Guidance note

BUSINESS RESILIENCE

A Guide to Protecting Your Business and Its People

FPA
Fire Protection Association

InFiReS

InFiReS and this Guidance

This document offers guidance arising from a project carried out by the Fire Protection Association under the sponsorship of the Insurers' Fire Research Strategy (InFiReS) funding scheme.

The scheme is operated by a group of insurance companies supporting a series of expert working groups and consultants who are researching and promulgating best practice for the protection of property and business from loss due to fire and other risks.

This InFiReS guidance was compiled by
Peter Brierley, Senior Consultant, Fire Protection Association

First published by

The Fire Protection Association

London Road

Moreton-in-Marsh

Gloucestershire GL56 0RH

Tel: 01608 812 500, Fax: 01608 812 501

E-mail: fpa@thefpa.co.uk, Website: www.thefpa.co.uk

 ISBN 1-902790 34-0

Copies of this document may be obtained from the publications department of the FPA, at the above address or by calling 01608 812 500 or e-mailing *sales@thefpa.co.uk.*

Printed in Great Britain by Modern Colour Solutions. 2.0/4.05

Contents

Introduction

This document provides an introduction to ways in which management can adopt measures which will help a business survive the effects of a significant and potentially damaging event, such as a flood or a terrorist incident. This approach to business resilience delivers a framework on which a company can build, whatever its size and whatever the nature of its business.

Being prepared for the worst situation that could occur is a sensible policy for dealing with lesser disruptions, and the process of business continuity management will inevitably increase the resilience of your business to disruptions of any size. The process of identification of potential threats, ways of risk reduction and calculation of the most effective response will prove to be a vital tool to any organisaton in the wake of a major incident or disaster. Experience proves that it is a lot easier to plan for the likely effects of potential disaster coolly and objectively in advance, than react in the aftermath.

So, What is Business Resilience?

Business resilience is about safeguarding your business, its people and assets. It should be part of your everyday management planning. If and when you are faced by disaster, that preparation can help minimise the impact and help speed recovery. Thus, business resilience and planning should be regarded as a priority for any business and is equally as critical for small companies as it is for large organisations.

Every year, around 20% of all businesses across the United Kingdom face an event that is unplanned, unwanted and sometimes challenges their very survival. In fact, 80% of affected businesses will never fully recover. That threat may come as a result of fire or flood, theft or fraud, or potentially even terrorist action, but no matter what the cause, businesses that successfully recover to thrive again are those that have:

- Assessed the likely impact on the business of significant and potentially damaging events
- Planned their response in advance
- Tested the effectiveness of the plan and revised it where needed
- Invested time, thought and, where necessary, money in managing risk.

Threats to the business

The well-managed company will already have assessed the everyday hazards that might threaten the business and will have put in place control measures in relation to:

- people
- fire
- security
- computers/networks/communications.

Reminders of the common hazards that should be considered are given in Illustration 2. Business managers may wish to look at the risk control aide-memoire on page 11 when assessing their own businesses.

Whilst risk cannot always be totally eliminated, the likelihood of an event threatening the business can be anticipated and the potential impact lessened by incorporating into the organisation an awareness of risk issues and the measures taken to control them. This is often referred to as Business Continuity Management. It aims to provide a framework within which a business can respond to significant events; embedding a risk-aware culture instils confidence in all those who have an involvement – stakeholders, customers and staff – that their interests are being protected.

Counter Terrorism

At a time of heightened awareness and when central and local government are radically revising arrangements for emergency planning and response, it is vital that business plays its part in improving resilience across the board. Does your business or its products make you particularly at risk from terrorism; does your location – in a city centre, for example – make you vulnerable to denial of access to your premises following an event, even though they may not be directly damaged? The implementation of appropriate measures will help reduce the risk from terrorist action and improve the resilience of your business. Detailed guidance can be obtained from the sources linked at the end of this document. In any event, you should consider the following:

- Manage staff securely: take up references; request proof of qualifications; verify the identity of new employees before confirming a job offer.
- Manage contractors securely: use only established, reputable contractors; investigate contractors' processes for validation of staff; institute procedures involving passes and photographs to identify the persons working at your premises; agree procedures for substituting temporary replacements when the usual staff are unavailable.

- Ensure that staff are aware of procedures to be followed in the event of a bomb warning or other threat at the premises, in the surrounding area or in the event of an instruction to evacuate the premises by the emergency services. Muster points should be established remote from the premises. Visitors and contractors must be accounted for in any evacuation. Bear in mind that it might be necessary sometimes to contain people within the building - if there is an external bomb threat, for instance. In such cases:
  - Designate a safe area where people can gather, away from windows and glazing.
  - The area should have access to toilets and drinking water.
  - The area should be structurally surveyed to ensure that it is blast resistant.
  - Protect against flying glass: this can significantly reduce the number and severity of injuries following an explosion, and can help lessen the scale of damage to your premises.

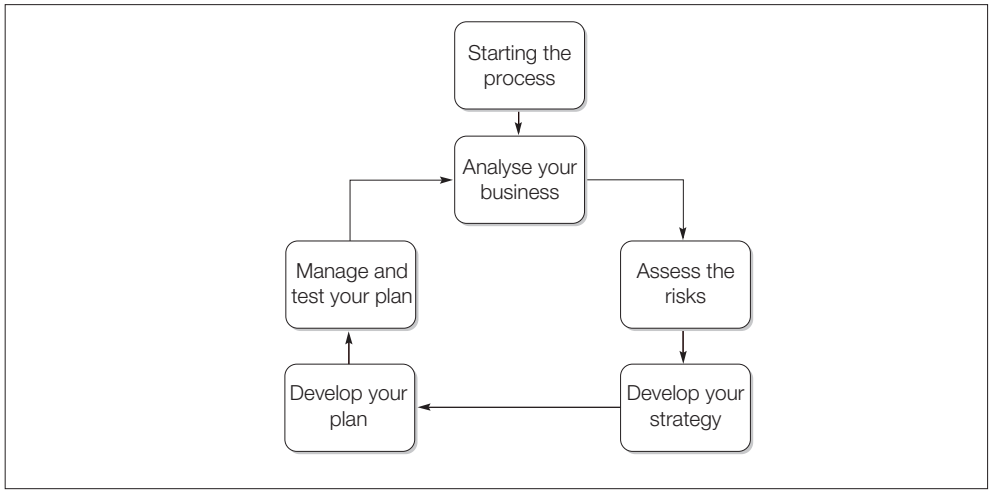
Illustration 1. Company activities and operational sectors linking business resilience planning to perceived threats.

This list of areas for attention will not be complete but within them the average business will find topics around which to assemble a plan of action.

- Basic operation
- Economic effects
- Market factors
- Company departments
  - Personnel
  - Administration
  - Finance
  - Legal
  - Production
  - IT
  - Storage and despatch . . . and the rest
- Logistics
  - Goods inwards
  - Production
  - Goods outwards
- Key people, key operations
- Utilities (electricity, gas, water, internet access)
- Business interruption planning (people, premises, equipment, materials, capacity)
- Equipment (expensive, vulnerable, irreplaceable)
- Health and safety compliance
- Fire and fire prevention planning
- Loss prevention by risk assessment
- Liabilities
  - Workplace
  - Employees
  - Contractual
  - Public
  - Professional
  - Product
  - Environmental
- Training
- Record keeping
- Legislation: awareness

Continuity management structure

There is a simple structure that can help you put your plan in place.



Not all plans need to be complicated but they do need to be easily understood, they need to be comprehensive but suitably tailored to the needs of your organisation. The business continuity management process will make a substantial difference to the possibility of surviving an incident. While it may seem an extra burden to prepare a plan, emergency situations place severe pressure on individuals to make decisions and take action under stressful conditions. Experience proves that such planning makes a substantial difference to the chances of surviving an incident. Above all, it needs to be kept up to date so that it reflects your business as it is, not as it was.

Starting the Process

Planning for business resilience is the responsibility of everyone who owns or manages a business. No matter what the size of the business, similar principles will apply.

- A senior person in the business should take charge of business resilience matters, which should be given the same importance in business planning as quality management, cash flow or health and safety, for example.
- The business resilience 'manager' should assemble a small team of people to survey the nature and mode of operation of the business. The task is to survey the business and make a list of its key features and areas of operation.
- The responsibility for managing business resilience must be clearly established – everyone in the business should understand the importance of resilience and know who is in charge.
- The scope of the work should be established since, for example, an organisation may already have an adequate and up-to-date plan for recovery from a failure of its IT system. Such plans would, however, need to be part of the main plan when complete.

Analyse Your Business

This part of the process is aimed at establishing which processes and functions are critical to the operation of the business and how quickly the impact of their loss will be felt, within what time scale.

Simply put, the task here is to ask:

- Which are the most critical areas of the business? (See Illustration 1.)
- How quickly would losing a function or process have an adverse effect?
- What equipment, staff and systems are necessary to maintain these critical functions?

You should consider:

- Physical assets, including buildings, plant and machinery and stock
- Processes, systems and communications

- Computer systems and the data held on them
- Staff
- Customers and suppliers

Remember to consider service level agreements or legal and contractual obligations that will need urgent attention.

It is often useful to list the functions in each department of your business and then grade them in terms of criticality from, say, 1 (low) to 5 (high). Then to each function allocate a time frame within which the impact would begin to be felt; this may for example be within four hours, within 24 hours, within 1 week. Once this is done, you will have a matrix identifying the priority areas of your business in terms of potential impact and you are ready to move on to the next stage once you are happy the analysis is correct and has been reviewed with appropriate colleagues.

Illustration 2. Potential risks/consequences and related topics

The topics listed on page 11 will help businesses deal with a range of everyday threats. However, you may need to take a broader view. Some of the potential considerations are listed in this table. Some may not be appropriate to your particular business.

Aircraft impact
Alarms
Arson
Assault
Bankruptcy of suppliers
Boiler failure
Bomb threat
Bottleneck in supply chain
Breach of duty or care
Beach of warranty
Burglary
Cash flow
Chemical spill
Civil disturbance
Collapse of buildings
Collapse of market
Combustible materials
Company takeover
Compensation claim
Computer failure
Computer virus
Contamination
Contractors' operations
Contractual liability
Death of staff
Defective structures
Defective products
Disgruntled employees
Distribution chain problems
Earthquake
Electricity failure/shortage
Embezzlement
Employee dishonesty
Environmental impact
Epidemic
Equipment failure
Equipment loss
Explosion
Facilities management
Failure of fire protection measures
Faulty goods
Faulty materials
Fire
Flammable gases/liquids
Flood
Fraud
Freezing weather
Gas leakage
Gas supply failure
Hazardous local events
Hot work
Ignition sources
Inadequate maintenance
Inadequate training
Industrial espionage
Insurance
Internet access
Internet hotel
Intimidation by protest group
Intruders
IT security
Key personnel
Kidnap
Labour relations
Lack of insurance
Lack of planning
Lack of supervision
Libel action
Lightning strike
Litigation
Location
Loss of customers
Loss of goodwill
Loss of market share
Loss of records
Negligence
Pollution
Poor housekeeping
Product liability
Product recall
Radioactivity
Raw material shortage
Regulatory requirements
Remote monitoring of alarms
Riot
Robbery
Sabotage
Security breaches
Smoking
Solvency
Spoilage
Staffing
Storm damage
Strike
Subsidence
Supply shortages
Taxation
Terrorism
Theft
Tidal wave
Transport damage
Trespassers
Troublesome neighbours
Upkeep of premises
Vandalism
Vehicle problems
Water damage
Water supply
Web site crash
Workplace

Assess the Risks

When thinking about the risks in your business, it is necessary to consider:

- How likely is it to happen?
- What will be the effect if it does?

Your answers to these questions will help you to gauge the threat from the risks identified so far. For instance, how much would you lose in cash terms if a particular function were off-line? How long could you afford it to stay off-line? Your assessment of these factors will guide you to the measures you need to take to protect your business.

There are a number of ways in which you can analyse the information already gathered. Firstly, ask 'What if' questions. For example:

- What if sales data were unavailable for an extended period?
- What if we couldn't get into the building for two weeks?
- What if we had no power supply?
- What if we had no means to pay invoices?
- What if our major supplier went out of business?

Secondly, consider the worst-case scenario. This is less about the nature of the event – it might be a fire or a terrorist bomb – and more about the effects of such an event. For instance, a major fire might destroy large parts of your premises and plant. This could lead to no production, loss of finished stock and an inability to supply customers: how would they respond? How could you communicate with them to ensure that they are not lost to you permanently? The same fire may have destroyed all your records, computer hardware and tooling specifications; how can you maintain cash flow or replace destroyed tools?

Best practice would also suggest consideraton of the impact of a major event affecting not only your business but also the local community. To this end, liaison with your local authority emergency planning department is to be recommended – to ascertain their likely response to such an event and also gather details of any roles identified for local businesses in the aftermath.

Finally, consider your staff. Identify those with special skills, knowledge or responsibilities that will be vital in different time frames after the event – within the first four hours, the first day and so on. Assess the risk that such staff may not be available.

Develop Your Strategy

The work done so far should have identified the way your business is organised, the risks facing it and the potential damage to the business from a range of scenarios. Developing your strategy is really about deciding what level of risk you are prepared to accept; this in turn will help you decide on the actions to be taken. It may be prudent to consult your insurer, who will be able to offer advice, guidance and solutions to some of your risk management problems. There are various options open to you:

- Accept the status quo
- Reduce the likelihood and/or the effect of the risks to a more manageable level
- Eliminate or reduce risks to negligible level.

The first option could be seen as something of a gamble, as it relies on the ability to recover from an event quickly and completely; however, your analysis and assessment work will have identified for you the dangers inherent in this approach – by the time you have recovered, customers may have found an alternative supplier or perhaps competitors will have stepped into the breach.

The third option can involve considerable expenditure, so the middle way is often the preferred route. Here, you should reduce as far as is practicable the risk of something happening – together with lessening its effects. Your Continuity Plan then details the way in which you will deal with any remaining risk in the event of an incident.

You should also consider the use of outside assistance as part of your recovery strategy. It may be possible to agree a reciprocal deal with another company to use facilities at each other's premises in the event of loss at either – such facilities could range from canteen to computer networks. Alternatively, contracts can be agreed with a specialist supplier for the provision of suitable temporary buildings and equipment when needed: this is known as a 'cold site'. A 'hot site' by contrast is one where you have access to fully equipped premises, usually within hours of the original event. Alternatively, you can rely on the market and simply take premises of the right size in a suitable location when you need them – but, when developing your strategy, don't forget the time delay in obtaining all necessary consents, completing legal processes and fitting the property out for occupation.

Develop Your Plan

In writing your plan it is important to use simple, clear, non-technical language so that everyone who will need to use it can readily understand. Remember, that what is a common expression in one part of your business may be unintelligible jargon in another.

Your plan should include:

- **A clear statement of purpose and scope.** Include here a statement of support from senior management to ensure that the plan carries sufficient weight within the business
- **Recovery management team.** Involve those people needed to get things moving and take the necessary decisions. Include deputies to cater for holidays and absences and bear in mind that incidents may occur at night or weekends. You may want to have additional members who join the team at later stages to work on elements of the recovery. Ensure that responsibilities are clear and that members of the crisis team know exactly how their communications will work. State where and when the team will meet, on-site or off-site, depending on circumstances.
- **Recovery procedures.** Be specific about the initial actions to be taken in the first few hours following an incident and specify reporting procedures so that progress can be monitored. Maintain up to date inventories of equipment and software so that replacements can be ordered. Ensure that mobile telephones will be available to team members.
- **Public relations.** Your public response to an incident may be the difference between success and failure in recovery terms. Remember that damage to your company's reputation or brand can do just as much damage as a fire. Plan how you will deal with the public, customers, suppliers and the media. There should be a single point of contact within the crisis team.
- **Staff.** Plan to communicate with staff to ensure that they know the up to date position. Use telephone cascades, local press advertising or other means as necessary.
- **External information.** Include here contact information for emergency services, utilities, insurance, neighbouring businesses. Outline the information each will need immediately after an incident.

Manage and Test Your Plan

Your plan is now complete and its contents have been publicised throughout the company to ensure that everyone is aware not only of their roles in the event of an incident, but also, especially, their responsibility to prevent problems in the first place. You could use this as an opportunity to identify and meet any relevant training needs.

However, this cannot be a one-off exercise. Businesses change and your plan must also change if it is to remain effective. So, make sure that the plan is reviewed and revised frequently and reflects the current position.

You should aim to exercise your plan after it is completed and following significant changes. You can test in a number of ways:

- Paper-based exercises can be useful. Get a group together and question the plan's provisions. Ask the 'what if' questions again. Listen to the feedback and amend the plan if necessary
- Test your telephone cascade by sending a test message, without warning, to the people at the top of the cascades. The last person on each cascade can then be contacted to see when they received the message. This helps you to check that your communications structure is working and, again, make changes if needed
- Full rehearsal means putting your plan into operation in a simulated environment. Though you will probably not be able to use alternative premises unless you have contracted for a 'hot site', the opportunity to have recovery management team members working together can highlight any shortcomings in planning or implementation.

Alternatively, it is possible to recruit a consultant company to help you test your plan – ask your insurance company for guidance on this option.

Finally, ensure that the recovery management team have the information and resources they will need to operate successfully in the aftermath of an incident, whether serious or minor. You should have an 'emergency box' or boxes, which should be located off-site or in a secure place, which can be accessed quickly following an incident and which contains items such as:

- Full copy of the Continuity Plan
- Staff lists with contact/cascade details
- Inventories
- External contact details
- Site plans
- Keys
- First aid kit
- Torches
- Batteries
- Writing materials and stationery
- High visibility jackets and hard hats

Summary

Business Continuity Management is a matter of proper business planning. There are numerous packages available in bookstores and via the internet which include templates to help construct a plan, but remember that the key to the process is knowing your own business, analysing it and addressing any problems identified.

Those who wish to involve themselves more deeply in the theory of the subject could look at the British Standard Institution's Publicly Available Specification 56 (PAS 56), which is BSI's first move towards publishing a British Standard on business continuity management. The main objectives of PAS 56 (see also Further Reading, page 12) are:

- to define the process, principles and terminology of business continuity management;
- to provide a framework for preplanning, anticipation and response;
- to describe evaluation techniques and criteria.

Last, but not least, make sure that your insurance cover is adequate and up to date and that its scope is broad enough to provide the financial help your business will need following damage – but remember, whilst insurance has an important role to play, this does not guarantee continued existence following a disaster. The chance of your business surviving will be significantly increased if you have anticipated the disaster and are able to respond effectively to minimise its impact.

Links

More information is available from:

- Your insurance broker or company
- Fire Protection Association: *www.thefpa.co.uk*
- Association of British Insurers: *www.abi.org.uk*
- Association of Insurance and Risk Managers: *www.airmic.com*
- Business Continuity Institute: *www.thebci.org*
- Emergency Planning Society: *www.emergplansoc.org.uk*
- Department of Trade and Industry: *www.dti.gov.uk*
- Home Office: *www.homeoffice.gov.uk*
- Institute of Risk Management: *www.theirm.org*
- UK Resilience (Civil Contingency Secretariat): *www.ukresilience.info*
- Survive: *www.survive.com*
- British Damage Management Association: *www.bdma.org.uk*
- Continuity Insurance and Risk: *www.cirmagazine.com*
- Continuity Central: *www.continuitycentral.com*

Specific advice on counter terrorism measures can be found at:

- *www.mi5.gov.uk*
- Via the Counter Terrorist Security Advisor at your local police force

Table. Risk control aide-memoire

People

- Maintain up to date lists of all employees, including part time, temporary and agency staff, detailing names, addresses, phone numbers and next of kin
- Ensure all visitors are logged in and out of the premises
- Provide staff with training in emergency and evacuation procedures in the event of both fire and terrorist action
- Write down your safety, fire and security policies and ensure staff understand them
- Train staff in the use of fire extinguishers and raising the alarm

Fire

- Identify significant hazards from processes, storage and services and how these can be removed or reduced
- Maintain high standards of housekeeping, including waste removal and a clear desk policy
- Ensure adequate fire extinguishers of the correct type are provided and that staff are trained in their use
- Consider the use of automatic control and suppression systems such as sprinklers to protect the whole premises or specialist systems such as gas flooding in high risk/high value areas, e.g. computer rooms
- Provide automatic fire detection and alarm systems that signal to an Alarm Receiving Centre upon activation
- Maintain compartmentation within the premises by ensuring walls, doors and shutters are in good condition and that where services or cables penetrate they are adequately fire-stopped
- Undertake a frequent and regular inspection of the premises, rectify any faults found and record your results
- Exercise close control of contractors working on your premises through a permit to work system
- Have all plant, machinery and services tested, inspected and maintained by competent contractors

Security

- Maintain all security devices in good condition and full working order
- Ensure that perimeter fences, walls and gates are in sound repair and secure
- Fit good quality locks to all external doors and protect ground floor and accessible upper floor windows appropriately: this may require shutters, grilles or bars in addition to key operated window locks
- Provide intruder alarm protection that signals to an Alarm Receiving Centre upon activation
- Ensure only authorised people have access to the premises by means of CCTV, static guarding and/or access control systems such as card/PIN or proximity card
- Provide security lighting externally
- Before allowing contractors or others to work on the premises ensure that you have checked their accreditation; if necessary, ensure they are accompanied on site at all times
- Ensure the premises are clear before locking up at the end of the day and that all valuable and sensitive documents, plans or patterns are secure
- Shred all sensitive documents before disposal

Computers, networks and communication

- Control passwords and means of access to and use of systems and networks, including those used by contract staff and those who have left the company
- Provide UPS to ensure safe shut-down in the event of power failure
- Consider provision of stand-by power generation capacity
- Regularly back-up data and software and keep copies in a fire-resisting data cabinet and off site in a secure location
- Consider automatic fire detection in and protection of computer rooms, not forgetting modems and other communication technology
- Keep your anti-virus software up to date
- Protect against lightning strike and power surges

Further Reading

Business continuity management – preventing chaos in a crisis, Department of Trade and Industry, 1999.

Business continuity management factsheets, Department of Trade and Industry, 2004:

Business continuity management
Process
Impact analysis
Risk analysis
Strategy
Plans and process
Risk reduction
Operational management
10 point plan
Testing.

'Business security measures', *Fire protection yearbook 2002,* ch.2, M.Gale (ed.), Fire Protection Association, 2002.

Business as usual: maximising business resilience to terrorist bombings, Home Office, 1999.

Dealing with disaster, 3rd edn, Cabinet Office, Brodie Publishing, 2003.

Disasters and emergencies: managing the response, W.R.Tucker, Institution of Fire Engineers, 1999.

Expecting the unexpected: business continuity in an uncertain world, Business Continuity Institute/London First/National Counter Terrorism Security Office (ACPO), 2003.

Fire risk management in the workplace: a guide for employers, 2nd edition, Adair Lewis and William Dailey, Fire Protection Association, 2002.

FPA Workplace Fire Safety Logbook (includes record forms on CD), Fire Protection Association, 2003.

Guide to business continuity management, PAS 56, British Standards Institution, 2003.

'Guidance for the protection of premises against terrorist attack', ch. 5*, An introduction to physical security techniques*, S.Kidd (ed.), Fire Protection Association, 1996.

The Prevention and Control of Arson, Adair Lewis, Fire Protection Association, 1999.

The Fire Protection Association, in connection with work carried out for the Insurers' Fire Research Strategy (InFiReS) funding scheme, produces a range of documents aimed at preventing losses in industry and commerce. See, in particular, the Recommendations publications in the Risk Control series, via www.thefpa.co.uk.

guidance note

BUSINESS RESILIENCE

A Guide to Protecting Your Business and Its People

FPA
Fire Protection Association

InFiReS