Business Continuity Management for Small and Medium Sized Enterprises

How to Survive a Major Disaster or Failure
Business Continuity Management for Small and Medium Sized Enterprises

How to Survive a Major Disaster or Failure

David Lacey
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>viii</td>
</tr>
<tr>
<td>Introduction</td>
<td>ix</td>
</tr>
<tr>
<td>How to use this book</td>
<td>xi</td>
</tr>
<tr>
<td><strong>1 Making the business case</strong></td>
<td>1</td>
</tr>
<tr>
<td>How much risk should you bear?</td>
<td>1</td>
</tr>
<tr>
<td>Safeguarding business interests</td>
<td>2</td>
</tr>
<tr>
<td>How much work is involved?</td>
<td>3</td>
</tr>
<tr>
<td><strong>2 Key concepts and principles</strong></td>
<td>7</td>
</tr>
<tr>
<td>What, how and who</td>
<td>7</td>
</tr>
<tr>
<td>Be selective and keep it simple</td>
<td>8</td>
</tr>
<tr>
<td>A process, not just a plan</td>
<td>9</td>
</tr>
<tr>
<td>The business continuity management cycle</td>
<td>9</td>
</tr>
<tr>
<td>The language of risk</td>
<td>11</td>
</tr>
<tr>
<td><strong>3 Deciding what to protect</strong></td>
<td>15</td>
</tr>
<tr>
<td>Assessing business criticality</td>
<td>15</td>
</tr>
<tr>
<td>Assessing the impacts of incidents</td>
<td>16</td>
</tr>
<tr>
<td>Conducting a business impact analysis</td>
<td>17</td>
</tr>
<tr>
<td><strong>4 Assessing risk</strong></td>
<td>21</td>
</tr>
<tr>
<td>The nature of risks</td>
<td>21</td>
</tr>
<tr>
<td>The risk management process</td>
<td>22</td>
</tr>
<tr>
<td>The lifecycle of risk management</td>
<td>23</td>
</tr>
<tr>
<td>Identifying critical assets</td>
<td>24</td>
</tr>
<tr>
<td>Assessing threats and risks</td>
<td>24</td>
</tr>
<tr>
<td>Building a ‘heat map’</td>
<td>25</td>
</tr>
<tr>
<td>Capturing further detail with a heat map</td>
<td>27</td>
</tr>
<tr>
<td>Building a risk register</td>
<td>27</td>
</tr>
<tr>
<td>Risk treatment</td>
<td>29</td>
</tr>
<tr>
<td>Communicating risk appetite</td>
<td>33</td>
</tr>
<tr>
<td><strong>5 Identifying hazards and threats</strong></td>
<td>37</td>
</tr>
<tr>
<td>Fire and Flood</td>
<td>38</td>
</tr>
<tr>
<td>Earthquakes</td>
<td>38</td>
</tr>
<tr>
<td>Terrorist attacks</td>
<td>39</td>
</tr>
<tr>
<td>Sabotage and vandalism</td>
<td>39</td>
</tr>
<tr>
<td>Equipment and supply chain failures</td>
<td>40</td>
</tr>
</tbody>
</table>

*This is a sample chapter from Business Continuity Management for Small and Medium Sized Enterprises.*

To read more and buy, visit [http://shop.bsigroup.com/bip2217](http://shop.bsigroup.com/bip2217)

© BSI British Standards Institution
6 Preventing and responding to fire
A continuous process 45
Identifying fire hazards 46
Identifying people and assets at risk 47
Assessing and reducing fire risks 47
Installing fire safety measures 47
Training and drilling staff 48
Maintenance considerations 49
Documentation 49

7 Preparing and planning for floods
Preparing for a flood 51
Establishing your level of risk 51
Identifying people and assets at risk 52
Implementing flood precautions 53
Arranging appropriate insurance 54
Drawing up an emergency flood plan 55
Training employees to deal with flooding 55
What to do after a flood 55

8 Physical security measures
Key principles and measures 60
Safeguarding premises 60
Protecting valuables and assets 62

9 Information security measures
Information security standards for SMEs 66

10 Back-up and fallback arrangements
Making back-up copies 75
Fallback options 77
Building resilience in computer systems 80

11 Preparing the plans
Types of plan and their relationship 85
Emergency plans 86
Contingency plans 87
Drafting your business continuity plan 88
Limitations of plans 89
Foreword

In 1996, I was Chief Executive of the Radiocommunications Agency, an Executive Agency of what was then the Department of Trade and Industry. At 19:02 on the evening of Friday 9 February, our agency headquarters building was destroyed in the Provisional IRA London Docklands ‘South Quay’ bombing. The Agency had a good continuity/disaster recovery plan and, largely, it worked well. This has given me a life-long respect for the importance of continuity planning.

Subsequently, my work with the Institute of Directors back in 2006 illustrated the weaknesses in many small and medium sized enterprises’ understanding of business continuity management. Highlights from one BCM survey included:

- 92% of survey respondents agreed that they had business critical data stored in their ICT systems. I wonder what the others had stored in their systems?
- 28% of respondents admitted to having no ICT business continuity or disaster recovery plans in place. This was worst amongst the smallest companies (1-25 employees) at 43% and in the ‘Distribution and Hotels’ sector at 42%.
- For those with business critical data stored, 11% admitted to backing-up less than once per week (if at all!), with ‘Distribution and Hotels’ the worst sector with 29% backing-up less than once per week.
- For those that did back-up at least once per week, 51% kept their back-ups on-site, with ‘Government, Education, Health and Personal Services’ the worst sector at 72%.
- Of those with Business Continuity plans in place, 90% felt that they were well positioned to survive a disaster (despite the lack of off-site back-ups by many...).

I’m not convinced that the passing of five years has entirely resolved these problems.

I very much welcome the publication of David Lacey’s straightforward and practical book. I commend this book to you. It provides exactly the kind of clear guidance sorely needed.

Professor Jim Norton, President 2011-12, BCS - The Chartered Institute for IT
Introduction

This book is a simple, practical guide on how to go about implementing business continuity management. It is written primarily for business directors and managers in small and medium sized enterprises (SMEs), but it is also a useful guide for consultants or managers working in large organizations with small business units or outlets.

Disasters such as fires, floods and terrorist attacks often strike indiscriminately and without warning. Their impact on business operations can be substantial, regardless of the size of the enterprise. Experience has shown that advanced planning is crucial to preventing and minimizing business damage.

Business continuity management is a simple management process that helps identify potential hazards to your business operations, and equips you with the information, plans and facilities to manage a major disaster or failure. It operates through a combination of techniques, including risk management, contingency planning and crisis management.

In recent years, most large organizations have developed business continuity plans and incident response processes to safeguard their business operations. This is not just in response to regulatory compliance demands, but also because it is a good business practice. Many small companies, however, have yet to catch up with this trend.

One reason for this is that business continuity management has traditionally been a big company practice, requiring specialist consultants, project teams and full time managers. Big organizations need large programmes because of the sheer complexity and scale of planning needed to respond to a major incident across a large enterprise.

The task is much simpler, however, for a smaller business unit. It need not demand a big budget and a large team of people.

This book sets out how business continuity management can be tackled by any small- or medium-sized enterprise, and with a minimum of budget, time and manpower. The objective is to present the key principles and learning points in a form that is digestible, appropriate and, hopefully, compelling.
Introduction

Both the approach and the content of this book are designed to be suitable for SMEs of any size, ranging from a micro company of less than ten people to a medium sized enterprise with hundreds of staff.

The guidance is aimed at ordinary business managers, and it assumes no specialist knowledge or skills. It is designed to enable managers to identify risks to business continuity, and to take simple, affordable steps to minimize their impact. It includes some useful ‘tips of the trade’ for assessing risks, drawing up contingency plans and managing incidents.

The material draws on the real-life experience of the author in developing business continuity strategies and plans for business units of all sizes, ranging from small retail outlets to large global enterprises. It also builds on research carried out on behalf of the UK Information Commissioner’s Office (ICO) and the UK Chapter of the Information Systems Security Association (ISSA) into the requirements of SMEs for security advice and standards.

This book is published at a time of increasing awareness of hazards to business continuity presented by all manner of disruption to normal running, including floods, malware, cyber attacks and even the effects of space weather. These concerns also come at a time when large corporate customers and regulators are beginning to set their sights on tackling weaknesses in supply chains.

With growing dependence on small contractors, big organizations will increasingly expect, and demand, that their SME suppliers raise their game in business continuity planning. This book shows how SMEs can rise to this challenge.

David Lacey
How to use this book

This book provides a logical, step-by-step sequence to understanding business continuity management. You can read it from cover to cover, or dip into selected chapters to find key recommendations on particular topics.

1. Making the business case
2. Key concepts and principles
3. Deciding what to protect
4. Assessing the risks
5. Identifying hazards and threats
6. Preventing and responding to fire
7. Preparing and planning for floods
8. Physical security measures
9. Information security measures
10. Back-up and fallback arrangements
11. Preparing the plans
12. Organizing your response team
13. Training and exercises
14. Learning from incidents
15. Reviewing business continuity plans
16. Summary of this book

Figure 1 – Step-by-step sequence to understanding business continuity management

Chapters 1 and 2 explain the benefits and principles of business continuity management, and include the life-cycle for developing and implementing a business continuity plan.
**How to use this book**

Chapters 3, 4 and 5 take you through the planning activities of identifying what to protect - and from what or whom - including how to carry out a risk assessment and how to develop a simple register of risks.

Chapters 6–9 set out practical guidance for common risks such as fire, flood and security incidents. Every enterprise faces a slightly different set of risks, but some threats and countermeasures are universal, and this chapter aims to provide helpful, prescriptive advice based on well established principles and practices.

Chapters 10 and 11 cover essential tasks to prepare you for a disaster, including back-up and fallback arrangements, as well as how to develop and structure the business continuity plan itself.

Chapters 12 and 13 provide advice on how to organize and train an incident response team.

Chapters 14 and 15 discuss techniques for improving business continuity plans and arrangements, including how to learn from incidents, and how to carry out a review of processes and plans.

Chapter 16 provides a concise summary of the contents of this book for readers who would like a reminder of the key learning points, as well as for those who lack the patience to read it from cover to cover.

Finally, Chapter 17 lists some useful sources of further advice.

There are also helpful summaries of key points at the end of each chapter.
1 Making the business case

This chapter aims to set out the case for business continuity management, and to persuade you that it is a necessary and smart use of your time.

How much risk should you bear?

An important question that will no doubt be going through your mind is, ‘Why should I bother to invest valuable time and money in drawing up a plan for something that might never happen?’

The simple answer is that it will reduce the operational risks to your business, and ensure your survival in the event of a major disaster.

Each business director has a different appetite for accepting risk. Some like to gamble in the hope of gaining a higher return, while others prefer to keep their heads down and play it safe. But whatever your outlook, it is better to have as many of these risks under your control as possible.

Small businesses face enormous risks in today’s highly competitive environment; it comes with the territory of running a small or medium enterprise. You might not be able to do much about the commercial risks you face, but you can certainly take steps to minimize your operational risks. Keep in mind that these risks are often related. A bad operational performance, for example, can affect customer confidence and future sales.

Not all of the risks we face are within our sphere of influence. Economic risks, for example, are part and parcel of the surrounding business environment. Disasters such as floods and earthquakes are the results of circumstances far beyond our control.

Yet many types of risks are created by our own actions. They arise from bad decisions, unconscious oversights or human errors. We can take steps to reduce these risks, though it might not be physically possible to eliminate every last one of them.

Disasters and equipment failures, however, remain inescapable risks, and their impact on business operations is growing with our increasing
dependence on technology, communications and transport. Every business needs to be prepared to tackle such major incidents as and when they arise.

Nearly one in five UK businesses suffers a major disruption every year. Your enterprise could very well be next. In fact, given these odds it is likely you will encounter some form of damaging incident at some point in the future.

Business continuity management will help you to ensure that your key business activities (such as sales, manufacturing, deliveries and purchasing) can be reliably carried out with minimal risk of interruption. It will also help to reduce the level of potential business damage from any form of disruption or ‘outage’, limiting your losses as well as safeguarding your reputation.

Developing the capability to continue to deliver products and customer services throughout environmental hazards will help you to retain your customers and win new business. A speedy response to a disaster helps safeguard your bottom line.

Business continuity management protects your business interests. It is a cornerstone of good corporate governance, as well as a smart business investment.

Safeguarding business interests

If you have already invested in an insurance plan to cover your premises and their contents, then it will also make sense to invest in a set of contingency plans to ensure business continuity. It is all part of the same concept: the need to plan for the worst to safeguard your longer term interests.

You should also consider investing in some form of business interruption insurance. This will compensate you for lost income, based on your financial records, though it is unlikely to provide cover for other possible consequential losses such as lost future business. Minimizing lost future sales will rely primarily on your ability to continue to satisfy your customers both during and immediately after a disaster.

If your clients include large organizations, it is likely that they will at some point ask you about your business continuity arrangements. The need to ensure business continuity across essential supply chains is increasingly being recognized by government agencies, supervisory bodies and large companies. The need for a business continuity plan might also be raised at some point by your bank manager, insurance company or investors.
Business continuity management is a vital element in maintaining your safety and security from hostile acts, such as terrorist attacks. In today's world of heightened terrorist threats, which can strike at any time without warning, business continuity planning is your best defence.

This point is acknowledged by security agencies such as MI5. In the words of Eliza Manningham-Buller, a former MI5 Director General:

*I am often asked what single piece of advice I can recommend that would be most helpful to the business community. My answer is a simple, but effective, business continuity plan that is regularly reviewed and tested.*

Even if you judge that you are unlikely to be a victim of a terrorist attack, you can still be affected by the consequences of such an event. Major incidents can result in damage to critical infrastructure, such as electricity supplies, transport and communications, which are vital to many business services.

Business continuity management is an essential process for any organization that is required to deliver services without interruption. That is why MI5 takes it very seriously. It is also why the UK Civil Contingencies Act 2004 mandates it for frontline responders, such as fire and rescue services. And it is why business continuity is a mandatory policy for all UK public sector organizations.1

**How much work is involved?**

How much preparation is needed to create a business continuity plan? The truthful answer is that it is likely to be quite a bit more than you expect, though the effort should be easily within your capabilities.

Reading this, you might be tempted to do as little as possible and hope that in the event of a major disaster, you will find an easy way of salvaging your assets and continuing your business. But experience has shown that managing your way through a major incident is far from simple. An effective crisis response demands smart planning, detailed preparation and regular rehearsal.

Incidents can of course vary enormously in their impact. Recovering from some hazards, such as an equipment failure or power outage, might be relatively easy. But disasters such as a major fire or flood are likely to cause major damage and upheaval. In such cases it is vital to respond quickly and effectively to contain the damage, establish alternative business facilities, and get back to business as quickly as possible. Ask

---

1 Business Continuity is one of the seven policies set out in the UK Government Security Policy Framework.
1 Making the business case

...
Learning points from this chapter

This brief chapter was intended to set out the arguments for developing a business continuity plan. Here are the key learning points to be taken from this chapter:

- Business continuity management reduces the risks to your business and might ensure your survival in a disaster.
- Regardless of your own appetite for risk, it is better to have as many risks as possible under control.
- Nearly one in five businesses suffers a major disruption every year. Yours could be next.
- Business continuity is a cornerstone of good corporate governance, and a smart business investment.
- If you invest in insurance cover, it also makes sense to invest in business continuity planning.
- If your clients include large organizations, it is likely they will at some point ask you about your business continuity arrangements.
- Business continuity management is your business’ best defence against terrorist threats.
- An effective response demands careful planning, advance preparations and regular rehearsal.
- Business continuity management is not a difficult or expensive task for a small enterprise.
- Simplicity is the key to a fast, smooth recovery.