

Disaster Recovery

1.1 Introduction

Every day, there is the chance that some sort of business interruption, crisis, disaster, or emergency will occur. Anything that prevents access to key processes and activities can be defined as a disaster. Companies can experience many different threats to their mission critical systems such as fires, floods, lightning storms and humidity to disgruntled employees, hackers, human error, power failures and viruses. A disaster can happen at any time and it is vital to be prepared in the event that one occurs.

Disaster recovery became an issue between the 1960's to the 1980's and entailed backing up mainframe computers. At present disaster recovery has stretched to incorporate all scenarios necessary to ensure the successful running of critical systems during an emergency and include the long-term recovery of the business.

Issues such as data protection, human resource concerns, vital records, telecommunications, risk management, security, environmental concerns, product recovery and the business premises are all documented in a disaster recovery plan/business continuity plan.

(Hawkins, Yen and Chou, 2000)

1.2 Reasons for Disaster Recovery

The United States Bureau of Labour performed a study in 2002, which concluded that 93% of companies that experience a considerable information loss become extinct within five years.

In fact it is estimated that 40% never even reopen.

(Hardy and Roberts, 2003)

In August 2003, North America experienced the biggest blackout in its history, which effected many businesses and will continue to do so for a long time.

The 11th of September 2001 is another example of a disaster that had the capacity to destroy any business. Surprisingly, most of the affected companies were able to keep their businesses alive due to the fact that they had business continuity plans in place.

Despite the range of threats that businesses face to their long-term survival, a 2002 Gartner study found that only 35% of SME's have a detailed disaster plan in existence. (Rike, 2003)

The importance of having some contingency plan to protect the company and its data, regardless of how basic it is, cannot be stressed enough. It is useless waiting until after a disaster occurs to try and recover operations because it is a stressful time and an immediate, carefully planned response is required.

Computer systems constitute the backbone of many businesses. Without adequate backup and protection facilities, a company could cease trading if a disaster of any magnitude occurs. Other consequences may include financial loss, reduction in customer confidence and a damaged reputation.

1.4 Types of Threats Facing Companies

It is difficult to account for every threat that a company is faced with. Disasters that have occurred in similar businesses and companies in the same area may be researched to ascertain the type of threats facing a company. Creative thinking techniques such as brainstorming could also be used to determine possible disaster scenarios.

Rike, 2003, categorises threats into three areas.

1.41. Natural or environmental disasters or hazards

A natural or environmental disaster could be anything from a fire, flood, earthquake, hurricane, lightning storm or an air crash. The location of the business premises and the local environment needs to be assessed to determine the exact external threats that the company faces.

1.42. Technical or mechanical hazards

Examples of technical threats include viruses, worms, power outages, backup failure, system failure and hacker attacks such as denial of service attacks.

1.43. Human activities or threats

These include accidental and intentional activities. Malicious attacks may originate from hackers, paid professionals, disgruntled employees or organised crime gangs. Unintentional threats may come from employees who accidentally delete or update information. Over dependence on one key person is also a threat to the system.

The following figure 1.4 is taken from Rike, 2003 and illustrates examples of possible threats to any business.

Potential Types of Exposure		
Natural Threats and Hazards	Technical and Mechanical Hazards	Human Activities and Threats
Fire	Power outage/failure	Computer error
Flood	Gas leak	Lost or misfiled documents/records
Hurricane	Software failure/malfunction	Vandalism
Earthquake	Sewage failure/backup	Theft
Lightning strike	Building structural failure	Bomb threat
Tornado, wind storm	Electrical shortage/faulty wiring	Civil disorder
Snow and ice storms	Toxic spill	Strikes
Wind	Radiation contamination	Kidnapping
Tidal wave	Loss of physical access to resources	Terrorism
Typhoon	Biological contamination	Sabotage
Mold and mildew	Train derailment/airplane crash	Loss of key personnel
Insects and rodents		Epidemic

Figure 1.4

1.5 Business Continuity Planning

1.51 Introduction to Business Continuity Planning

A business continuity plan details how a company will respond to a disaster and reduce its effects. The plan is detailed enough to ensure that the key business processes can be functional within a measured time scale but generic enough that the plan is applicable to a range of disasters. A continuity plan must be updated regularly especially if there is any changes to the business processes, environment or information systems.

Without a formal plan to follow in an emergency, there will be turmoil and uncertainty. A business continuity plan will make disaster recovery cheaper and more efficient instead of relying on an ad hoc plan.

The phases involved in developing a business continuity plan are discussed.

The terms business continuity plan and disaster recovery plan are used interchangeably within this report.

Different backup strategies are available depending on how mission critical the process or system is.

1.52 The Advantages and Limitations of a Business Continuity Plan

The advantages and limitations of having a disaster recovery plan must be considered in order to decide whether or not a budget should be allocated to a business continuity plan.

1.51 The Advantages of a Business Continuity Plan

Firstly, any emergency can be a stressful time and a difficult time to think logically. Having a business continuity plan reduces the amount of panic as each person has been allocated some task and hopefully all of the important activities will have been catered for.

Secondly, minimal disruption is caused to the company because temporary measures have already been prepared and just need to be implemented.

Thirdly, the company is less reliant on key individuals. If these employees have been injured during the disaster, another person can take over their tasks.

Fourthly, data security is critical to the company and is one of its most valuable assets. The company data must be protected above all else. A backup should be made hourly and sent to an external server daily.

Fifthly, the safety of the employees must be considered. A new safe work environment may be needed, as might a support group depending on the severity of the disaster.

Lastly, the business continuity plan incorporates many of the problems facing the company after an emergency and provides tested solutions to these problems. This leaves management to address other concerns.

1.52 Limitations of a Business Continuity Plan

Firstly, developing a successful business continuity plan can be expensive. It takes time and many work hours to identify the key operational systems. Outsourcing the disaster recovery plan can also be expensive. The costs of developing the plan are justifiable however when compared with the costs of not preparing one and performing disaster recovery ad hoc. (Hawkins, Yen and Chou, 2000)

Secondly, sometimes a perceived increase in safety measures can cause staff to believe there is less chance of the risk occurring, this can lead to less cautious behaviour, termed risk homeostasis. Companies should be aware that risk management strategies would not necessarily reduce the risk.

Thirdly, there is often a sense of ambiguity about who is responsible for what area of risk management; this should be clearly defined in the continuity plan.

1.53 Developing the Business Continuity Plan

Rike, 2003 suggests that there are seven phases in the development of a business continuity plan.

1.531 Attaining the support and commitment of top management

The first phase involves cooperation from top management. These staff members must coordinate the business continuity plan and ensure adequate resources are allocated to it such as money, staff hours and training. Only senior management has the power to make these key decisions.

(Savage, 2002)

1.532 Creating a planning committee

The second phase requires groups to be formed who will help develop the disaster recovery plan and will perform roles and responsibilities.

Hawkins et al, 2000 suggest that there should be four teams co-ordinated by the managing director – the initial response team, the restoration team, the recovery operations team and the logistical support team.

The initial response team evaluate the extent of the damage and decide on what recovery strategy to take. Next the restoration team limit damage control and reactivate software, the network configuration, data files and communications. The recovery operations team generally takes over if the initial response team decide that key processes need to be moved to a new location. Finally the logistics support team ensure that staff can access the alternative location and they also offer support to employees in the form of travel, covering costs incurred and counselling.

1.533 Performing risk management

Risk management is a technique used to assess the potential risks to the business processes and the systems, the value of the information and processes that are at risk and how vulnerable the assets are to the risk. The impact of the risk occurring is evaluated, as is the cost of the loss of the asset such as information, time and goodwill. The cost of replacing the asset must also be calculated. This information is used to prioritise the risks and decide how the risks may be counteracted.

There are two ways of evaluating risk analysis – quantitative risk analysis and qualitative risk analysis.

Quantitative risk analysis looks at the probability of a loss occurring and the amount that would be lost if the risk occurred. In qualitative analysis the estimated potential loss is used in a formula such as $\text{risk} = \text{assets} \times \text{threats} \times \text{vulnerabilities}$.

(Symantec, 2000)

Assets are anything of value that are worth securing, threats are anything that could attack an asset in any way and vulnerabilities are weaknesses, which may be exploited to attack an asset. For example assets threats and vulnerabilities could be assigned a number in the range of 0-1 in order to estimate the value or likelihood of each element of the equation. Risks can be prioritised using this formula and dealt with accordingly.

(Savage, 2000)

1.534 Establishing mission critical systems

There are many possible threats to most businesses and so it is impossible to be protected against each one. Instead the mission critical business processes and core systems should be identified and safeguards should be implemented to protect them.

Criteria necessary to perform each key process must be considered such as equipment, communications devices, procedures and vital records. Some non-essential activities will become important a while after the disaster once all of the critical processes are secure. Plans will have to include how to perform them in the longer term.

1.535 Collecting data

In this phase, response measures need to be determined and put into operation. Alternative operating locations must be established, checklists need to be written, inventories of important records and contracts need to be gathered and backup methods decided upon.

When writing up the business continuity plan a suitable location will have to be identified where the mission critical business processes can continue in the short-term. Current ways of performing activities may not be suitable in this new location and this problem will have to be addressed.

There are a number of choices available to companies as alternative business locations.

A fully mirrored recovery site is one option, which enables automatic switching from the live site to the backup site in the event of a failure. This option is expensive and is not suitable for a start up manufacturing company. (Savage, 2002)

Secondly a hot site can be outsourced to a disaster recovery vendor. The alternative location will be fully equipped with all of the requirements of the company such as computer hardware, software, office supplies and communication facilities. The business can be in operation a few hours after a disaster has occurred. This type of disaster recovery is too expensive for a start up company.

(Hawkins, Yen and Chou, 2000)

Another alternative is a buddy site. An agreement could be made to temporarily use the systems of another manufacturing company who has similar hardware and software. It is difficult to keep the systems in sync however.

(Savage, 2002)

Fourthly a mobile recovery facility could be available which contains the necessary computer equipment and has its own generator.

(Hawkins, Yen and Chou, 2000)

A cold site is another choice, which could be used where an emergency location is selected and is ready for use but currently has no equipment in it. An agreement should be made with a vendor to supply the skeleton configuration necessary as promptly as possible. A working site generally takes approximately two to three working days.

(Hawkins, Yen and Chou, 2000)

Lastly, a relocate and restore strategy could be implemented where no plan is in place. A suitable location and information systems must be found after a disaster has occurred. This is not suitable for the manufacturing company because information systems are critical to the business.

(Savage, 2002)

A new location will only be necessary in extreme cases however and most of the time the systems may be relocated to an unaffected part of the premises.

(Savage, 2002)

System backup is one of the most important parts of disaster recovery because if the data integrity, availability, confidentiality, authenticity and reliability are not maintained then the data is useless. Since the organisation relies heavily on its data, reliable system backup is crucial.

There are two types of backup strategies available - in-house backup and offsite backup.

The in-house backup involves placing backup servers across the company. It reduces costs by avoiding external vendors. Offsite backup systems encrypt data and send it to an external location. It is costly to involve a third party vendor but necessary when the importance of the data is considered.

1.536 Documenting the plan

When the risks have been determined, a generic response to cover any disaster will have to be documented in the business continuity plan. The roles and responsibilities of each person should be clear.

1.537 Testing the plan

The plan will not be perfect after its first draft. Important issues will have been missed or backup measures will not have been sufficient. The only way to find these mistakes and stressors is by simulating the plan at least verbally if not physically. The plan can be tested after business hours or in sections to avoid too much disruption.

Paton, 1999 recommends that a neutral figure with authority and experience should run the simulation in a no blame atmosphere so that an outside perspective is applied to the plan. Feedback can then be used to make improvements to the plan. Training should also be held to familiarise staff with the plan.

1.538 Other Considerations

Other considerations that may be included in the continuity plan include how to store hazardous materials and customer relationship management. The skeleton staff required to operate the systems must be identified and kept with the plan along with their contact details. A method of accounting for employees must also be available. A temporary web site or phone line may need to be established to inform employees, customers and suppliers about important updates.

A representative who will manage the media and make press statements must also be assigned. This is vital to preserve customer, supplier and employee confidence. Staff will have to be reassured that they will be getting their pay cheques
(Savage, 2002)

1.6 Conclusion

A disaster is anything, which influences the operation of the critical business processes. It can be a major disaster, which affects the building or an electrical storm, which corrupts the data on the system.

Regardless of the event, the business must be able to recover from the emergency as swiftly as possible and get all of the key processes back in **operation**. By having a business continuity plan despite how simple it may seem, can ensure that the company survives.

This report was written to illustrate how dependent a company is on its information systems, to realistically outline the threats that the computer systems face and to highlight ways that the company can prevent and react to potential disasters.

1.7 References

Hardy, V. and P. Roberts. 2003. "International Emergency Planning for Facilities Management", *Journal of Facilities Management*. London: Vol. 2, Iss. 1; pg. 7.

Hawkins, S. M. 2000. "Disaster Recovery Planning: A Strategy for Data Security", *Information Management and Computer Security*. Vol. 8, Iss. 5; pp. 222-229.

Paton, D. 1999. "Disaster Business Continuity: Promoting Staff Capability", *Disaster Prevention and Management*. Vol. 8, No. 2; pp. 127-133.

Rike, B. "Prepared or Not...That is the Vital Question", *Information Management Journal*. Lemexa: Vol. 37, Iss. 3; pg.25.

Savage, M. 2002. "Business Continuity Planning", *Work Study*. Vol. 51, No. 5; pp.254-261.

Symantec Corporation. 2001. "Assets, Threats and Vulnerabilities: Discovery and Analysis. A comprehensive approach to Enterprise Risk Management".

<http://enterprisesecurity.symantec.com/PDF/AxentPDFs/RiskMgmt.pdf>