Disaster Recovery and Business Continuity

A quick guide for organisations and business managers

Thejendra B.S

Third edition

itgp™

Disaster Recovery and Business Continuity

A quick guide for organisations and business managers

Third edition

Disaster Recovery and Business Continuity

A quick guide for organisations and business managers

Third edition

THEJENDRA B.S

IT Governance Publishing

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 publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. 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.

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

www.itgovernance.co.uk

First published in the United Kingdom in 2007 by IT Governance Publishing: 978-1-905356-14-0.

Second edition published in 2008: 978-1-905356-37-9.

Third edition published in 2014
ISBN: 978-1-84928-538-4

ABOUT THE AUTHOR

Thejendra B.S is an Information Technology (IT) manager for a software development firm in Bangalore, India. He has also worked in other countries, such as, Saudi Arabia, Dubai, Bahrain, Qatar, Singapore, and Australia.

His introduction to IT began over 20 years ago, when after gaining a degree in electronics he took on the role of field manager. Since then he has developed a wealth of experience and knowledge of IT, and is familiar with a wide range of roles including IT support, help desk, asset management and IT security.

Thejendra is experienced in the areas of disaster recovery (DR) and business continuity (BC). He has dealt with many organisations – of all sizes and nature of business – around the world and has implemented numerous small to large IT projects worth millions of pounds.

Visit his website *www.thejendra.com* for details on his other books and articles. He can be contacted on *thejendra@yahoo.com* or *thejendrabs@gmail.com*.

FOREWORD

The increasing dependence of organisations on IT systems and the growing range of threats they face, from an act of nature to a terrorist attack, means that organisations that are unprepared for the worst will not usually survive the unexpected. Therefore, over the last ten years disaster recovery and business continuity have become critical business issues.

Business continuity is one of the most important areas of operational risk. This was recognised by the regulatory authorities in the Basel Accord, legislation from the UK's Companies Act 2006 and the US Sarbanes-Oxley Act, which all require an organisation's directors to take appropriate action to identify and deal with operational risk. A significant development for companies that wish to identify and apply best management practice in mitigating this risk was the emergence of the British Standard BS25999, which was the world's first formal Standard for Business Continuity Management (BCM). It contained both the code of practice and specification for a management system against which an organisation can achieve third party accredited certification. BS25999 was replaced by ISO/IEC 22301 in 2012, which enables organisations to demonstrate to their customers and partners their planned business resilience, and those that have such a certificate will inevitably gain a competitive advantage over those that don't.

In the US, ISO/IEC 22301 feeds into the voluntary private sector preparedness (PS-Prep) accreditation and certification scheme, which is a nationally recognised programme to develop excellence in disaster recovery and business continuity planning.

For smaller organisations, this book is a welcome guide to all the key aspects of disaster recovery and business continuity.

Alan Calder

Founder and Executive Chairman
IT Governance Ltd.

PREFACE

DR and BC are often considered to be a costly, complex and over complicated task that can only be handled by specialists. Executives and managers of small or medium-sized organisations and IT departments often live with the misconception that such activities are beyond their expertise or affordability, and are perhaps considered to be optional academic subjects that are only applicable to larger organisations. Consequently, many of those who are responsible for continuing with business as usual (BAU) may live with the constant fear and the never-ending question of how to protect their business in the event of a disaster, and who would help if such a disaster should occur. This book simplifies the procedures and processes used to successfully implement a workable DR and BC plan. It removes any doubts or uncertainties about how it can be easily achieved with the help of a simple combination of qualified internal members of staff, contractors, external consultants and some common sense.

It provides a short description and explanation of the various DR and BC terms and concepts used. The book draws on the best management practice contained in ISO22301, the latest Standard, to ensure that organisations of any size are able to benefit from its guidance.

Some chapters provide examples of IT and non-IT disasters that could strike an organisation at any time, and may be elaborated on with the use of a fictitious organisation called RockSolid Corp.

Unless stated otherwise, the names of any companies or people mentioned in any examples are fictitious. Where names of actual companies and products are mentioned, they are the trademarks of their respective organisations.

Thejendra B.S

January 2014

CONTENTS

CHAPTER 1: INTRODUCTION TO DISASTER RECOVERY AND BUSINESS CONTINUITY

‘Meet success like a gentleman and disaster like a man.’

Frederick Edwin Smith (1872-1930)

During the last decade, organisations have undergone huge technical and non-technical transformations, and in the last few years the business world has changed significantly. Regardless of the industry, more and more organisations around the world are operating 7 days a week, 24 hours a day. Competition has increased dramatically, and multiple options for a customer’s demand are available at the click of a mouse. Even a small organisation with only a few staff members depends on technology to compete globally in order to remain in business, which is of paramount importance to every organisation. It’s almost impossible to run any organisation without the use of a computer or telecom-related technology, and this can’t be achieved using the same methods and processes that were used five or ten years ago. For example, any organisation today will require computers, databases, internet access, e-mail, web-hosting and telephones for running its business. Furthermore, the advancement in new technology and its ready availability has enabled an organisation to implement and use it to great effect just to continue with business as usual.

Although an organisation may have implemented modern technologies, they may, or may not have the expertise to support them internally. As a result, there is a high dependence on external, qualified contractors and service providers that can provide timely and efficient service for various mission critical IT functions of an organisation.

Today, because of the numerous technical interdependencies that have become a necessity in all areas of business, no organisation is immune to risk. Therefore, preventing, minimising and avoiding the risk of all types of unexpected disaster or threat has become particularly important. Traditional methods of protection may have been by means of an insurance policy. This would provide cover and protection against damage to key equipment, for example, in the event of a fire or flood, or any other event which the policyholder may have opted for. However, today's business needs and requirements demand more than this, or simply '*hoping for the best'*. An organisation has to protect itself from the ever increasing number of physical and virtual threats and risks.

With so much dependence on technology, those responsible are constantly faced with the same questions, such as:

- How can one manage predictable disasters striking an organisation?
- Who is best qualified to protect an organisation?
- What qualifications and mindset does one need to work in a DR and BC department?
- Where and how can one find or identify such people?

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 organisations the concepts hold good for large organisations too.

- IT managers
- Chief technical officers or chief information officers
- Business managers and consultants
- Board members
- Risk and safety officers
- IT consultants
- Anyone who has been assigned the responsibility for overseeing DR and BC for their organisation.

What is a disaster?

A disaster is generally considered to be '*an occurrence causing widespread destruction and distress, or a catastrophe*'. In a business environment, any event or crisis that adversely affects or disables an organisation's ability to continue with business as usual is a disaster.

According to various surveys and studies conducted by agencies like DRJ (Disaster Recovery Journal) and Forrester Research, many organisations worldwide go out of business every year because of a disaster - many of which were fully preventable. Many small organisations are often unable to recover from a major disaster, and even larger organisations may find it difficult. As a result, it is vital that organisations constantly minimise all predictable and controllable risks and ensure that they have a properly tested disaster recovery plan in place, should an event occur. A disaster recovery plan is now a mandatory audit and compliance requirement in many organisations. Naturally, organisations won’t be able to safeguard themselves against all types of disasters, but they can definitely prevent and safeguard their business against many of the more common types.

Disasters can occur in a variety of forms, as demonstrated by the following examples. As mentioned earlier, a fictitious company called RockSolid Corp is used in many examples throughout this book.

Example 1 – Natural disaster

Due to a mishap, there was a serious fire in RockSolid’s computer data centre and all of the mission critical computers that contained years of business data, together with any required business applications, were destroyed. This would automatically mean that most of the organisation’s members of staff would be unable to continue with their work, and within a small amount of time the whole organisation could come to a standstill, because it is unable to continue with ‘business as usual’. For an organisation to recover from such a disaster, it would require a huge amount of time, cost and effort. However, although some losses may be measurable, other losses also have to be considered, which perhaps may not be so easily measured, for example, damage to an organisation’s reputation.

Example 2 – Technical disaster

A hacker intrusion into an organisation's computers can result in a serious technical fault, such as a deadly virus attack or a software bug that causes all of its computers to shut down.

Example 3 – Lack of knowledge

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

Help desk: 'Which one?'

Finance Department: 'The one that we use in our department. It's a black system with a green keyboard.'

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

Finance Department: 'What about our data?'

Help desk: 'I'm afraid we can't recover the data. The disk is dead and we have not been backing up the data of that server, because nobody told us to. Finance did not approve the purchase of a tape drive for this machine.'

Finance Department: 'Oh no. We have our entire payroll, purchasing, billing, sales and other important financial data for the entire company on that machine. Five years of data!'

Help desk: 'Unfortunately there is nothing we can do. Please excuse me, I have to go and attend another call.'

A situation like that can cripple your organisation within hours.

To summarise, in no time at all, an organisation can inflict serious damage to its business simply through lack of adequate knowledge, or by having a '*penny wise, pound foolish'* way of thinking.

And there are other types of potential disaster. Some disasters could even be deliberate, such as, sabotage, theft, or espionage.

What is disaster recovery (DR)?

Computer systems and networks are extremely complex and complicated, and in view of this and the inter-dependencies of various equipment, processes and people, etc., a disaster can strike anywhere at any time. The current business environment is highly competitive, and the days when an organisation could resume business as usual at its leisure; that is, within a few days or weeks, are over.

If a mission critical computer system is not working, or unavailable, then in no time at all an organisation may be unable to continue with its business as usual. Therefore, it must be able to quickly resume its mission critical business functions from almost the exact point in time that the disaster struck, because it's almost impossible to switch over to an alternative manual or legacy process for any length of time. Although global awareness of DR and BC is increasing, very few organisations are well enough equipped and prepared to respond to a disaster and quickly continue with its business as usual functions.

DR is the methodical planning, preparation and execution of all the steps in the process that will be needed to recover from a disaster quickly. It is mainly *technology-focused*, for example, voice and data communication systems, servers and computers, databases, critical data, web servers and e-mail. A DR plan should have tested and proven methods to tackle and recover from all predictable and controllable IT disasters for each of the pre-mentioned examples and more. If there is a mission critical server running critical software, then a DR plan for the server could be a 'standby' that's located elsewhere and running the identical software with daily data synchronization. In addition, the main system can also have disk mirroring, tape back-ups, a periodic image back-up and proper change management processes, for added precautions.

Well implemented DR is of critical importance to an organisation. It should be documented and periodically updated with details of the contact information for key members of staff, the locations of back-ups, recovery procedures, vendor and contractor information, contracts, communications procedures, and a testing schedule. Additional elements may be necessary depending on the size of an organisation. Further information can be found on this in *Chapter 15*.

What is business continuity (BC)?

BC ensures that an organisation's mission critical business functions can continue to operate regardless of a disaster striking. It is a process that identifies various risks or threats to an organisation, and provides responsive measures to safeguard the interests of its key stakeholders, customers, reputation, brand value, etc. Should a disaster strike, the natural approach would be to deploy all critical members of staff to concentrate their effort on making a recovery; which may be done within a matter of minutes, hours or days - or not at all. However, in many customer focused organisations; in parallel to responding to a disaster, it's also essential to ensure that certain '*minimum*' business functions '*continue*' to operate regardless. BC is mainly *business-focused* and will concentrate on strategies and plans in the event of a disaster. It will prepare organisations and their business areas to survive serious business interruptions, and provide the ability to perform certain mission critical business functions - even during a disruptive event. For example, if a major disaster strikes the main mission critical computer system of a bank during banking hours, a quick decision can be made to continue with business as usual. This could be by allowing customers to continue depositing and withdrawing a nominal amount of cash until the problem is fixed. This is BC. It ensures that customers have a minimal acceptable service in spite of a disaster, and also helps preserve the bank's reputation and image etc.

Note: A BC solution need not always require a technical solution for a technical disaster. It's about providing quick workable alternatives to minimise adverse impact. Anything that meets the purpose can be classified as BC. Business continuity management (BCM) is managing risks to ensure that mission critical functions continue to provide an acceptable level of service, even in the event of a major IT or non-IT disaster. If, for example, the entire data centre that housed all of the important servers was damaged by a fire, electrical short circuit, or some other unexpected disaster, the BCM team should be able to assist in recovering the organisation from such situations using pre-planned methods - BC planning (BCP). It should prepare an organisation for DR actions that apply before, if, or when a disaster occurs.

If budgets and resources were unlimited, it’s probable that an entire organisation could be duplicated elsewhere. However, such luxury is rarely available, nor practical. The final decision of the appropriate BC action that should be implemented in response to each type of disaster should be made in consultation with a number of departments and business managers. As previously stated, a BC method need not always require a technical solution. The BCM team must be able to provide cost-effective and acceptable disaster prevention solutions to each mission critical business function.

What is Crisis Management?

Depending on the nature of a disaster, it may be necessary for an organisation to convene a group of senior managers to, for example, control adverse media reports, manage customer satisfaction, or retain deserting customers. This is crisis management. It is also panic prevention, and its function becomes important to protect an organisation from a disaster such as negative and exaggerated media reports, that may cause widespread panic and have an adverse impact on it, for example, its stock price, or reputation. In the event of a major disaster, a crisis management team can ensure that such situations and possibilities are controlled by taking proactive action to minimise the impact, and therefore its losses.

Table 1: Summary and examples of concepts

Disaster	A bank's mission critical computer fails during peak banking hours. Critical business functions are halted - cashiers are unable to verify account balances, or conduct electronic transactions.
Disaster Recovery (DR)	Members of IT can repair the computer by replacing the hard disk and restoring data as fast as possible. However, this could take several hours or more than a day.
Business Continuity (BC)	Bank management decide to allow customers to make transactions manually, using 'withdrawal' and 'paying-in' slips.
Crisis management (CM)	Senior executives of the bank assure customers that the technical problem won't cause any financial loss or improper accounting to anyone.

Note: Although the academic definitions and meanings of DR and BC are different, this book uses both terms in parallel, so the answers and concepts hold good for both in many cases.

Why are DR and BC important?

Many organisations have become extremely dependent on technology for their business as usual operations, and to provide a service to their customers. An important concern is that any major damage to an organisation's infrastructure can result in severe financial losses, loss of reputation, and may even result in its closure. This is because it can be extremely difficult and complex for an organisation to switch over to manual processes for any length of time during a business interruption. For example, it isn't possible to revert to manual typewriters, telex and hand-written documents if the whole computer system, Internet and e-mail network is down. Many are also internally and externally inter-connected via the Internet, hence any technology-related failures external to the organisation can result in it being globally isolated. Some of the reasons why DR and BC are important for an organisation are as follows:

- Organisations have become extremely dependent on IT. As a result, IT failures are more likely to affect an organisation than failures in other areas, of its business, and the impact of such a failure is more likely to be severe.
- In a networked, workflow type of environment, a failure can affect many departments and units.
- IT environments have become extremely complex and inter-related, so the number of potential failure points is increasing all the time.
- In the event of an IT failure, there isn't enough time to recover 'at one's leisure', because of end-user, customer and other business pressures.
- Without a proven DR and BC process an organisation could go out of business very quickly.

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

This is actually a tricky question. An organisation may have employed its own members of IT staff, or external contractors to provide technical support and operate a critical server. Many would assume the real owners are the staff supporting the IT equipment, or the operators handling the business functions, because they operate the system, and as such, understand how it works. However, this is an incorrect assumption. The real owners are the organisation's business managers, because if the main server stops operating, the members of IT staff can't be held responsible for the organisation failing to continue with business as usual. They may know what it takes to repair or restore the system, but it's the business managers who should know and understand the big picture, such as the impact that the potential loss of any mission critical business and IT functions can have on the organisation, that is, in terms of financial, reputational and legalities. Hence, the business managers are the real owners of DR, BC and CM, and as such, are responsible for ensuring that the necessary budgets, manpower, resources and alternative methods are in place to tackle and prevent a disaster. Some of the ways in which an organisation's business managers can demonstrate ownership are as follows:

- **Knowledge:** Understand the financial, reputational, regulatory or legal impact that a disaster can have on an organisation's mission critical business function, or IT equipment.

- **Financial support:** Provide the necessary budgets for comprehensive maintenance, such as, hardware, software, telecom equipment, spares, and back-up devices. For example, if an organisation's business manager declines to approve the purchase of equipment or necessary software that is of an acceptable standard of quality, or fail to enter into a hardware maintenance contract agreement for an important server, then members of IT staff won't be able to take the relevant appropriate action in the event of a server crash, data loss or other technical problem that may occur.

- **Manpower:** Ensure that departments have the necessary resources in all areas. It is common for an organisation to have insufficient manpower to provide support and maintenance, but nevertheless demand the best from an under-resourced workforce. The common saying '*Hire an Einstein, but refuse his request for a blackboard*' describes a situation that is prevalent in many organisations worldwide. Reduced manpower and facilities in critical areas will inevitably, directly or indirectly, affect the organisation. (Member of staff ratios will be covered in more detail later in the book).

- **Implement recommendations:** Establishing DR and BC is an expensive business. Listen to recommendations proposed by members of IT and support staff for implementing DR and BC environments. Not every critical IT function can be worked around with a low-cost alternative. It is common practice in many organisations to ignore, or avoid IT and non-IT recommendations - using cost as an excuse. If an organisation is serious about implementing DR and BC, then senior management must provide support in terms of the necessary costs and budgets for implementing all sensible recommendations, industry standards and workarounds necessary, even though a disaster may never strike.

- **Be involved:** Senior management at all levels must get involved in all aspects of an organisation's DR and BC processes, and adopt a '*Show me*' or '*Prove it to me*' attitude to ensure its business is truly protected. It is a mandatory business and audit requirement for many organisations to have a BC or DR site, which is an alternative site that can be used if the primary or main site fails or becomes inaccessible.

- **Policies:** As with other essential policies, such as, in human resources (HR), or finance, a DR and BC policy must be enforced for all critical systems by senior management.

- **Sustained commitment:** DR and BC is a continuous exercise, and it's worth remembering that its facilities are similar to insurance, that is, they are a constant expense. It isn't enough to show an interest and invest on a one-off basis, because establishing proper DR and BC facilities requires continuous commitment and expenditure.

What is the cost of a disaster?

A disaster can lead to substantial costs, implications and long-term damage; not only in terms of the financial cost, such as the equipment or process that's failed, but possibly many other hidden costs and issues. It can even have long-term cascading affects, and depending on the nature of the organisation's business the various costs associated with a disaster could include the following:

- loss of business

- loss of reputation

- loss of customers
- stock prices falling or free-fall
- reduced staff productivity
- billing costs
- unnecessary expenditure
- fines and penalties - regulatory
- lawsuits
- travel and logistics expenses
- insurance and other associated miscellaneous costs
- other industry-specific losses.

Business costs: This is the anticipated loss of money that an organisation would have lost if its systems weren't working. For example, if its business is operated via a website, such as Amazon.com, it could lose thousands of pounds an hour in revenue to its competition for each hour that its website was down.

Productivity costs: This is calculated using the number of affected members of staff, and multiplying this by their hourly cost. For example, if an organisation hired ten external consultants at £100 an hour to develop software on a server, and that server was down for three hours, it would incur a loss of £3,000. This is because the amount will still have to be paid to the consultants without any productive work in return.

Reputation costs: No specific formula exists to calculate the costs of an organisation's reputation. It can range from a minor manageable scratch, to a total crash of its share value and image to customers and the general public. For example, if an organisation's purchase order system is down, resulting in a delay of orders beyond committed delivery dates, it runs the risk of losing those orders to its competitors, or suffers reputational damage due to not fulfilling them in time.

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

Other costs: Costs specific to an organisation, for example, as a result of a customer taking legal action for a delay.

Depending on the disaster, one or more of the above losses could ruin an organisation, demonstrating the importance of paying due attention to DR and BC practices and processes. Each of the above costs should be considered in sufficient detail, and the probability of an occurrence must be calculated to ensure proper BC alternatives. Any damage must be estimated in terms of, for example, revenue, reputation, security and members of staff. Based on this calculation, a detailed BC plan should be prepared and implemented to ensure that its business activities can resume following a disruption.

Who are the right persons to manage DR and BC?

An organisation's business managers may argue that DR and BC are now almost a mature science, with numerous consultants, templates, certifications and best practices available to everyone. If an organisation has a requirement to set-up DR and BC, there are many suitably qualified and competent professionals available to carry out the role. However, the ideal candidates to manage a DR and/or BC function will still need some special skills that training programmes or certification are usually unable to teach - and they need to be of a very different mindset.

Skill 1: Nature of a pessimist

The most suitable person to carry out the role in an organisation’s DR and BC department is one who is able to think, speak and plan as a pessimist, and constantly spreads a healthy dose of pessimism. Every organisation that’s serious about risk management should nurture, promote and respect such an individual in order to protect its business from any risks they may face.

It’s easy to dispute why an organisation should have a requirement for a pessimist, and it’s unlikely that a statue has ever been erected in honour of one. Most people insist on the need for brave leaders, such as those who are able to make tough decisions, are flamboyant and able to lead and boldly take the less travelled road. This wouldn’t be expected of a pessimist. Braveness, toughness and other leadership skills are required to run and grow an organisation, but those whose thinking is ‘out of the box’ are often not suitable for protecting it, because of what they are, and what they don’t want to be.

Investing in a pessimist could be the best business decision taken to save an organisation from a disaster. A Chinese proverb says, ‘*Only a coward can create the best defences*’. This method should be an approach to protecting an organisation. A brave person doesn’t usually make the effort to create many defences, because of the self-belief and confidence of having the power and strength to withstand and tackle any danger. However, this person is incapable of seeing risks in the same way that a pessimist is able to, or of demonstrating the ability to identify the numerous risks and dangers that exist in practically anything. A pessimist is constantly aware of the numerous dangers that exist and cannot be tackled and therefore, responds by building the best possible defences. This can benefit an organisation, because this person is able to smell and see a risk in an instant, just as a shark is able to smell blood from miles away.

Pessimists have a unique and special advantage by having no limits in their ability to identify risks and things that an ordinary person can't. Pessimists think in an extremely paranoid fashion and fear controls their imagination. They trust no one, not even themselves, and have an '*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, and can get into nit-picking detail by viewing risks in numerous ways.

For a pessimist, everything is a risk. Fear helps a pessimist build fantastic fences. A brave leader will not hesitate to go to war, but a pessimist will prevent war from happening as long as possible, or forever. In an organisation, a brash and brave manager may take a quick decision to lay-off a critical member of staff over a trivial matter, whereas, a pessimist may think of how the incident could affect the organisation, what safeguards are currently available, and how the situation could worsen. A pessimist thinks in terms of possible lawsuits, any influential contacts the member of staff may have, or the damage that the aggrieved person could inflict on the organisation.

Skill 2: Leave no important task unfinished

Another important skill a DR or BC professional must have is to leave no task unfinished as explained in a popular farm hand story.

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?

The terms DR and BC site are sometimes used interchangeably. Either way, it is usually an alternative site that can be used by an organisation if the primary or main site fails, or becomes inaccessible. For example, if an organisation is struck by a major IT disaster that prevents its members of staff from providing critical technical support on various financial applications to a key external client. In response to DR, certain support staff can immediately relocate to the DR or BC site, start providing technical support and continue to do so while the main site is being fixed. The site must of course have the necessary IT infrastructure and facilities to provide the required minimum, or mutually agreed level of support.

Depending on the size of an organisation or its importance, a DR or BC site can be any or all of the following:

- A small or fully-fledged alternative workable office with essential technical set-up in the same location.
- A small or fully-fledged alternative workable site with essential technical set-up at a different location, that is in a different state, or even a different country.
- A branch office where essential functions can continue.
- An outsourced location provided by a third party service provider. Many organisations provide generic or custom-made locations for other organisations for a fee.

- Certain activities can also be carried out from home if remote connectivity options are available.

What is a command centre?

A command centre is a facility with an adequate means of communication, for example, telephones, internet availability and other basic facilities required to begin recovery operations. Typically, it is a temporary facility used by senior management, or those tasked to begin coordinating the recovery process until the alternative sites are functional.

Where should a DR or BC site be located?

Several factors need to be considered when establishing where a DR or BC site should be located, It depends on the nature of the organisation's business and its dependent items, for example, its contractor services, communication links and material availabilities. Also, consideration should be given to any political, geographical, natural, human or any other risks which may be associated with its location. For example, a software development organisation that is heavily dependent on international telecom links should not have its site located in a remote area where telecom contractors are unable to provide data and voice links. On the contrary, a small manufacturing organisation, for example, could probably have its site fitted with some essential equipment, located anywhere that has an electrical supply and transport facilities. Basic communication can be done using mobile phones or laptops connected with wireless internet.

From a logistics perspective, if essential services are to continue quickly, it is sensible to have an alternative DR or

BC site located reasonably near the main site to avoid long travel times and associated logistics problems. Travelling time is a key factor to consider when deciding on the location of a site. Other factors to consider are as follows:

- Data transfer requirements between both sites.
- Periodicity and amount of data.
- Ease of travel between both sites.
- Availability of support services, for example telecom contractors, computer contractors and spare parts.
- Availability of essential facilities, such as power and water. It is also preferable to have the site powered by a different electrical power grid to that of the main site.
- Political and civil issues at the location. For example, it does not make sense to set up the site at a location that may suffer periodic civil and political disturbances.
- Some organisations prefer to locate their sites in other countries. For example, many software development companies in India have a site in Singapore which operates in parallel, synchronizing its data. Therefore, if a disaster was to strike the main site in India, a core essential team in Singapore can continue with business as usual and keep their data intact.

Establishing and maintaining a ready-to-use DR or BC site can be an expensive business. Fortunately the need to use it may never occur, but as with an insurance policy, one can never predict when it will be necessary.

Can an organisation manage DR and BC alone?

DR and BC is not rocket science. In fact, it is common sense to ensure that an organisation does not suffer as a result of factors that are within its control. However, its planning must be developed with the effort of several departments. Although an individual in a small organisation may oversee it, it's not an individual effort. The person best suited to carry out the role of a DR or BC manager is one that is paranoid and worries about anything and everything, but is still able to communicate. Before developing a plan, every organisation must classify its functions in terms of priorities and impacts. Business and technical managers must analyse the business together, and rank it in terms of priorities and business impact. For example, an organisation may classify all of its business functions as low, medium and high priorities, with a business impact for each. Obviously, not everything carried out by an organisation can be classified as high priority or high impact.

Questions to support classification could include:

- What business functions must be up and running within minutes or hours in the event of a disaster striking? For example, an organisation that is highly dependent on e-mail for its business cannot afford to have its server down. Therefore, it may classify e-mail as high priority, thereby taking all necessary steps to have an alternative e-mail system in place. Whereas, an organisation that depends heavily on a web server may classify all its web systems as high priority.

- What business functions can be down for 24 hours? An organisation that depends occasionally on facsimiles may classify its facsimile services as medium priority, because it can tolerate a day's downtime.

- What business functions can be down for more than 24 hours, more than two days, or a week? Certain software development projects and product development that are still in the design or development stage may be able to tolerate a few days or weeks of downtime and as a result classify it as a low priority.

Successful running of a DR or BC site may also depend on other factors. If an organisation has several experienced members of staff who are familiar with the details of all of the business processes, that is, how they work and their importance, then it is possible for them to develop fairly good DR or BC planning. Alternatives are the use of external consultants, or the use of standard templates. Templates are detailed prepared checklists that compare an organisation's preparation. For example, a fire department may provide a template or checklist that provides details of checks for fire prevention. It is also possible to have a building inspected by a fire department to certify whether it's safe or not. Similarly, a back-up software manufacturer can provide a checklist of the important things to take into account both during, and after a backup of data.

Important tip: Anything within an organisation's control must get the necessary priority, budgets and importance. The following checklist can be used:

- What areas and business functions are *completely* within an organisation's control? Computers, data and back-ups are usually within an organisation's control for recovery. Any loss here can be handled by the organisation by implementing various safeguards and budgets, using its own manpower and resources.

- What areas and business functions are *partially* within an organisation's control? There could be some dependence on an external service provider, such as a telephone network that is provided by a telecommunication organisation. It cannot have its own independent telephone network that is separate from the external world — it's dependent on local and international telecommunication service providers. Problems and loss of service by the service provider can affect an organisation's business, but will not be within its control. However, if it is unable to use landlines, perhaps mobile phones can be used temporarily until the telecom department fixes the fault.

- What areas and business functions are *outside* of the organisation's control? For example, if an office is located in close vicinity of an oil or gas terminal, and a fire occurs within those facilities, it can affect the organisation's buildings and any others nearby. Or, in the event of a terrorist attack, the police may cordon off the whole area, thus prevent members of staff from travelling to and from the workplace. Senior management will have no say or control in such matters, but will simply have to cooperate regardless of the loss of business. In such an event, an organisation may have to resort to an insurance claim, an alternative site, delays, etc.

What about DR and BC assistance from external consultants?

Nowadays, DR consultancy itself is a big business, and many consultants and consultancy firms have sprung up all over the world claiming to be the best of them all. It's also industry-specific. However, it isn't possible to get a single, good DR consultancy that covers the entire range of business and technical processes; even though they may all claim to be experts in every area. It is necessary to evaluate the need for inviting external consultants, and then decide the way forward. In most cases, a combination of internal and external expertise would be appropriate.

The best consultants to start the process could already be within an organisation. An experienced professional knowledgeable of the requirements in the event of a disaster striking their area of work, together with a combination of internal experienced members of staff, and external consultants would be a good choice. An organisation must select DR consultants carefully, and avoid those who only give superficial advice. However, it may not be easy to pin-point a single consultant for all business needs, but to make a choice based on the area of DR coverage. Credentials and references play an important role in selection, for example, hire a reputable, or experienced IT person to recommend IT DR methods and a reputable financial consultant to provide financial DR methods.

Ideally, a DR or BC consultant must be a '*nuts and bolts*' person, that is, someone who can sit with key members of staff to understand the needs and requirements, so as to recommend practical real-world solutions. If an organisation requires a DR facility for its financial systems, the consultant should sit with the finance team and gain an understanding of how the system works, together with the software, type of equipment and data synchronization that's required. This should be undertaken before recommending a suitable DR setup, and the consultant must be able to demonstrate its working with a mock run.

The importance of practical experience: Sir Francis Bacon said long ago, '*Knowledge is power*'. Perhaps this can be modified for today's world as '*Practical knowledge is power*'. Although professional certifications are becoming very important in any role, practical and real-world knowledge is of paramount importance. It is also important to '*first learn the trade before experimenting with tricks of the trade*'. Practical, hands-on experience and implementation ability are the keys to good DR consultancy.

What kinds of disaster should an organisation be aware of?

Disasters can come in all shapes and forms and be internal or external. Therefore, different factors need to be considered for each critical system. All of an organisation's processes and systems should be classified into broad categories and tackled one at a time. The DR or BC selection process starts with an assessment of the potential risks and their probability and impact for a particular enterprise. Next is a business impact analysis (BIA). This helps to determine which applications and systems require the most protection. This is based on the value of the data and the business impact of downtime, as well as other cost factors. Some of the common types of risks are,

- **Technical risks:** This will cover all IT-related issues, such as, including back-ups, data storage and retrieval, loss of equipment, communication failures, virus attacks, software problems and power failures.

- **Non-technical risks:** Building security, theft, fire hazards and access by unauthorised personnel.
- **Financial and legal risks:** Stock market manipulation, bankruptcy, fraud, financial irregularities, failure to comply with legal regulations or standards.
- **Human risks:** Loss of important members of key staff to competitors, or resignations, death, injury, illness, disgruntlement, workplace harassment and industrial espionage.
- **Reputational risks:** All factors that can affect an organisation's image, for example, harassment of members of staff, litigation, legal turmoil and bad publicity.
- **Dependency risks:** If an organisation depends on external companies, contractors and even other countries for its business, it could be at risk. For example, a restaurant that is dependent on the existence of a large organisation nearby may go out of business if that organisation relocates.
- **Natural risks:** Fire, flood, earthquake and hurricane.
- **Political risks:** Change of government and policies, civil disturbances and terrorism.

An organisation can broadly classify risks with their probability of occurrence and impact, as follows:

Table 2: Simple risk analysis

RISK	PROBABILITY	IMPACT
Technical	High	High
Political	Low	High
Financial	Medium	High
Fire	High	High

Note: DR and BC is an ongoing process. It can *never* be perfect or complete.

What is a technical risk?

An organisation will use one or more of the following IT systems:

- Computers of various sizes and capacities ranging from small laptops to large mainframes.
- Data back-up systems to store and retrieve large amounts of data.
- E-mail systems for internal and external communication.
- Telecommunication systems, for example, facsimile, dial-up lines, mobile phones, leased lines for connecting offices, branches between different geographical locations.
- Various software programmes, for example, office suites, databases, remote connectivity tools, monitoring tools, design software and e-mail.

- Website servers for hosting intranets and public servers.

… and potentially dozens of other enterprise technologies.

Each of the above must be interconnected if an organisation is to function, but each has the potential to fail in a number of areas. A simple cable disconnection on an international data leased line can cut off every part of an entire organisation. Heavy usage of any such equipment always entails a hidden risk. Similarly, any item of equipment can fail in its own unique way, or behave erratically for various reasons. For example, if the power supply fluctuates there is a high probability of computer disks crashing, or corruption of data on many computers. All such IT-related failures, or potential failures can be classified as technical risks, and sufficient workable cost-effective alternatives are needed to minimise risk.

What are some of the most common technical risks?

Some of the most common technical risks to an organisation are listed below, and will be covered in more detail in later chapters. Risks that can range from simple problems to absolute catastrophes are as follows:

- Risk to data
- Virus risks
- Power failure risks
- Local area network (LAN) failures
- Information security risks
- Telecommunication risks.

What are some of the most common non-technical disasters?

Some of the most common non-technical disasters and risks that an organisation may face are as follows:

- Members of IT staff
- IT contractors
- Reputation
- Financial
- Labour union
- Legal
- Political
- Natural
- Terrorist.

Most of these will be covered in a separate chapter on non-IT disasters – *see Chapter 12.*

What is a business impact analysis (BIA)?

This is a detailed analysis of the impact on an organisation if a specific set of IT or non-IT services aren't available. Its purpose is to determine the risks, for example, in terms of loss of revenue, reputation or productivity if an IT infrastructure or other mission critical facility is down due to a disaster. A BIA will consider the impact of the following:

- Damage to premises or data centre.

- Damage to IT systems, such as servers, computers, networks or telecommunications.
- Damage to important data in terms of loss or corruption.
- Loss of key members of staff, such as IT support or business managers.
- External and internal customers if a disaster occurred.
- Legal and reputational implications if a disaster occurred.
- Dependencies on external contractors and suppliers.
- Security threats, for example viruses and hackers who may steal confidential information.
- Damage and loss of power, air conditioners, etc., required for IT services.
- Damage due to, for example, sabotage, natural disasters and political threats.
- Other industry-specific impacts.

An example, of a very basic BIA could be as follows:

Table 3: Simple business impact analysis

System	**Probability**	**Impact of downtime**
Organisation web server down	High	£5,000 in lost business per hour
Organisation local	Medium	Productivity loss of

network down		£50 per hour, per member of staff

Organisations could prepare similar tables to decide which critical business functions require priority in a business continuity plan (BCP).

Who can invoke BC?

As part of a BCP an organisation must first decide what qualifies as a disaster. Any routine equipment problem, maintenance downtime and short-term problem should not be termed as a disaster, thus invoking alternative facilities. The decision to brand an IT shutdown as a disaster must be taken only by the organisation’s senior management and IT managers. A business recovery team can also be constituted: this is a group of qualified senior members of staff responsible for maintaining the business recovery procedures, and for coordinating the recovery of the organisation’s critical business functions. For example, if an entire IT infrastructure is out of action as a result of power failure, but the failure is expected to be rectified within a short period of time, then the organisation need not classify it as a disaster, thereby invoking its DR or BC plan. On the other hand, if it is ascertained that the power failure is more severe, and can’t be restored within a timescale that is deemed acceptable, then the senior management may invoke the DR procedures.

The following types of disaster can necessitate invoking BC beyond the agreed recovery time objective (RTO) and recovery point objective (RPO) (explained in *Chapter 2*):

- Severe or major business impact to an organisation
- Adverse customer impact

- High risk exposure to organisation
- Critical system down.

What are the options available for BC?

Technically and financially it's possible to build a duplicate of an organisation, but not everyone may want this, or can afford such a luxury. BC is industry-specific. For example, the emergency services like the police or ambulance may not be able to afford to have their IT and other infrastructure out of action even for a few minutes, whereas a small car parts manufacturer may be able to withstand it for quite some time. Therefore, depending on the size of an organisation, the nature of its business and its budget, there are a number of options as follows:

Manual: The use of manual methods if possible.

Other offices: If it is decentralised and has many independent branches, then it may be possible to use their facilities until the affected branch comes online again.

Cold standby: It may have an alternative site with basic IT and non-IT facilities that can be used during extended failures.

Warm standby: This requires re-establishing mission critical systems and services within a short period of time - usually achieved by having redundant equipment that can be used in the event of a disaster.

Hot standby: This requires an alternative site that has continuous mirroring of live data and configurations. This option is usually used by banks and the military, or if there is no downtime tolerance.

What is a DR or BC exercise?

A way of testing the DR 'readiness' of an organisation is to conduct frequent mock exercises of the various areas included in the DR plan - usually by simulating a crisis situation. Such mock exercises test an organisation's ability to respond to a disaster in a planned and effective manner instead of becoming chaotic. For example, if the finance department server is a mission critical DR item, a mock exercise could be conducted at the weekend, or after normal working hours, by invoking a mock disaster. Such a disaster may involve shutting down the system and relocating the finance team to the DR site. All issues should be recorded, and any limitations, deficiencies, or any missed out items should be noted. The exercises will provide first-hand experience of an organisation's ability to cope and manage in the event of a real disaster. Follow on action may then be taken to ensure a better or more effective DR. For example, if an issue was raised that it isn't possible to operate the finance application without connecting at least one printer, then this should be a follow up action prior to the next exercise.

What are the biggest roadblocks for DR or BC?

Every organisation would like to have 100% DR and BC. However, very few organisations are actually willing to make the necessary investments in terms of resources and costs to ensure reliable DR and BC environments. Some of the biggest roadblocks that prevent proper DR and BC are as follows:

- **Lack of sustained management commitment:** A primary roadblock for DR will be lack of sustained commitment. For example, senior management may approve the establishment of a DR or BC site at a time when they are particularly influenced by business and competitive pressures, but may not be willing to invest in the necessary ongoing cost and resources to keep the site fully operational at all times.

- **Inadequate budgets:** Business managers are unable, or unwilling, to invest sufficiently to establish DR and BC options. DR options require investment in redundant equipment, spares, data synchronization equipment, software, hardware, training, insurance and alternative sites.
- **Manpower:** Lack of willingness to invest in additional technically qualified members of staff that are required to maintain and manage a DR site.
- **Knowledge:** Lack of knowledge about what is required to establish proper DR.
- **Other reasons:** Various internal factors, office politics, and limitations.

It is a fact that, in many cases, DR and BC plans simply remain on paper, or have insufficient capability to handle real disasters. If an organisation is to ensure that it's protected from preventable disasters, it needs to invest in the necessary costs and resources.

What are the costs of establishing a proper DR facility?

The costs of establishing a proper DR facility depend on various factors and the nature of the organisation, but generally they can be classified as follows:

- **People:** The number of additional members of staff, contractors and trained members of staff.

- **IT:** The number of additional computer systems, software licences, telephones and communication systems.
- **Maintenance and ongoing:** It isn't enough to simply establish a fully-fledged DR plan as a one-off exercise. It must be properly maintained and periodically updated with new systems, software, data updates, dry runs, etc.
- **Infrastructure and other:** Building rent, electricity, air conditioning, security, transport, telephone.
- **Other costs:** Various one-off or ongoing.

Some dos and don'ts

Do

- Identify a dedicated team within an organisation to be responsible for DR and BC.
- Ensure each member of a DR and BC team understands their role. Clearly establish the scope of DR and BC plans.
- Analyse all business functions and arrange them in order of importance.
- Develop an in-house policy to enforce DR and BC best practices.
- Hold periodic meetings on DR issues and regularly update the DRP.
- Keep customers and members of staff up to date and informed.

- Conduct regular DR mock exercises. Keep up to date with new regulatory requirements, industry practices, standards and qualifications.

Don't

- Take DR and BC functions lightly.
- Give DR inadequate budgets and resources.
- Ignore an organisation's internal talent and knowledge

Are there any international qualifications or training for DR and BC?

More and more employers are looking at certification as a condition of employment. Therefore, because it's often a qualifying pre-requisite for hiring consultants, many universities and institutions have started to provide diploma and graduate courses on DR and BC. There are primarily two recognised professional institutions certifying the BC professional: The Business Continuity Institute (BCI, *www.thebci.org*) based in the UK, and the Disaster Recover Institute International (DRII, *www.drii.org*) based in the USA. Both are member-owned, not-for-profit organisations that offer certification at different levels.

Are there any international standards for BC planning?

ISO22301:2012 (ISO22301) Business Continuity Management Systems (BCSMS) – Requirements is the International Standard for Business Continuity. Launched in May 2012 it replaced the British Standard BS25999-2 and set outs the requirements for a Business Continuity Management System (BCMS). ISO22301 is based on the 'Plan-Do-Check-Act' model as found in other management system standards. An accredited certification scheme exists that enables an organisation to achieve external certification of their BC arrangements.