulties that arose.

He admits that communications broke down. Rescue teams from different states were unable to work together. Following the disaster, firefighters arrived from neighbouring states bringing their own gear. However, when the oxygen for their breathing masks ran out, it was discovered that the New York oxygen tanks could not connect to the masks of crews from other states. Meanwhile, the fire trucks that came over the Hudson River from New Jersey to fight the fires were not as effective as expected because the New York hoses could not attach to the trucks.

As a result of the experience, the agency now plans to focus on creating national standards for equipment, on fixing communications problems, and on ensuring that response teams from across the United States can work together more effectively.

The new sense of urgency and the measures being put in place can be gauged by visiting some of the websites listed in Appendix 3.

The ability to respond effectively to disasters depends on a good deal of planning, training and exercising. It is the emergency planner's role to produce plans to deal with the consequences of a major emergency, and there will be many lessons learned from the attack on the World Trade Center on 11 September. The lessons will be not just about prevention but also about the response and the mitigation of the effects.

Brian Ward, Chair, Emergency Planning Society, UK

THE APPROACH TO EMERGENCY PLANNING

The following is based on some of the recommendations of the UK authorities in relation to emergency planning.

Organizations involved in emergency planning sometimes use the terms 'major emergency', 'major incident', 'disaster' and 'large-scale emergency' to describe the same event.

In the UK, the following is used as a useful working definition for any of these terms:

> *Any event happening, with or without warning, causing or threatening death or injury, damage to property or to the environment or disruption to the community, which because of the scale of its effects cannot be dealt with by the emergency services and public service providers as part of their day-to-day activities.*

While some causes of major emergencies can be sudden and unpredictable, certain kinds of activity carry particular risks. These include industrial sites, transport operations and oil/gas pipelines. Since experience and risk analysis can indicate the most probable types of incident associated with these activities and the likely consequences of these incidents, it is possible to make plans for the appropriate actions to be taken. Such plans will smooth the response to incidents and remove some of the necessity to make decisions under crisis conditions. Plans should still, however, be sufficiently flexible to allow for unforeseen emergencies or for conditions being different to those envisaged.

The overriding motivation for emergency planning must be the safety of the public and protection of the environment, and the need to prevent, or mitigate the effects of, major emergencies. This process of prevention, planning and response is known as civil protection. In order to achieve this, organizations providing public services need to respond together in a co-ordinated manner.

The principal emphasis in the development of any plan must be on the response to the incident and not the cause of the incident. There are an infinite number of possible emergency scenarios and it is impossible to plan for them all. However, incidents tend to result in a much smaller range of short and long-term outcomes, such as the need to evacuate, to treat large numbers of casualties, or to make secure and then repair damaged infrastructure or tackle environmental pollution.

By concentrating on planning to deal with outcomes, it is possible to respond to a large range of incidents within the framework of a limited number of plans. Such plans need to be flexible: to allow for all weathers and times of day/night, to

work when key people are on holiday, and to be usable even when the results of an incident have unexpected complications.

All organizations that provide a service in a major emergency will be working to a common aim to:

- save life;
- prevent escalation of the incident;
- relieve suffering;
- safeguard the environment;
- protect property;
- facilitate criminal investigations and other judicial, technical and public enquiries;
- continue to maintain normal services at an appropriate level and inform the public;
- promote self-help and recovery;
- restore normality as soon as possible;
- evaluate the response and identify lessons to be learned.

THE APPROACH TO A MAJOR INCIDENT

The emergency services in London have joined with representatives of the local authorities to agree how they will respond to a major incident. This group is known as the London Emergency Services Liaison Panel (LESLP), and has produced a manual which is essential reading for contingency planners in London.

The manual has been drafted in accordance with the latest agreed procedures of the Association of Chief Police Officers, the Chief and Assistant Chief Fire Officers Association, the Ambulance Service Association, London boroughs and the Home Office. The work of LESLP has been recognized widely as being a role model of inter-agency co-operation in the planning and response to a disaster, and it is being used here to help to describe what happens at the scene of a major incident.

The following extracts from the manual provide a good overview of:

- the approach to major incidents;
- the roles and functions of the different services;
- the actions and priorities at the scene;
- management of the scene;
- command and control;
- local authority assistance;
- occupiers' response.

Major incidents

Definition

A major incident is an emergency (including known acts of terrorism) that requires the implementation of special arrangements by one or all of the emergency services and will generally include the involvement, either directly or indirectly, of large numbers of people. For example:

- the rescue and transportation of a large number of casualties;
- the large-scale combined resources of the police, London Fire Brigade (LFB) and London Ambulance Service (LAS);
- the mobilization and organization of the emergency services and support services, for example local authority, to cater for the threat of death, serious injury or homelessness to a large number of people;
- the handling of a large number of enquiries likely to be generated both from the public and the media, usually to the police.

Declaration

A major incident may be declared by any officer of one of the emergency services who considers that any of the criteria outlined above has been satisfied.

Despite the fact that what is a major incident to one of the emergency services may not be so to another, each of the other emergency services will attend with an appropriate pre-determined response. This is so even if they are to be employed in a standby capacity and not directly involved in the incident.

Stages

Most major incidents can be considered to have four stages:

- the initial response;
- the consolidation phase;
- the recovery phase;
- the restoration of normality.

An investigation into the cause of the incident, together with the various hearings, may follow on.

Main functions of the emergency services

Rescue will most frequently be the prime function required of the emergency services. Responsibility for the rescue of survivors lies with the London Fire Brigade. The care and transportation of casualties to hospital is the responsibility of the London Ambulance Service. Police will ease these operations by co-ordinating the emergency services, local authorities and other agencies.

Police

The primary areas of police responsibility at a major incident are:

- the saving of life, together with the other emergency services;

- the co-ordination of the emergency services, local authorities and other organizations acting in support at the scene;
- to secure, protect and preserve the scene and to control sightseers and traffic through the use of cordons;
- the investigation of the incident and obtaining and securing evidence, in conjunction with other investigative bodies where applicable;
- the collection and distribution of casualty information;
- the identification of the dead on behalf of the Coroner;
- the prevention of crime;
- short-term measures to restore normality after all necessary action has been taken.

Fire brigade

The primary areas of LFB responsibility at a major incident are:

- life-saving through search and rescue;
- fire-fighting and fire prevention;
- rendering humanitarian services;
- management of hazardous materials and protecting the environment;
- salvage and damage control;
- safety management within the inner cordon.

Ambulance service

The primary areas of responsibility for the LAS at a major incident may be summarized as:

- to save life, together with the other emergency services;
- to provide treatment, stabilization and care of those injured at the scene;
- to provide appropriate transport, medical staff, equipment and resources;
- to establish effective triage points and systems, and determine the priority evacuation needs of those injured;
- to provide a focal point at the incident for all National Health Service (NHS) and other medical resources;
- to provide communication facilities for NHS resources at the scene, with direct radio links to hospitals, control facilities and any other agency as required;
- to nominate and alert the receiving hospitals from the official list of hospitals to receive those injured;
- to provide transport to the scene for the medical incident officer (MIO), mobile medical/surgical teams and their equipment;
- to arrange the most appropriate means of transporting those injured to the receiving and specialist hospitals;
- to maintain emergency cover throughout the LAS area and return to a state of normality as soon as possible.

Actions by first officers at the scene

A major incident should be formally declared as soon as the criteria are satisfied.

Police

The primary duties of the first police officer on the scene are to assess the situation and ensure the following information is passed back to their control room.

The mnemonic CHALET has been devised to help:

- *Casualties* – approximate numbers of dead and injured.
- *Hazards* – present and potential.
- *Access* – best access routes for emergency vehicles.
- *Location* – exact location of the incident.
- *Emergency* – emergency services present and required.
- *Type* – type of incident with brief details of numbers of vehicles, buildings etc., involved.

The officer should then:

- decide whether to declare a major incident;
- take interim charge until relieved by a more senior officer;
- maintain contact with the control room.

The officer must not get personally involved with the rescue work.

Fire brigade

Since the initial call to a major incident may not carry sufficient information to indicate the severity of the situation, the incident commander will assess the situation and report. This message will include the phrase: 'Initiate major incident procedure'.

The incident commander will take all necessary measures to:

- assess the effectiveness of fire fighting or other measures carried out before his/her arrival;
- identify the risks associated with the location, including those details held on the brigade's central risks register;
- form a plan of action to deal with the developing situation;
- decide on appropriate additional resources;
- take effective command and issue instructions to effect the plan of action;
- maintain operational command of the fire fighting and rescue operations within the inner cordon;
- evaluate the situation and any potential for development, preparing to brief a more senior officer on the incident, the police and ambulance service officers attending;
- liaise with other emergency service incident officers at the earliest opportunity and provide a safety briefing.

Ambulance service

The first ambulance or paramedic response vehicle may arrive on scene before the ambulance incident officer (AIO). The following procedures should be adopted;

- report arrival on scene to Central Ambulance Control (CAC);
- confirm incident appears to be a 'major incident';
- liaise with emergency services incident officers;
- provide CAC with a detailed situation report, and use CHALET;
- request ambulance/medical resources required pending the arrival of the AIO.

The duty officer or first vehicle attendant should act as AIO until relieved by the nominated senior ambulance officer.

Scene management

Cordons

Cordons are established around a scene for the following reasons:

- to guard it;
- to protect the public;
- to control sightseers;
- to prevent unauthorized interference with evidence or property;
- to facilitate the operations of the emergency services.

Recent cases underline the importance of scene security for all agencies involved in the response. It should be noted that unauthorized access to the site of a major incident could jeopardize both the rescue and investigation. Any difficulties with identification should be referred immediately to the appropriate control vehicle at the Joint Emergency Services Control Centre (JESCC).

Three cordons will be established. This will be done by the police in consultation with other agencies:

- *Inner cordon* – provides immediate security of the hazard area and potential crime scene.
- *Outer cordon* – seals off an extensive area around the inner cordon.
- *Traffic cordon* – set up at or beyond the outer cordon to prevent unauthorized vehicle access to the area around the scene.

In terrorist or suspected terrorist incidents, it is a criminal offence to contravene a prohibition or restriction imposed under Section 16(c) of the Prevention of Terrorism Act. This includes crossing a police cordon.

For all known or suspected terrorist incidents, all personnel should be aware of the possibility of secondary devices. Police will be responsible for checking rendezvous points (RVPs), marshalling areas, JESCC and cordon points for suspicious objects.

Command and control

Initial control

It is possible that early in the incident members of one service will spontaneously carry out tasks normally the responsibility of another. As soon as sufficient staff arrive, each service can be expected to establish unequivocal command and control functions for which it is normally responsible

Gold, silver and bronze

'Gold', 'silver' and 'bronze' are titles of functions adopted by each of the emergency services, and are role-related not rank-related. These functions are equivalent to those described as 'strategic', 'tactical' and 'operational' in other documents about emergency procedures. In summary, the roles of each can be described as:

- *Gold – strategic.* Gold is the commander in overall charge of each service, responsible for formulating the strategy for the incident. Each gold has overall command of the resources of their own organization, but delegates tactical decisions to their respective silver.
- *Silver – tactical.* Silver will attend the scene, take charge, and be responsible for formulating the tactics to be adopted by their service to achieve the strategy set by gold. Silver should not become personally involved with activities close to the incident, but remain detached.
- *Bronze – operational.* Bronze will control and deploy the resources of their service within a geographical sector or specific role and implement the tactics defined by silver.

It should be understood that the titles do not convey seniority of service or rank, but depict the function carried out by that particular person. From the outset it is important that the senior officers of each service on scene liaise with each other. This will be the foundation upon which all later meetings will be based.

As the incident progresses and more resources attend the RVP, the level of supervision will increase in proportion. As senior managers arrive they will be assigned functions within the gold, silver and bronze structure. Senior officers arriving at their respective command/control vehicles are to establish contact with their incident commanders and should also make contact with the police silver in order to notify any transfer of command. It is important that the titleholder wears a uniquely identifiable tabard and passes it on to their successor.

By using this universal structure, the emergency services will be able to communicate with each other and understand each other's functions and authority.

Inter-agency resources

Any service may request temporary assistance from another's personnel and use of its equipment. In these circumstances, while the supporting service will relinquish the immediate control of those resources to the other service for the duration of the task, it will nevertheless keep overall command of its personnel and equipment at all times.

Personnel from one service who help another in this way should be given tasks only for which they are trained, and not simply supplement the other service in a potentially dangerous situation. For instance, police officers may be directed to implement cordons or become stretcher-bearers to release fire fighters for rescue work. They should not undertake hazardous rescue work themselves.

Local authority assistance

Response

The main functions of a local authority during a major incident are to maintain existing services to the community in addition to providing requested support to the emergency services. Each of the 32 London boroughs and the Corporation of London employ a person who performs the function of emergency planning officer and is responsible for preparing the local authority response to civil emergencies.

Following the declaration of a major incident, the local authority acts in support of the emergency service. Its response will be flexible and in proportion to those resources available at the time.

Notification

Local authorities take time to mobilize, and therefore early notification is required. They need to be updated constantly as the incident progresses so that their response is measured and appropriate. Good liaison between the emergency services and the local authority, particularly at the scene, is essential and will be enhanced by the presence of the local authority's control vehicle (or other facility) at the JESCC.

Involvement

The local authorities are able to supply considerable assistance to deal with particular problems, such as:

- the provision of technical advice and resources;
- environmental health management;
- logistical support through local authority or contract resources;
- long-term management for the restoration of normality.

It is in the later stages of a major incident (the recovery period and return to normality) that the local authority's involvement may be prolonged and extensive. It may include:

- rehabilitation of the community;
- social services;
- counselling;
- emergency finance;
- emergency housing;
- the provision of equipment, transport and staff;
- the provision of suitable premises for some of the functions described elsewhere in this manual, particularly in relation to casualties.

Mutual aid

- Local authorities are arranged into groups, and each authority is able to call on the assistance of others within its group.
- There are five such groups in London, each led by a 'lead borough'.

Assistance could include the shared use of vehicles, equipment and personnel, and could extend to other authorities outside the group which are willing to assist.

Occupiers' response to an incident

It is to be expected that any occupier of premises within a cordoned area, be they residential or business occupiers, would want to gain access to their premises as soon as possible. Similarly, the police will wish to restore as much normality as possible as quickly as they can.

However, this is subject to two constraints:

- The area around a major incident is a potential crime scene, and the police and other investigators need to carry out a painstaking enquiry to gain material evidence. This could take some time, and during that period people will be excluded from the area so that vital evidence is not lost.
- Damage caused by the incident may make the area unsafe to enter. The local authority would exercise its powers to remove those imminent dangers that represent a major safety hazard. It may be considered unsafe to allow owners to move in and attempt to deal with their properties simultaneously. In such cases, in the interest of public safety, the local authority may engage approved contractors to board up and commence repair work.

The inner cordon

An inner cordon may well be in place for a prolonged period. However, the boundaries could be redrawn once the search for evidence has been completed, but the immediate area may be out of bounds for days or, in some instances, weeks.

After a time, the police may, subject to advice from the local authority surveyor, allow a limited number of people to enter their premises to undertake damage assessment or retrieve some items.

The outer cordon

The police will aim to keep drawing in the outer cordon so that, at any time, only areas that have yet to be cleared for safety are within it. As premises are progressively freed from the cordon, occupiers will need to be on hand to secure their premises. The police, assisted by the local authority, will ensure that occupiers likely to be affected are given sufficient advance notice of the movement of the cordon boundaries.

(Extracts from material published by LESLP. These extracts are based on the LESLP Manual, a full version of which is available to download from the website: www.leslp.gov.uk).

LIAISON WITH THE FIRE AUTHORITIES

One of the most important contacts to be established is that with your local fire authority/service/brigade.

In some cases, this contact will have been initiated by the fire authority, in particular if your site is a significant one in the area or if there are particular risks associated with your industry or location. In other cases, this contact will have been made by your services, buildings, engineering, security or equivalent department.

Often this contact is neglected by the business continuity manager who either feels that it is not a responsibility of the post or that it has been looked after by someone else in the organization.

It is important that this liaison is established and that responsibility for it is included in the business continuity manager's job specification.

Fire authorities welcome and encourage such liaison, and will get involved with an organization in preparing a pre-fire plan. Pre-fire planning involves getting to know the characteristics of a site, a building, or a business that are vital in a firefighting operation. Such characteristics include layout, content, electrical panels, sprinkler systems, stairways, elevators, exits, false ceilings and any special hazards that may be present. These plans are standard practice for hospitals, hotels, schools, public halls, theatres and other premises where there is a high concentration of people.

A pre-fire plan is usually in a fixed format, and starts with a request for a drawing of the site/premises plus details of site and building entrances and exits, location of gas and electricity services and shut-off points, fire-alarm indicator panels, external stairs, etc.

The fire officers would then visit the site and note the location of the relevant items on the plan. They would also meet the key emergency liaison people and get a good feel for the nature of the site and the arrangements in place.

At that stage the fire authority would file the material at headquarters to be provided to the fire crews called to any incident at that location. Increasingly, this information will be associated with GIS (geographic information systems) and 3D drawings, and made available in electronic form to personnel in fire tenders or other operational vehicles.

MAJOR ACCIDENT HAZARDS

There are demanding directives and legislation that apply to potential hazards involving dangerous substances. This means that there will be close contact between the business and both the regulators and the emergency services.

In 1996, the EU published its Council Directive 96/82/EC – known as Seveso II. Its aims were the prevention of major accidents that involve dangerous substances, and the limitation of their consequences for people and the environment. It is regarded as the most significant international development in this area. The directive became mandatory for industry and the public authorities throughout the EU from February 1999.

In the UK, the Control of Major Accident Hazard Regulations 1999 (COMAH) brought the country into compliance with the Directive.

At present, work is proceeding to broaden the scope of the Directive in response to recent industrial accidents. The cyanide spill into the Tisza river in Romania, following a dam burst, demonstrated that certain storage and processing activities in mining have the potential to produce major accidents. The accident at a fireworks store in The Netherlands, where a series of explosions resulted in 21 deaths and almost 1,000 injuries, demonstrated the major hazard potential arising from storage of such items.

The Directive will extend the scope of industries and premises covered, and will oblige the operators to implement a safety management system that includes a detailed risk assessment on the basis of possible risk scenarios.

Appendices

Appendix 1

Business Continuity Institute – the ten standards

The BCM profession has become increasingly conscious of the need for a relevant methodology to provide a structure to work within. The Business Continuity Institute (BCI) is an important worldwide body which is striving to ensure that the profession operates to accepted professional standards. Along with the Disaster Recovery Institute International (DRII), which is based in the United States, it has developed an internationally accepted set of standards. Aspiring members of the BCI must have a sound understanding of these ten competencies or certification standards.

These standards cover the following areas.

PROJECT INITIATION AND MANAGEMENT

Establish the need for a business continuity plan (BCP), including obtaining management support and organizing and managing the project to completion within agreed time and budget limits.

The professional's role is to:

- lead sponsors in defining objectives, policies, and critical success factors;
- co-ordinate and organize/manage the BCP project;
- present (sell) the project to management and staff;
- develop the project plan and budget;
- define and recommend project structure and management;
- manage the process.

RISK EVALUATION AND CONTROL

Determine the events and environmental surroundings that can adversely affect the organization and its facilities, considering disruption as well as disaster, the damage such events can cause, and the controls needed to prevent or minimize the effects of potential loss. Provide cost-benefit analysis to justify investment in controls to mitigate risks.

The professional's role is to:

- understand the function of probabilities and risk reduction/mitigation within the organization;

- identify potential risks to the organization;
- identify outside expertise required;
- identify vulnerabilities/threats/exposures;
- identify risk reduction/mitigation alternatives;
- identify credible information sources;
- interface with management to determine acceptable risk levels;
- document and present findings.

BUSINESS IMPACT ANALYSIS

Identify the impacts resulting from disruptions and disaster scenarios that can affect the organization, and techniques that can be used to quantify and qualify such impacts. Establish critical functions, their recovery priorities, and interdependencies so recovery time objective can be set.

The professional's role is to:

- identify knowledgeable and credible functional area representatives;
- identify organization functions;
- identify and define criticality criteria;
- present criteria to management for approval;
- co-ordinate analysis;
- identify interdependencies;
- define recovery objectives and timeframes, including recovery times, expected losses and priorities;
- identify information requirements;
- identify resource requirements;
- define report format;
- prepare and present business impact analysis.

DEVELOPING BUSINESS CONTINUITY STRATEGIES

Determine and guide the selection of alternative business recovery operating strategies for recovery of business and information technologies within the recovery time objective, while maintaining the organization's critical functions.

The professional's role is to:

- understand available alternatives, their advantages, disadvantages, and cost ranges, including mitigation as a recovery strategy;

- identify viable recovery strategies with business functional areas;
- consolidate strategies;
- identify off-site storage requirements and alternative facilities;
- develop business unit consensus;
- present strategies to management to obtain commitment.

EMERGENCY RESPONSE AND OPERATIONS

Develop and implement procedures for responding to and stabilizing the situation following an incident or event, including establishing and managing an emergency operations centre to be used as a command centre during the emergency.

The professional's role is to:

- identify potential types of emergencies and the responses needed (e.g., fire, hazardous materials leak, medical);
- identify the existence of appropriate emergency response procedures;
- recommend the development of emergency procedures where none exist;
- integrate disaster recovery/business continuity procedures with emergency response procedures;
- identify the command and control requirements of managing an emergency;
- recommend the development of command and control procedures to define roles, authority, and communications processes for managing an emergency;
- ensure emergency response procedures are integrated with requirements of public authorities.

DEVELOPING AND IMPLEMENTING BUSINESS CONTINUITY PLANS

Design, develop and implement the business continuity plan that provides recovery within the time objective.

The professional's role is to:

- identify the components of the planning process;
- control the planning process and produce the plan;
- implement the plan;
- test the plan;
- maintain the plan.

AWARENESS AND TRAINING PROGRAMMES

To prepare a programme to create corporate awareness and enhance the skills required to develop, implement, maintain and execute the business continuity plan.

The professional's role is to:

- establish objectives and components of the training programme;
- identify functional training requirements;
- develop training methodology;
- develop an awareness programme;
- acquire or develop training aids;
- identify external training opportunities;
- identify vehicles for corporate awareness.

MAINTAINING AND EXERCISING BUSINESS CONTINUITY PLANS

Pre-plan and co-ordinate plan exercises, and evaluate and document plan exercise results. Develop processes to maintain the currency of continuity capabilities and the plan document in accordance with the organization's strategic direction. Verify that the plan will prove effective by comparison with a suitable standard, and report results in a clear and concise manner.

The professional's role is to:

- pre-plan the exercises;
- co-ordinate the exercises;
- evaluate the exercise plans;
- exercise the plans;
- document the results;
- evaluate the results;
- update the plan;
- report results/evaluation to management;
- understand strategic directions of the business;
- attend strategic planning meetings;
- co-ordinate plan maintenance;
- assist in establishing audit programme for the business continuity plan.

PUBLIC RELATIONS AND CRISIS CO-ORDINATION

Develop, co-ordinate, evaluate, and exercise plans to handle the media during crisis situations. Develop, co-ordinate, evaluate and exercise plans to communicate with and, as appropriate, provide trauma counselling for employees and their families, key customers, critical suppliers, owners/stockholders and corporate management during the crisis. Ensure all stakeholders are kept informed on an as-needed basis.

The professional's role is to:

- establish public relations programmes for proactive crisis management;
- establish necessary crisis co-ordination with external agencies;
- establish essential crisis communications with relevant stakeholder groups;
- establish and test media handling plans for the organization and its business units.

CO-ORDINATION WITH PUBLIC AUTHORITIES

Establish applicable procedures and policies for co-ordinating continuity and restoration activities with local authorities, while ensuring compliance with applicable statutes or regulations.

The professional's role is to:

- co-ordinate emergency preparations, response, recovery, resumption and restoration procedures with public authorities
- establish liaison procedures for emergency/disaster scenarios;
- maintain current knowledge of laws and regulations concerning emergencies.

Appendix 2

Business continuity manager – sample job specification

The responsibilities of this post will vary among organizations. The role will vary depending on the nature and size of the organization – the degree of centralization of control, geographic dispersion, organization structure, group structure, public or private sector, utility, services, financial services, manufacturing, wholesale/retail, etc. It will be influenced by regulatory requirements and the degree to which the business continuity and risk management functions have developed to date. Titles can also vary, and can include business continuity planner, disaster recovery co-ordinator and emergency planning manager.

The job description here is for the person responsible for business continuity on an organization-wide basis who would typically report to the group risk director or a level close to the CEO.

POSITION OBJECTIVES

The main objectives of the post are:

- the creation and maintenance of a business continuity culture throughout the organization;
- the co-ordination and development of arrangements, plans and procedures to ensure that the organization can respond to a serious incident in such a way that loss is minimized and the critical business functions and services can resume as quickly as possible;
- co-ordination, development, communication, maintenance and exercising of appropriate business continuity plans for the organization;
- involvement in (if not management of) the response required in the case of any emergency.

REPORTING RELATIONSHIPS

Reports to assistant CEO, with regular reporting to audit/compliance committee of board, and close working relationships with CFO, risk director and head of internal audit.

MAJOR DUTIES AND RESPONSIBILITIES

- Perform risk analysis for each business unit or functional area to identify areas of vulnerability.
- Recommend, and agree with management, appropriate risk management strategies which include disaster avoidance and risk reduction strategies.
- Perform business impact analyses (BIA) in conjunction with local management.
- Identify critical business processes and agree acceptable recovery time targets.
- Agree priorities with senior management based on the outcome of the BIA processes.
- Co-ordinate the development of plans and procedures for all areas, which take account of identified priorities and specify the resources, including personnel, required for the satisfactory resumption of business operations in the event of an incident.
- Ensure that these plans are revised regularly to ensure that they take account of organizational, process or technology changes.
- Co-ordinate the arrangements for exercising plans and evaluating the results of the exercises.
- Ensure there is satisfactory documentation developed and maintained and that adequate training is provided for all concerned.
- Establish and maintain contact with local emergency services agencies.
- Establish emergency response team(s) and ensure that membership and contact details are reviewed and updated regularly.
- Co-ordinate activities in the event of a disaster.

KNOWLEDGE/SKILLS REQUIRED

As with a number of other key functions, knowledge of the organization, its structures, business and people is often more significant than the professional knowledge of the BCM practitioner. If the right person is available from within the organization, it is relatively easy to become acquainted with the methodology and approach to BCM – and these can be supplemented by the judicious use of external help.

- Significant knowledge of the organization or of the industry.
- In-depth knowledge of the process and methodology of BCM – perhaps gained initially by responsibility for the development of the organization's IT disaster recovery (DR) plan.

- Working knowledge of DR planning techniques, including risk analysis and business impact analysis.
- Knowledge of the range of recovery strategies and options so as to recommend and assist with the implementation of recovery solutions.
- Since IT is so significant for most modern businesses, a thorough knowledge of current DR planning, technologies and resilience and recovery options is essential.
- Significant project management skills – as demonstrated by responsibility for major projects. (A number of people became involved in BCM following their successful management of the Y2K project.)
- Ability to see the 'big picture' but still able to give sufficient attention to planning details.
- Ability to formulate investment proposals based on good financial and risk management principles.
- Good verbal and written communication skills.
- Strong leadership, analytical, organizational, human relations and decision-making skills.
- Good administrative skills.

EDUCATION/EXPERIENCE

- Third-level business-related degree or professional qualification.
- At least five years' experience in DR/BCM.
- Attendance at relevant BCM courses or workshops.
- Membership of the BCI or DRII.

Appendix 3

Bibliography, useful contacts and websites

BIBLIOGRAPHY

Books

Butler, Janet G. and Badura, Poul (1994) *Contingency Planning and Disaster Recovery: Protecting Your Organization's Resources*. Computer Technology Research Corp.

Doughty, Ken (2001) *Business Continuity Planning – Protecting your Organization's Life*. Auerbach.

Fulmer, Kenneth L. (2000) *Business Continuity Planning – A Step-by-Step Guide*. Rothstein.

Hiatt, Charlotte J. (2000) *A Primer for Disaster Recovery Planning in an IT Environment*. Idea Group Publishers.

Hiles, Andrew and Barnes, Peter (1999) *The Definitive Handbook of Business Continuity Management*. Wiley.

Jones, Edmond D. (2000) *Business Continuity Self-Assessment Checklist*. Rothstein.

Sadgrove, Kit (1997) *The Complete Guide to Business Risk Management*. Gower.

Toigo, Jon William (2000) *Disaster Recovery Planning*. Prentice Hall PTR.

Journals

Civil Protection
Available free from:
Civil Contingencies Secretariat
Cabinet Office
70 Whitehall
London SW1A 2AS
UK
Available on-line at: www.ukresilience.info/contingencies/cont_publications.htm

Disaster Recovery Journal
11131 E. South Towne Square
St Louis, MO 63123
USA
www.drj.com

International Journal of Business Continuity Management
www.survive.com

Risk Management Magazine
www.rmmag.com

Risk Transfer Magazine
arkgroup
4th Floor
Zeeta House
200 Upper Richmond Road
London SW15 2SH
UK
www.risktransfermagazine.com

Rothstein Catalog on Disaster Recovery
www.rothstein.com
One of the most comprehensive sources of books, software tools, videos and research reports related to BCM and DR.

Strategic RISK
www.strategicrisk.co.uk

USEFUL CONTACTS AND WEBSITES

American Society for Industrial Security (ASIS)
www.asisonline.org

Association of Contingency Planners International (ACP)
www.acp-international.com
Established in 1984, the ACP is a non-profit trade association dedicated to fostering continual professional growth and development in effective contingency and business resumption planning.

Association of Insurance and Risk Managers (AIRMIC)
www.airmic.com
AIRMIC has a membership of about 1,000 UK and overseas risk managers in industry, commerce and public service. It is dedicated to the interests of professionals practising, or responsible for, insurance and risk management. The association assists its members in terms of self-development, technical awareness

and internal working relationships, as well as representing their interests with the insurance market, government and the media.

Association of Local Authority Risk Managers (ALARM)
www.alarm-uk.com
ALARM assists, advises and represents public sector organizations in the UK in the development of risk management strategies. It has over 1,200 members and has been instrumental in raising the profile of risk management in the public sector.

Australian Emergency Management Association
www.ema.gov.au

Australian Institute of Risk Management
www.unirisk.se

British Security Industry Association (BSIA)
www.bsia.co.uk

British Standards Institute (BSI)
www.bsi-global.com

Business Continuity Institute (BCI)
PO Box 4474
Worcester
WR6 5YA
UK
www.thebci.org.uk
Established in 1994, the aims and objectives of the BCI are:

- to promote the art and science of BCM;
- to define the professional competencies expected of business continuity professionals;
- to provide an internationally recognized certification scheme for the business continuity profession;
- to provide a programme of continuous professional development to enable members to maintain their professional competencies;
- to provide and maintain a code of practice and ethics applicable to the supply of business continuity services and consultancy, whether by suppliers or by staff acting on behalf of the organization;
- to establish a membership that can be relied upon by employers and purchasers of service to undertake assignments with professional competence and integrity;

- to encourage the growth and provision of services to support the membership in their endeavours to meet and maintain the defined professional standards.

The BCI has over 1,100 members in 35 countries. It has five membership grades – student, affiliate, associate, member and fellow.

Canada – Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)

www.epc-pcc.gc.ca

www.ocipep.gc.ca

In 2001, the Canadian prime minister announced the creation of OCIPEP which encompassed the existing functions of Emergency Preparedness Canada. The office was charged with developing and implementing a comprehensive approach to protecting Canada's critical infrastructure. It was given the task of providing national leadership to help ensure the protection of the infrastructure, in both its physical and cyber dimensions, regardless of the source of the threats or vulnerabilities. It is the Canadian government's primary agency for ensuring national civil emergency preparedness.

The objectives of the office are:

- to build partnerships with the private sector, the provinces, territories and municipalities, and key international partners – the United States in particular;
- to promote dialogue among Canada's critical infrastructure owners and operators, and foster information-sharing on threats and vulnerabilities;
- to provide a focal point for the federal government's own cyber incident analysis and co-ordination efforts, and support federal departments and agencies in meeting their responsibilities for protecting their IT systems and networks;
- to promote other areas of co-operation such as raising awareness, enhancing education and training, and promoting information technology security research and development;
- to achieve an appropriate level of national civil emergency preparedness.

Computer Security Institute

www.gocsi.com

Established in 1974, CSI has thousands of members worldwide, and provides a wide variety of information and education programmes to assist practitioners in protecting the information assets of corporations and governmental organizations.

ContinuityPlanner.com
www.continuityplanner.com
This is the host site of *E-ZINE* which is published bi-weekly and is read by some 10,000 professionals in business continuity and emergency management in North America and around the world.

Contingency Planning and Management
www.contingencyplanning.com
The aim of Contingency Planning and Management is to be a central resource for technology, products, services, information and management strategies that support business continuity.

Contingency Planning Exchange (CPE)
www.cpeworld.org
The CPE consists of contingency planners representing a wide cross-section of business, government and industry in the United States. It is managed by a volunteer executive board, and among its objectives is provision of a forum for its members to exchange information, and guidance for them on all business continuity issues.

Contingency Planning and Recovery Institute
www.masp.com/cpri

Deloitte & Touche
www.deloitte.com

Department of Trade and Industry (UK)
www.dti.gov.uk/epd/index
www.dti.gov.uk/cii/datasecurity
The Information Security Breaches 2002 sponsored by the DTI can be accessed at this site. This survey, which is intended to help UK business understand the risks in the information security arena, is the sixth such survey since 1991. The survey was managed by PricewaterhouseCoopers, in association with a number of specialist IT security companies.

Disaster Recovery Information Exchange Canada (DRIE)
www.drie.org
Founded in 1994, DRIE Canada aims to become the primary source of information and education for contingency planners across Canada. It is a non-profit mutual benefit association of systems and business professionals engaged in, or having an interest in, the various forms of planning for an emergency or a disruption of normal operations.

Disaster Recovery Institute International (DRII)
111 Park Place
Falls Church
VA 22046-4513
USA
www.dr.org
Founded in 1988 in St Louis, MO, to provide a base of common knowledge in contingency planning, this non-profit organization aims to:

- promote a base of common knowledge for the business continuity planning/ disaster recovery industry through education, assistance and publication of the standard resource base;
- certify qualified individuals in the discipline;
- promote the credibility and professionalism of certified individuals.

It has about 2,500 members in 15 countries. It claims to administer the industry's premier global certification programme for qualified business continuity and disaster recovery planners. It has three membership grades – associate (ABCP), certified (CBCP) and master (MBCP).

It has one full international affiliate – DRI Canada – and a number of international representatives.

Disaster Resource Guide (USA)
www.disaster-resource.com
This site includes articles on DR-related topics, lists of products and services, and is generally a comprehensive source of crisis/emergency management and business continuity management information.

Emergency Planning Society (EPS)
Northumberland House
11 The Pavement
Popes Lane
London W5 4NG
UK
www.emergplansoc.org.uk
The EPS was formed in 1993 through the merger of bodies founded in the 1940s. It is a non-profit professional body for individuals and organizations that have an involvement with any form of emergency, disaster or crisis planning or management. It has over 1,300 members, largely in the UK and Ireland. The primary aims of the society are to promote effective emergency planning and management and to promote the professional interests of its members.

In the UK, the EPS is recognized by government departments as an appropriate consultation body on all aspects of emergency planning and management. It is represented on various working parties and forums. It has established a number of professional interest groups dealing with issues such as:

- oil pollution
- nuclear safety
- chemical accidents
- business continuity management
- crowd safety.

Federal Emergency Management Agency (FEMA)
www.fema.gov
FEMA is an agency of the US government, established in 1979 with headquarters in Washington DC and reporting to the President. Its mission is to reduce loss of life and protect the nation's critical infrastructure from all types of hazards through a comprehensive, risk-based, emergency management programme of mitigation, preparedness, response and recovery.

Following September 11, FEMA and the Structural Engineering Institute of the American Society of Civil Engineers, in association with New York City and a number of other agencies, studied the performance of buildings at the World Trade Center site. The executive summary, findings and recommendations of the resulting report are available on the FEMA website.

Federation of European Risk Management Associations (FERMA)
www.ferma-asso.org

Financial Services Authority UK (FSA)
www.financialsectorcontinuity.gov.uk
The Bank of England, HM Treasury and the FSA maintain a joint website about continuity management in the UK financial sector. The website is intended to help users know who is doing what in this area. It provides an overview of the main organizations involved in this work within the financial services sector. It outlines their responsibilities and activities, and gives a brief summary of the key issues being addressed. It is intended to be a central point of information.

Fire Protection Association
www.thefpa.co.uk

Gartner
www.gartner.com

Global Association of Risk Professionals (GARP)
www.garp.com
GARP is a non-profit, independent, international association of risk management practitioners and researchers.

Globalcontinuity.com
Portland House
Aldermaston Park
Aldermaston
Berkshire RG7 4HR
UK
www.globalcontinuity.com
A leading online information service for everyone involved in business risk and continuity planning. A very comprehensive, up-to-date and proactive site. Highly recommended.

Globalcontinuity.com has more than 32,000 members in 120 countries and provides real-time breaking news and business continuity information and services to industry professionals. It is owned by the Neverfail Group, which was founded in 1993 as Adam Associates, a consultancy and disaster recovery firm.

IBM
www.ibm.com/services
IBM Business Continuity and Recovery Services is a business unit within IBM Global Services. Its services include hot sites, consultancy, risk analysis and management, disaster avoidance, recovery assessment and planning services, and critical business process continuity services.

Information Security Forum (ISF)
www.securityforum.org
The ISF is an independent, non-profit association of leading organizations that is dedicated to clarifying and resolving key issues in information security and developing security solutions that meet the business needs of its members. The forum's Standard of Good Practice is available to non-members and can be obtained from www.isfsecuritystandard.com

INFOSYSSEC
www.infosyssec.org
A security portal for the information system security industry.

Institute of Chartered Accountants in England and Wales (ICAEW)
www.icaew.co.uk

Institute of Directors
www.iod.com

Institute of Emergency Management (IEM)
www.iem.org
The IEM, based in the UK, was incorporated in 1996 by professional emergency planners and managers who recognized the need to research and improve the response to major incidents.

Institute of Internal Auditors
www.theiia.org
www.iia.org.uk

Institute of Risk Management
www.irmgt.co.uk

Interactive Risk Forum
www.riskforum.com

International Association of Emergency Managers
www.iaem.com

London Emergency Services Liaison Panel (LESLP)
www.leslp.gov.uk
LESLP was established in 1973 and consists of representatives from the Metropolitan Police Service, London Fire Brigade, City of London Police, British Transport Police, the Ambulance Service and local authorities. Its purpose is to ensure a partnership approach between all the relevant agencies in the planning for, and the response to, a major incident of whatever kind within the Greater London area. The work of the LESLP has been recognized as a role model of inter-agency co-operation in the planning and response to a disaster.

National Association of Securities Dealers (NASD)
www.nasdr.com
A regulation website.

National Center for Crisis and Continuity Co-ordination (NC4)
www.nc4.us
NC4 is a US for-profit organization focused primarily on advancing crisis management and business continuity readiness through public-private sector collaboration. It began operations in June 2002.

National Computer Security Centre (NCSC)
www.nsa.gov/isso/partners/ncsc
The NCSC of the National Security Agency in the United States is a world leader in information systems security standards and solutions.

National Emergency Management Association
www.nemaweb.org

National Infrastructure Security Co-ordination Centre (NISCC)
www.niscc.gov.uk
www.uniras.gov.uk
The NISCC is the interdepartmental organization set up in the UK to co-ordinate and develop work within government departments and agencies, and organizations in the private sector to defend the UK Critical National Infrastructure against electronic attack. Its work is focused on critical IT systems within the following sectors – telecommunications, energy, financial, transport, central government, water and sewerage, health services and emergency services.

National Security Agency (NSA)
www.nsa.gov
The NSA is the US cryptologic organization. It co-ordinates, directs, and performs highly specialized activities to protect US information systems.

Operational Risk Research Forum
www.orrf.org

Practical Risk Management
www.pracrisk.com

PricewaterhouseCoopers
www.pwcglobal.com

Public Agency Risk Managers Association
www.parma.com
US forum that promotes, develops and facilitates education and leadership in public sector risk management.

Public Risk Management Association (PRIMA)
www.primacentral.org
PRIMA is a non-profit association offering risk management education programmes, management information, and publications to people involved in public sector risk management in the United States.

Risk and Insurance Management Society (RIMS)
www.rims.org
RIMS is a non-profit organization dedicated to advancing the practice of risk management, a professional discipline that protects physical, financial and human resources. The site includes an online risk management journal.

Risk Information
www.riskinfo.com
www.rmisweb.com

Risk Management Reports
www.riskreports.com

Risk Professionals On Line
www.rpo.com

Society of Industrial Emergency Services Officers (SIESO)
www.sieso.org.uk
SIESO aims to be a forum for sharing experience, ideas and practices for avoiding industrial accidents and improving the planning and management of responses to them.

Society for Information Management
www.simnet.org

SlumbergerSema
www.slb.com
A major supplier in the world of business continuity. Its consultants work with clients through every step of the business continuity process, from planning to implementation and testing.

Strohl Systems
www.strohlsystems.com
A leader in business continuity planning software and services. It offers a number of software products in the business continuity arena, such as LDRPS, which are market leaders.

Sunguard
www.sunguard.com
A leading worldwide provider of high-availability infrastructure for business continuity. In November 2001 it acquired Comdisco Availability Solutions which also had a high profile in the business continuity industry.

Survive
107-111 Fleet Street
London EC4A 2AB
UK
www.survive.com
Survive is an international, industry-wide group for business continuity practitioners with a membership of about 3,000. Its mission is to facilitate the spread of best practice throughout industry so that organizations are better prepared to maintain critical business functions in the face of any interruption to normal processes.

Synstar International
www.synstar.com
A leading provider of business continuity services in Europe.

TIEMS (The International Emergency Management Society)
www.tiems.org
TIEMS was founded in 1993. It is a non-profit organization that organizes an annual forum for the exchange of ideas on the avoidance, mitigation, response to and recovery from disasters.

UK Government Emergency Response Site
www.ukresilience.info
The aim of this site is to provide information that will support organizations during disasters. It is a source of public information during events of national importance, as well as being a very significant site in relation to many aspects of emergency planning and advice. The site is run by the News Co-ordination Centre of the Cabinet Office's Civil Contingencies Secretariat.

Appendix 4

Glossary of terms

Access denial Any damage, failure or other condition that causes denial of access to a site, building or the working area within the building, e.g. fire, flood, contamination, riot, industrial action, loss of services, air conditioning failure, forensics.

Activation The implementation of recovery procedures, activities and plans in response to the declaration of an emergency, designated incident or disaster.

Alternative site A location, other than the normal facility, that can be used to conduct business functions.

Back-up The regular and systematic copying of important computer data, which can be used if the original data is lost, corrupted or is otherwise unavailable.

Bandwidth A characteristic of a communications channel that is the amount of information that can be passed through it in a given amount of time, usually expressed in terms of bits per second. Very important in terms of speed of internet access and in designing remote back-up facilities for computer operations.

Biometrics Increasingly important technologies for authenticating the identity of an individual user of computer systems by using fingerprints, palm prints, retinal scans, or other biological signatures.

BS 7799 A British Standards Institute (BSI) standard for information security management. Section 9 deals with business continuity management.

Business continuity co-ordinator A key member of the business recovery management team who is assigned the overall responsibility for co-ordination of the recovery planning programme, ensuring team member training, testing and maintenance of recovery plans.

Business continuity management (BCM) The act of anticipating incidents that will affect mission-critical functions and processes for the organization, and ensuring that the organization responds to any incident in a planned and rehearsed manner; *or* those management disciplines, processes and techniques that seek to provide the means for continuous operation of the essential business functions under all circumstances.

Business continuity planning (BCP) The advance planning and preparations that are necessary to identify the impact of potential losses; to formulate and implement viable recovery strategies; to develop recovery plan(s) that ensure continuity of organizational services in the event of an emergency or disaster; and to administer a comprehensive training, testing and maintenance programme.

Business continuity programme An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and recovery plans, and ensure continuity services through personnel training, plan testing and maintenance.

Business impact analysis (**BIA**) A management-level analysis that identifies the impacts of losing company resources. It measures the effect of resource loss and escalating losses over time in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

Business recovery services Vendor-provided services intended to aid businesses in recovering critical business processes/activities following an unplanned interruption.

Cluster Two or more computers that are interconnected for the purpose of improving reliability, availability, serviceability and/or performance.

Cold site One or more data centres or office space facilities equipped with sufficient environmental conditioning, electrical connectivity, communications access, configurable space and access to accommodate the installation and operation of equipment by critical staff required to resume business operations. Essentially it is a shell site that is prepared to receive computer and communications hardware and software that may be used on an ongoing basis for emergency system operations if a primary computer facility is unavailable.

Contingency plan A plan of action to be followed in the event of a disaster or emergency that threatens to disrupt or destroy the continuity of normal business activities and that seeks to restore operational capabilities.

Crisis An abnormal situation, or perception, that threatens the operations, staff, customers or reputation of an enterprise.

Crisis management team (**CMT**) A group of executives who direct the recovery operations while taking responsibility for the survival and the image of the enterprise.

Data recovery The process of salvaging data stored on damaged media such as magnetic disks or tapes.

Data replication The practice of maintaining an up-to-date, 'hot' standby of the most critical computer data for immediate point-of-failure recovery.

Declaration A formal statement by authorized personnel that a state of disaster exists and that the emergency activities and plans should be activated.

Disaster Any accidental, natural or malicious event that threatens or disrupts normal operations or services for sufficient time to affect significantly, or to cause failure of, the enterprise; *or* an event, or series of events, that disrupts the business for an unacceptable period of time.

Disaster recovery plan (**DRP**) A plan to resume or recover a specific essential operation, function or process of an enterprise; *or* a statement of actions to be taken before, during and after a disaster.

E-commerce The use of computers and electronic communications in business transactions. It may include the use of EDI (electronic data interchange), electronic funds transfer, internet advertising, websites, online databases, computer networks and POS (point-of-sale) computer systems.

Electronic vaulting In critical computer systems, this relatively costly service provides for data to be sent directly from the subscriber to the hot site. This involves a direct-access storage device (DASD) being dedicated to the subscriber and updated in real time via a fast communications link.

Emergency An actual or impending situation that may cause injury, loss of life, destruction of property or interfere with normal business operations to such an extent to pose a threat of disaster.

Encryption A method of defeating attempts to eavesdrop on data communications by encoding the data according to a scheme known only to the originator and recipient of the transmission.

Extranet The part of an organization's internal computer network that is available to outside users, for example, information services to customers.

Fire classifications Class A: a fire involving solid materials, usually of an organic nature, in which combustion normally takes place with the formation of glowing embers; Class B: a fire involving liquids or liquified solids; Class C: a fire involving gas or gases; Class D: a fire involving metals; Class F: a fire involving cooking fats or oils.

Fire compartment A building, or part of a building, comprising one or more rooms, spaces or storeys, constructed to prevent the spread of fire to or from another part of the same building, or an adjoining building.

Fire resistance The ability of an element of building construction, component or structure to fulfil, for a stated period of time, the required stability, fire integrity and/or thermal insulation and/or other expected duty in a standard fire resistance test.

Firewall A system designed to prevent unauthorized access to or from a private computer network. Firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet.

High availability (HA) The ability of a system to perform its function without interruption for an extended period of time. HA can be accomplished through special HA software and the implementation of redundant system and network hardware components. In a properly designed HA system, all of the possible failure modes for critical applications, network connections and data storage have been identified and the recovery times have been analyzed.

Hot site A data centre facility or office facility with sufficient hardware, communications interfaces and environmentally controlled space capable of providing relatively immediate back-up data processing support.

Hot standby A redundant or spare system that is available to take over the functions of a failed system immediately upon detection of failure.

Information risk The chance or possibility of harm being caused to a business as a result of a loss of confidentiality, integrity or availability of information.

Intranet An internal internet belonging to an organization and accessible only to the organization's employees.

Invocation A formal notification to a service provider that the services are now required because of an incident – e.g. the need to use a contracted hot site or recovery work area.

ISO 17799 This is an international version of the British Standard 7799. One section deals specifically with business continuity management.

Maximum acceptable outage (MAO) The maximum time that a given resource or function can be unavailable before the organization will sustain unacceptable consequences.

Maximum probable loss Calculation of the estimated financial loss that may be incurred by an organization in the event of an outage. It should take into consideration revenue/cost, losses incurred associated with property and equipment, software and data, the application of business interruption and property insurance and mitigating expenses.

Mirroring A method of storage in which data from one disk is duplicated on another disk so that both drives contain the same information, thus providing data redundancy.

Operational risk The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from certain external events.

Public key infrastructure (PKI) The total system used in verifying, enrolling and certifying users of a security application.

Recovery point objective (RPO) In IT terms, the point in time to which computer data must be recovered in order to resume processing business transactions.

Recovery time objective (RTO) The target timeframe for restoration of critical business processes and services; *or* in an IT context, the maximum period of elapsed time from the disaster required to complete the recovery of critical computer data to allow for the resumption of business transaction processing.

Redundant array of inexpensive disks (RAID) A method of combining hard disks into one logical storage unit which offers disk-fault tolerance and can operate at higher throughput levels than a single hard disk.

Risk assessment and management The identification and evaluation of operational risks that particularly affect the enterprise's ability to function.

Risk reduction or mitigation The implementation of the preventative measures that risk assessment has identified.

Single point of failure (SPOF) A critical function, support service, or other key resource that cannot be effectively redirected or recovered elsewhere, in an organization; *or* from an IT perspective, one component or path in a system, the failure of which would make the system inoperable.

Social engineering A computer attack based on deceiving users or systems administrators at the target site. Social engineering attacks on computer systems are typically carried out by telephoning users or systems administrators and pretending to be an authorized user, to attempt to gain illicit access to systems. 'I have forgotten my user-id and password, please help me!'

Spoofing Pretending to be someone else – e.g. using someone else's password to gain access to a system.

Structured walk-through An exercise in which team members verbally review each step of a plan to assess its effectiveness, identify gaps, bottlenecks, constraints and other deficiencies and opportunities for enhancements.

Tabletop exercise The exercising and testing of a business continuity plan, using a range of scenarios, while not affecting the enterprise's normal operation.

TCP/IP Transmission Control Protocol/Internet Protocol – the networking protocols used in the internet and similar data networks.

Trusted third party (**TTP**) An agency providing security-related services and activities to one or more entities in a given security infrastructure – usually PKI.

Turnbull Nigel Turnbull, Chairman of the Institute of Chartered Accountants in England and Wales (ICAEW) Committee on the Guidance for Directors on Internal Controls. The report/guidance that issued from this working group is known as 'Turnbull' or the Turnbull Report.

Uninterruptible power supply (**UPS**) A back-up power supply capable of storing and allocating enough power to provide for momentary power outages and for the controlled shutdown of systems and equipment in the event of interruption of normal electrical service.

Virus (**computer virus**) A software program that on execution inserts copies of itself into other programs. A 'worm' is similar to a virus but it has the ability to spread over a network. The majority of viruses are now spread by e-mail, and anti-virus software at the e-mail server is the most effective way of stopping or minimizing the spread of viruses.

Vital record A record that is essential for preserving, continuing or reconstructing the operations of the organization and protecting the rights of the organization, its employees, its customers and its stockholders.

Warm site An alternate site that has been partially equipped for recovery operations: an intermediate level between a cold site and a hot site.

Work area recovery An alternate site location specifically designed to house business operations during the recovery from a disaster.