

**DISASTER RECOVERY AND BUSINESS  
CONTINUITY**

**A Quick Guide for Small Organizations and Busy  
Executives**

**Second Edition**

## ABOUT THE AUTHOR

Thejendra BS is an IT manager for a software development firm in Bangalore, India. Starting as a field engineer in the previous century after his electronics degree, he has more than 17 years' experience in a wide range of roles in IT areas such as support, helpdesk, DRP, BCP, asset management, IT security, and IT project implementation. He has also worked in Saudi Arabia, Dubai, Bahrain, Qatar, Singapore and Australia, and has wide experience of dealing with countless customers and organizations of all sizes and flavours. In addition, he is also a freelance writer and writes articles on management, self-help, stress management, technical, workplace issues, humour and other topics that are frequently syndicated around our planet through several RSS feeds. His articles have also been published on reputed websites such as [cnbc.com](http://cnbc.com), [cio.com](http://cio.com), [techrepublic.com](http://techrepublic.com), [ezinearticles.com](http://ezinearticles.com), [itmuseum.org](http://itmuseum.org), [sourcingmag.com](http://sourcingmag.com), [geekleaders.com](http://geekleaders.com) and many ezines.

Visit his website [www.thejendra.com](http://www.thejendra.com) for details on his other books and articles. He can be contacted on [thejendra@yahoo.com](mailto:thejendra@yahoo.com).

*Other titles by this author from ITGP:*

Practical IT Service Management (2008)

# **Disaster Recovery and Business Continuity**

A Quick Guide for Small Organizations  
and Busy Executives

**Second Edition**

THEJENDRA BS



**IT Governance Publishing**

## **PUBLISHER'S NOTE**

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publishers and the author cannot accept responsibility for any errors or omissions, however caused. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher, or in the case of reprographic reproduction in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publishers at the following address:

IT Governance Publishing  
IT Governance Ltd  
Unit 3, Clive Court  
Bartholomew's Walk  
Cambridgeshire Business Park  
Ely  
Cambs  
CB7 4EH  
United Kingdom

[www.itgovernance.co.uk](http://www.itgovernance.co.uk)

© Thejendra BS 2007, 2008

First published in the United Kingdom in 2007 by IT Governance Publishing (978-1-905356-14-0)  
Second edition 2008 (978-1-905356-37-9)

## FOREWORD

Business Continuity and Disaster Recovery have, over the last five years, become critical business issues. The increasing dependence of organizations on IT systems and the growing range of threats they face – from acts of nature to terrorist attacks – mean that organizations unprepared for the worst usually do not survive the unexpected.

Regulatory authorities recognize the challenge and, in the Basel Accord and in legislation from the UK's Companies Act 2006 to the US Sarbanes-Oxley Act, require company directors to take appropriate action to identify and deal with operational risk. Business continuity is one of the most important areas of operational risk and, for companies that wish to identify and apply best management practice in mitigating this risk, the emergence of the British Standard, BS25999, is a significant development. BS25999 is the world's first formal standard for business continuity management. It contains both a code of practice and a specification for a management system against which organizations can achieve third party accredited certification. Because they will be able to demonstrate to customers and partners their planned business resilience, organizations that have such a certificate will, inevitably, gain a competitive advantage over those that don't.

This book is a welcome guide – for smaller companies – to all the key aspects of business continuity and disaster recovery planning.

Alan Calder, Ely, 2008

## PREFACE

Disaster Recovery and Business Continuity (DR and BC) are often seen by organizations as a costly and complex rocket science that can only be handled by specialists and magicians. Often, individual businessmen, IT departments and managers of small and medium organizations live under the misconception that such activities are beyond their expertise or affordability, and perhaps applicable only to large organizations. Many business owners still live in constant fear and have nagging doubts about how to protect their businesses from various disasters, and who will help.

This book clears away such doubts and myths to show you how DR and BC can be successfully implemented with a simple combination of qualified internal staff, vendors, external consultants and plain common sense. This is a quick guide to business recovery best practice that draws on the new British Standard BS25999 and that can be almost read like a story book. It is designed to be a concise handbook for technical and business staff in organizations wishing to know what disaster recovery and business continuity are all about. The entire book is written in a question and answer format for easy comprehension and speedy reading. Every effort has been made to organize the material as an introductory, self-study book. The chapters are short and just to the point. The answers to the various questions are also concise and rarely exceed one page. Real world examples are used wherever necessary, along with mild doses of humour. Each chapter covers only one specific area of DR and BC, and contains a set of basic and essential questions, which the author tries to explain in simple, jargon-free language.

Unless stated otherwise, the names of companies and people mentioned in the examples in this book are fictitious. But the names of actual companies and products mentioned are the trademarks of their respective organizations.

I would like to thank both Alan Calder for inviting me to write this book and Michael Bentley for his excellent editorial assistance.

**Thejendra BS**

January 2008



# CONTENTS

CHAPTER 1: Introduction to Disaster Recovery and Business Continuity .....	1
CHAPTER 2: Data Disasters .....	44
CHAPTER 3: Virus Disasters .....	65
CHAPTER 4: Communication System Disasters .....	74
CHAPTER 5: Software Disasters .....	82
CHAPTER 6: Data Centre Disasters .....	90
CHAPTER 7: IT Staff Disasters .....	96
CHAPTER 8: IT Vendor Disasters .....	108
CHAPTER 9: IT Project Failures .....	120
CHAPTER 10: Information Security .....	133
CHAPTER 11: Disaster Recovery Tools.....	141
CHAPTER 12: Introduction to Non-IT Disasters .....	145
CHAPTER 13: Disaster Recovery at Home .....	177
CHAPTER 14: Plenty of Questions.....	187
CHAPTER 15: How Do I Get Started? .....	198
APPENDIX 1: Sources of Further Information.....	244
APPENDIX 2: Disaster Recovery Training and Certification.....	248
APPENDIX 3: Business Continuity Standards.....	254
APPENDIX 4: Making DR and BC Exciting.....	258
APPENDIX 5: Disaster Recovery Glossary .....	260
APPENDIX 6: ITG resources .....	294



# **CHAPTER 1: INTRODUCTION TO DISASTER RECOVERY AND BUSINESS CONTINUITY**

'Meet success like a gentleman and disaster like a man.'

*Frederick Edwin Smith (1872-1930)*

---

The business world has changed significantly in the past few years. Organizations have undergone huge technical and non-technical transformations over the last decade. Regardless of the industry, more and more businesses are operating on a 24x7 global basis. Competition has also increased dramatically and is now available at a click of a mouse button. Even small organizations with less than a dozen employees depend on several modern technologies and worldwide competition to remain in business. To stay in business, alive and kicking, is of paramount importance to every modern organization. Today, it is not possible to run your business using the same methods and processes that were used five or ten years ago.

Secondly, the advancement and easy availability of new and useful technologies have enabled thousands of organizations worldwide to implement and use them extensively for their day-to-day functions. Today it is almost impossible to run any modern organization without the use of some computer or telecom-related technology. For example, every modern organization will require several computers, databases, Internet access, e-mail, web-hosting, telephones, etc, for running its day-to-day operations. In addition, the customers of every organization have also become heavily dependent on technology for various needs which must be serviced

## *1: Introduction to Disaster Recovery & Business Continuity*

through technology. Though organizations may have implemented several modern technologies they may or may not have the expertise to support them internally. Hence, a high dependence on external qualified vendors and service providers is also very critical. For example, if a vendor is not able to provide timely and efficient service for critical IT functions or a database, the organization can get into serious trouble.

Nobody is immune to risks, but preventing, minimizing and avoiding disasters of all kinds have become extremely important to every organization today. Less than a decade ago concepts like disaster recovery (DR) and business continuity (BC) were almost unknown or just considered as optional academic subjects. The only traditional method organizations followed for DR or BC was to sign up to some insurance for their key equipment along with a few optional covers. But protecting today's business requires going beyond having some insurance cover and keeping your fingers crossed. In addition to normal business pressures, there is an added pressure to continuously protect businesses from all kinds of threats and risks to survival.

With so much dependence on technology, an important question facing business managers today is: 'how can you handle predictable disasters striking your business?' Secondly: 'who are the best persons to protect your business?' 'And what sort of qualification and mindset does one need to work in a DR and BC department?' 'Where and how can you find or identify such persons?' And so on.

**How this book will help:** Many managers still live in constant fear about how to protect their businesses from various disasters, and worry about who will help. This book clears away such doubts and shows you how DR and BC can

## *1: Introduction to Disaster Recovery & Business Continuity*

be successfully implemented with a simple combination of qualified internal staff, vendors, external consultants and plain common sense. This simple book is aimed at small organizations and IT departments wishing to get a bird's eye view of the many DR and BC practices around. The various chapters will elaborate on a variety of IT and non-IT disasters that can strike an organization at any time. Each chapter gives short descriptions and explanations of the various terms and concepts used in DR and BC. A fictitious company called RockSolid Corp is used in many examples throughout this book. The entire book is written in a frequently asked question (FAQ) format for easy and speedy reading.

This book also draws on the best management practice contained in BS25999 to ensure that small organizations are also able to benefit from this guidance.

### **Who should read this book?**

This book is aimed at anyone who is directly or indirectly involved with disaster recovery or business continuity. If you belong to one of the groups mentioned below then you will find this book extremely useful. Though the book is aimed at small and medium organizations the concepts hold good for large organizations too.

- IT Managers
- Chief Technical Officers or Chief Information Officers
- Business managers and consultants
- Board members

## *1: Introduction to Disaster Recovery & Business Continuity*

- Risk and safety officers
- IT consultants
- Anyone who has been assigned the responsibility for overseeing DR and BC for their organizations.

### **What is a disaster?**

A general dictionary defines a disaster as an '*occurrence causing widespread destruction and distress, or a catastrophe*'. In a business environment, any event or crisis that adversely affects or disables your organization's critical business functions is a disaster. According to a number of reputable surveys and studies, hundreds of organizations worldwide go out of business every year because of the disasters that strike them, many of them fully preventable. Most small businesses cannot recover from major disasters, and even large organizations sometimes struggle.

Disasters can come in all shapes and sizes, and from all directions. This can be explained through some examples.

**Example – Natural disaster:** Suppose that, due to some mishap, there was a major fire in the RockSolid computer data centre, and all the main computers containing years' of data and required business applications get burnt down. This would automatically mean that none of the RockSolid employees would be able to do any work. The entire business could come to a standstill within hours. Recovering from such a disaster would require a huge amount of effort, time and money. In addition, there could be losses in terms of reputation, losing customers, insurance and legal hassles, etc.

**Example – Technical disaster:** Instead of a fire, suppose there was a serious technical fault, caused by a hacker intrusion, a deadly virus attack or a software bug, that resulted in all computers shutting down. This would also mean that none of the

## *1: Introduction to Disaster Recovery & Business Continuity*

RockSolid employees would be able to work and business would come to a standstill. Recovering from such a disaster would also require a huge amount of effort, time and money.

**Example – Lack of knowledge:** Organizations can also cripple themselves due to lack of adequate knowledge or by having a *penny wise, pound foolish* way of thinking.

**Finance Department:** *'Hello, techies. Our finance server is not working. Can you fix it immediately?'*

**Techie:** *'Which one?'*

**Finance Department:** *'The one that we use in our department. The black system with the green keyboard.'*

**Techie:** *'I had a look at it, but the hard disk is dead. We will have to replace it. I will call the vendor and arrange for a replacement if possible.'*

**Finance Department:** *'What about our data?'*

**Techie:** *'Can't recover. The disk is dead, and we have not been backing up the data of that server, because nobody told us to. Besides, you did not approve purchase of a tape drive for that machine. Your previous finance manager was maintaining the system herself because of confidential data.'*

**Finance Department:** *'Gasp!!! We have all our payroll, purchasing, billing, sales and other important financial data for the entire company and customers on that machine. We have just keyed in five years' data!'*

**Techie:** *'Too bad. Got to go. I have to attend another support call somewhere.'*

**Finance Department:** *'Help! Call the CFO!! Call the CEO!!! Call the Army!!!!'*

## *1: Introduction to Disaster Recovery & Business Continuity*

A situation like this can cripple a five-year-old business within an hour. And there are other types of potential disaster. Some disasters could even be deliberate – sabotage, theft, espionage, etc. Hence it is necessary to ensure that organizations have properly tested plans to recover and minimize all predictable and controllable disasters at all times. Today, having a proper and tested DR plan is also a mandatory audit and compliance requirement in many organizations. Naturally, organizations will not be able to safeguard themselves against all types of disaster, but they can definitely safeguard their business against many common types of preventable disasters.

### **What is disaster recovery?**

No modern organization can run its daily operations without computers, software, telecommunications, the Internet and so on. Disasters can cripple businesses within hours. Today's computer systems and networks are also extremely complex and complicated. In view of the complexity and inter-dependencies of various equipment, processes, people, etc, disasters can strike at any point and at any time. In today's highly competitive, 24x7 global business environment the leisurely time when a business could take days and weeks to resume operations is over. If a critical computer system is not working, or unavailable, then businesses may have to close down virtually over night. In many cases it is almost impossible to switch over to alternative manual or legacy processes for any length of time. Today, businesses must be able to resume operations quickly, almost to the exact point where they stopped when the disaster struck. Though awareness of disaster recovery is increasing everywhere, very few organizations are actually well-equipped to handle

## *1: Introduction to Disaster Recovery & Business Continuity*

disasters and restore normal operations as swiftly as possible.

Disaster recovery (DR) is the methodical preparation and execution of all the steps that will be needed to speedily recover from a disaster, usually one caused by technology. Disaster recovery planning is mainly *technology-focused*. Technology can mean voice and data communication systems, servers and computers, databases, critical data, web servers, e-mail, etc. Your DR plan should have tested and proven methods to tackle and recover from all predictable and controllable IT disasters for each of the above. For example, if there is a critical server running some crucial software, then your DR plan for that system can be a standby system in an alternative location running the identical software and having daily data synchronization. In addition, the main system can also have disk mirroring, tape backups, a periodic image backup, proper change management processes, etc, for added precautions.

A proper DR plan is of critical importance to your business. It should be documented and periodically updated with key staff, contact information, locations of backups, recovery procedures, vendor information, contracts, communications procedures, and a testing schedule. Additional elements may be necessary, depending on company size. More details are provided later in the book.

### **What is business continuity?**

Business continuity (BC) ensures that certain essential business functions can continue to operate in spite of various disasters striking your organization. BC is a process that identifies various risks that threaten your organization and

## *1: Introduction to Disaster Recovery & Business Continuity*

provides measures to safeguard the interests of its key stakeholders, customers, reputation, brand value, etc. Suppose a technical or non-technical disaster strikes your organization. Naturally all your critical staff will be deployed to try to recover from the disaster. Recovering from the disaster could range from a few minutes to several days, or never. But it is essential in many customer-oriented organizations to ensure that certain ‘minimum’ business functions ‘continue’ to operate even while the main disaster is being attended to. Unless the disaster is very severe and hits all areas, or is not under the control of your management, the entire organization need not come to a standstill.

BC is mainly *business-focused* and will concentrate on strategies and plans for various disaster events. BC planning will prepare business areas and organizations to survive serious business interruptions, and provides the ability to perform certain ‘*critical business functions*’ even during a disruptive event. For example, if a major disaster strikes a small bank’s main computer during banking hours, the bank management can speedily decide to allow customers to still deposit and withdraw a nominal amount of cash until such time as the main computer is fixed in the background. This is business continuity, and will ensure that customers have some minimal acceptable service in spite of a disaster. Having business continuity will also help preserve the company’s reputation, image, and so on.

**Note:** A business continuity solution need not always be a technical one, though there could be a technical disaster. Business continuity is all about providing speedy workable alternatives to minimize adverse impact. Anything that meets the purpose can be classified as business continuity.

## *1: Introduction to Disaster Recovery & Business Continuity*

Business continuity management is managing risks to ensure your critical *business* functions can continue to provide acceptable levels of service even in the event of a major IT or non-IT disaster. For example, if your entire data centre that houses all the important servers gets damaged in a fire, electrical short circuit or some other sudden disaster, your BC management team should assist in recovering the company from such situations in previously planned ways. Your BC management should prepare your organization for disaster recovery options that apply *before, if* and *when* a disaster occurs.

If your budgets and resources were unlimited, you could probably build a twin of your entire organization elsewhere. But such luxuries are rarely available, nor practical. The ultimate choice of which business continuity option you need for each type of disaster should be made in consultation with several departments and business managers. As stated before, your business continuity method need not always be a technical solution. Your BC management team must be able to provide cost-effective and acceptable disaster prevention solutions to each of your critical business functions.

### **What is crisis management?**

Depending on the nature of a disaster, it may be necessary for your organization to convene a group of senior managers to control adverse media reports, handle customer satisfaction, retain deserting customers, etc. This is crisis management. Crisis management is also panic prevention. For example, in the event of a major disaster in a reputable organization, suppose there was no crisis management team. Then, there could be a possibility of a newspaper publishing

## *1: Introduction to Disaster Recovery & Business Continuity*

a negative report causing adverse impacts on the business, stock price, reputation, etc. The media can often blow a simple issue out of all proportion, causing widespread panic and mayhem. Hence a crisis management function becomes important to protect your business from such situations. A crisis management team can ensure that such situations and possibilities are controlled by proactively taking measures to minimize losses of various kinds, including reputation losses.

**Figure 1: Summary and examples of concepts**

Disaster	A reputable bank's main computer's hard disk fails on Monday morning during peak banking hours. Banking operations are halted. Tellers cannot verify account balances or do any electronic transactions.
Disaster recovery (DR)	Technical staff repair the computer by replacing the hard disk and restoring data as fast as possible. Repair and restore could take several hours or more than a day.
Business continuity (BC)	Bank management allow all customers to withdraw up to one thousand dollars manually by filling in and signing a paper withdrawal slip. Other transactions also done by filling in paper forms. Paper information to be fed into the main computer later.
Crisis management (CM)	Senior executives of the bank assure customers that the technical problem will not cause any financial loss or improper accounting to anyone.

## *1: Introduction to Disaster Recovery & Business Continuity*

**Note:** Although the academic definitions and meanings of DR and BC are different, both terms are used simultaneously in many questions in this book. The reason for this is that the answers and concepts hold good for both in many cases. This book does not worry too much about the exact textbook or academic definitions of various terms. This is because, in the real world, businessmen are not unduly concerned about exact textbook definitions. They are only concerned about quick practical solutions for recovering from business disasters. The main objective of this book is to educate organizations and IT departments on practical and real-world ways of preventing various predictable disasters and continuing in business – it is not a theoretical textbook.

### **Why are DR and BC important?**

As mentioned earlier, organizations have become extremely dependent on technology for their day-to-day operations and servicing their customers. It is not possible for any modern organization to switch over to manual processes for any length of time during a business interruption. A business interruption is any event (sudden or anticipated) that can disrupt normal business at an organization's location. For example, it is not possible to switch back to manual typewriters, postal service, telex, and hand-written documents, etc, if the entire computer, Internet and e-mail network is down. Another important concern is that any major damage to the infrastructure can result in severe financial losses, loss of reputation, and may even result in closure of the business. Today most companies are interconnected among themselves, and to the outside world via the Internet. Any technology-related or other major failures in the company can result in the company being cut off from

## *1: Introduction to Disaster Recovery & Business Continuity*

the rest of the world. Some of the reasons why disaster recovery and business continuity are important for your business are listed below:

- Businesses have become extremely dependent on IT. So failures in IT are more likely to affect the business than other areas, and that impact is more likely to be severe.
- In a networked, workflow type of environment a failure can hamper many departments and units.
- IT environments have become extremely complex and inter-related, so the number of potential failure points is increasing day by day.
- When IT fails there is not enough time to recover at a leisurely pace, because of end-user, customer and other business pressures.
- Without a proven DR and BC process organizations can go out of business within hours or days.

### **Who are the real owners of DR, BC and CM?**

This is actually a tricky question. Most people would say the owners would or should be the person(s) supporting the IT equipment, or the operators handling the business functions. After all, you might argue they are the ones operating the system or know how it works. But this is an incorrect assumption. Actually, the true owners of DR, BC and CM are the business managers of your organization. Your organization may have hired some IT staff or an external vendor to provide technical support and baby-sit an important server. But, speaking from a business perspective, those IT staff, operators or external vendors are not really the owners of your DR, BC or CM for your organization. For

## *1: Introduction to Disaster Recovery & Business Continuity*

example, if the server stops operating you cannot hold the IT staff responsible for your organization being unable to conduct its business. They may know what it takes to repair or restore the system, but it is your business managers who should know or understand the potential loss in terms of financial, reputation or legal aspects of stoppage of various critical businesses and IT functions. Your business managers are responsible for ensuring provision of necessary budgets, manpower, resources, alternative methods, etc, to tackle and prevent disasters. They are the real owners of, and ultimately responsible for, DR, BC and CM. The various ways in which your business managers can demonstrate ownership are as follows:

- **Knowledge:** Understand what the loss is in terms of financial, reputation, regulatory or legal consequences for disasters related to their critical business functions or IT equipment.
- **Financial support:** Provide necessary budgets for comprehensive maintenance of hardware, software, telecom equipment, spares, backup devices, etc. For example, suppose your business managers do not approve the purchase of a good tape drive and the necessary software, or fail to enrol into hardware maintenance for an important server – the IT staff will not be able to do much in the event of a server crash, data loss or some other technical problem on that server.
- **Provide necessary manpower:** Your business managers must ensure that departments have the necessary manpower in all areas. It is very common in organizations to skimp on manpower when it comes to support, maintenance, etc, but demand the best from a slave-sized workforce. The common saying ‘Hire an Einstein, but

## *1: Introduction to Disaster Recovery & Business Continuity*

refuse his request for a blackboard’ describes a situation that is prevalent in many organizations worldwide. Reduced manpower and facilities in critical areas will inevitably, directly or indirectly, affect the business. See the question on staff ratio later.

- **Implement recommendations:** Your business managers must listen to recommendations proposed by technical staff, support staff, etc, for implementing DR and BC environments. Establishing DR and BC is an expensive business. Not every critical IT function can be worked around with a low-cost alternative. It is a common practice in many organizations to ignore or avoid IT and non-IT recommendations by giving standard excuses, like cost, even though organizations will be perfectly capable of affording it. If you are serious about DR and BC, then your senior management must support the necessary costs and budgets for implementing all sensible recommendations, industry standards and work-arounds necessary for DR and BC.
- **Get involved:** Senior management, including the CEO, must get involved in all aspects of their organization’s DR and BC processes. You must have a ‘Show me’ or ‘Prove it to me’ attitude to ensure your business is truly protected. Nowadays, having a BC or DR site for many organizations is a mandatory business and audit requirement.
- **Policies:** Just like other essential policies in HR, finance, etc, a DR and BC policy must be enforced for all critical systems by the senior management.
- **Sustained commitment:** DR and BC is a continuous exercise. Remember – DR or BC facilities are like

## *1: Introduction to Disaster Recovery & Business Continuity*

insurance and cost money constantly. It is not enough to show interest and invest some money on a one-off basis. Continuous commitment and expenditure are required to establish proper DR and BC facilities.

### **What is the cost of a disaster?**

A disaster will lead to numerous costs, implications and even long-term damage. It is not only the financial cost of the equipment or process that has failed. There can be hidden costs and problems. It can even have long-term cascading effects. Depending on the nature of the business, the various costs associated with a disaster could include:

- Business losses
- Reputation losses
- Losing customers
- Stock prices dipping or free-fall
- Employee productivity losses
- Billing losses
- Unnecessary expenditure
- Fines and penalties
- Lawsuits
- Travel and logistics expenses
- Insurance and other hassles
- Other industry-specific losses.

**Business costs:** The anticipated loss of money that the company would have made if the systems were working, eg,

## *1: Introduction to Disaster Recovery & Business Continuity*

if the company were doing its business via a website. Amazon.com, for example, could lose thousands of dollars to its competition if their website were down even for a few hours.

**Productivity costs:** Number of employees affected multiplied by their hourly cost. For example, assume that your organization had hired ten external consultants at a rate of \$100 an hour each for developing a software application installed on a particular file server. If that particular server was down for three hours during business hours then your organization would suffer a loss of \$3,000 for those three hours. This is because that amount will still need to be paid by you to those consultants without any productive work in return.

**Reputation costs:** No specific formula exists to calculate reputation costs. They can range from a minor manageable scratch to a total crash of your company's stock value and image in the eyes of customers and the general public. For example, if your company purchase order system is down, causing purchase orders to be delayed beyond committed delivery dates, your company may run a risk of losing those orders to your competitors or suffer loss of reputation due to not fulfilling orders in time, etc.

**Direct costs:** Costs for repair or replacement of the failed equipment, manpower costs, vendor costs, liabilities, etc.

**Other costs:** Other costs specific to your industry, for example, a customer may bring a lawsuit against your organization for delay.

Depending on the disaster one or more of the above losses can ruin your organization – hence the importance of paying due attention to DR and BC practices and processes. Each of

## *1: Introduction to Disaster Recovery & Business Continuity*

the above should be considered in sufficient detail and the probability of occurrence must be calculated to ensure proper business continuity alternatives. Damage must be estimated in terms of revenue, reputation, security, employees, etc. Based on the study, a detailed BC plan should be prepared and implemented to ensure resumption of business processes following a disruption. Today, having a BC plan is a mandatory business, audit and compliance requirement for many organizations. You may have to prove to regulators and your customers that your internal processes are strong enough to withstand disasters and continue servicing customers. For example, the RockSolid Corp may have to prove to its major external customers that it has adequate DR facilities and that RockSolid can provide essential services even in the event of a disaster.

### **Who are the right persons to manage DR and BC work?**

DR and BC are nowadays almost a mature science and there are umpteen numbers of consultants, templates, certifications and best practices available to everyone. If organizations need to establish DR and BC it is easily possible to get competent resumés by the hundred within hours of posting a job advertisement. In spite of such availability, the perfect candidates to manage a DR or BC function need some special skills and a very different mindset, as explained below. They need two skills that no training programme or certification can usually teach:

#### *Skill 1: Nature of a coward*

The kind of people who are perfectly suitable for DR and BC departments are those who can think like cowards, talk like cowards, plan like cowards and constantly spread a healthy

## *1: Introduction to Disaster Recovery & Business Continuity*

dose of cowardice around the organization. Every organization that is serious about risk management should nurture, promote and respect cowards in their DR and BC departments to protect their businesses from all the risks they face.

Now you may dispute why any organization needs cowards. Nobody has ever erected a statue honouring a coward. Everyone insists on the need for brave leaders everywhere, people who can make tough decisions, are flamboyant, lead and boldly take the road 'less travelled'. Nobody has ever heard of a coward doing all that. True, braveness, toughness and all those cool flamboyant leadership skills are required to run and grow a business. But if your thinking is a bit warped and out of the box, such people are not exactly suitable for protecting the business because of what they are and what they don't want to be. Let me begin my argument in favour of cowards with a couple of examples.

### **Example**

A ship's captain wanted sailors for his ship. So he called a dozen hefty-looking chaps and asked who in the group were brave and excellent swimmers. About five of them lifted their hands. To everyone's surprise, the captain selected the remaining seven as his sailors. When asked why he chose the cowards he replied, 'The chaps I selected do not know how to swim and are not very brave. So they will try the hardest to keep the ship afloat.'

Investing in cowards could be the best business decision you can take to save your business from predictable and even unpredictable disasters. A Chinese proverb says, 'Only a coward can create the best defences'. This method should be your approach to protecting your business. A brave man usually does not bother to create many defences because he is always confident that he has the power and strength to

## *1: Introduction to Disaster Recovery & Business Continuity*

withstand and tackle any danger. Also, he is incapable of seeing risks the way a coward can. But a coward knows there are always countless dangers all around that he cannot tackle. So he tries to build the best possible defences. He sees risks and dangers in practically anything that normal people cannot. Applied to your business he or she can smell and see a risk in an instant like a shark that is able to smell blood from miles away.

Cowards have a special advantage that nobody else has. They have no limits in their ability to see and cover risks. They see things that ordinary people cannot, they think in an extremely paranoid fashion. Fear controls their imagination. A coward trusts no one, not even himself. Cowards have a 'I will believe it when I see it' and 'Prove it to me' attitude. They don't believe anything they have not personally seen working to their absolute satisfaction. They can get into nit-picking detail and view risks from countless directions.

For a coward, everything is a risk. Fear helps a coward build fantastic fences. A brave leader will not hesitate to go to war. But a coward will prevent war from happening as long as possible or for ever. For example, a brash and brave manager may take a quick decision to fire an employee on flimsy grounds. But a coward will think of how this incident could affect the business, what safeguards are currently available and how the situation could take an ugly shape. A coward thinks in terms of lawsuits, or the influential contacts the employee may have, or the damage an aggrieved employee could do to the organization.

### *Skill 2: Leave no important task unfinished.*

Another important skill a DR or BC person must have is to leave no task unfinished, as shown in the following example.

## *1: Introduction to Disaster Recovery & Business Continuity*

### **Example**

A young man applied for a job as a farm-hand. When the farmer asked for his qualifications, he said, 'I can sleep when the wind blows'. This puzzled the farmer, but he liked the young man and hired him nonetheless.

A few days later, the farmer and his wife were awakened in the night by a violent storm. They quickly began to check things out to see if all was secure. They found that the shutters of the farmhouse had been securely fastened. A good supply of logs had been set next to the fireplace. And the young man slept soundly. The farmer and his wife then inspected their property. They found that the farm tools had been placed in the storage shed, safe from the elements. The tractor had been moved into the garage. The harvest was already stored inside. There was drinking water in the kitchen. The barn was properly locked. Even the animals were calm. All was well. It was only then that the farmer understood the meaning of the young man's words, 'I can sleep when the wind blows'. Since the farmhand did his work loyally and faithfully when the skies were clear, he was prepared for the storm when it broke. And when the wind blew, he was not afraid. He could sleep in peace. And, indeed, he was sleeping in peace.

Moral of the story?

There was nothing dramatic or sensational in the young farm-hand's preparations. He just faithfully did what was needed each day. The story illustrates a principle that is often overlooked about being prepared for various events that occur in life. It is only when we are facing the weather that we wish we had taken care of certain things that needed attention much earlier.

### **What is a DR or BC site?**

A 'DR site' is a disaster recovery site. A 'BC site' is a business continuity site. The terms are sometimes used interchangeably. Either way, it is usually an alternative site that can be used by the business if the primary or main site fails or becomes inaccessible. For example, assume that your

## *1: Introduction to Disaster Recovery & Business Continuity*

organization provides critical technical support on various financial applications to a key external client. Suppose there is a major IT disaster in the organization preventing your staff from providing support to that client. Then, as part of disaster recovery, certain identified support staff can immediately relocate to your DR or BC site and start providing technical support. Essential support can continue from there while the main site is being rectified. Of course, the DR or BC site must have the necessary IT infrastructure and facilities to provide the required minimum or mutually agreed level of support.

DR or BC sites can be any or all of the following, depending on organization size, importance, and so on:

- A small or fully-fledged alternative, workable office with essential technical set-up within your city.
- A small or fully-fledged alternative workable site with essential technical set-up outside the city or in a different state or even a different country.
- A branch office where essential functions can continue.
- An outsourced disaster recovery location provided by a third party service provider. Nowadays, many organizations provide generic or custom-made disaster recovery locations for other organizations for a fee.
- Certain activities can also be done from home if remote connectivity options are available.

### **What is a command centre?**

A command centre is a facility with adequate phone lines and other basic facilities to begin recovery operations.