CHAPTER 1: INTRODUCTION

1.1 Purpose and Significance of Study

The ideal world would make disaster recovery plan, a redundant task. Nobody would want to face his/her business around them collapse due to fire, flood, theft or terrorist attack. Nonetheless, these things do happen and it is unpredictable.

The IT industry has been buzzing with Disaster Recovery ever since the September 11 attack in the United State of America last year. The concept of Disaster Recovery has been around for many years but only lately do organisation start realising the important of it. Many businesses invested a lot of money and time on information infrastructure; i.e. automating manual processes, telecommunication enhancement, hence making the disaster recovery more complex each day. Till date, disaster recovery is not just about getting systems back online after power failure but companies are expecting to recover business from 'disaster recovery plan' after unforeseen disasters.

Disaster is defined in Webster's New World Dictionary, *'great or sudden misfortune that results in loss of life, property, etc'*. Recovery is defined as *'to regain something lost or stolen'*. Disaster Recovery Plan is basically the prepared plan of how to regain the sudden misfortune.

According to Dr. Sellayapan, there are three basic types of disasters. There are natural disasters, accident threats as well as deliberate disasters.

Accidental threats are unintentional errors caused by humans or unexpected catastrophes. For example, disasters like flood and fire. The threat can result in damage of computer equipment and documents. Valuable data can be lost. A user may accidentally delete valuable data in a master file during file update. The organisation may have to resort to manual system until data is restored. Another accidental threat that often happened is telecommunication problems. Many

applications today are in a distributed nature, either via network based or internet based and these applications are 100% dependent on telephone, coaxial, LAN or fibre optics, it is possible that the transmitted data maybe lost or corrupted while on transit.

Another disaster is a deliberate disaster or man-made disasters. Examples would be the disaster that was faced by Microsoft Corporation and September 11 US Attack. People cause deliberate threats intentionally. People may be from within the organisation or external. They are actually computer criminals, basically their intention is to destroy the system or to steal valuable confidential information or money electronically. There are four identified threats to a company. First is data theft. Stealing of documents or diskettes to be sold to competitors. Next, sabotage, which has simple objective of damaging the firm's computer system. Thirdly, hackers are deliberate threat as the person who gains access to computer system, uses it unlawfully. Lastly, computer virus, a program when executed would spread and infect other programs and destroy the system. According to Computer Security Institute (ComputerWorld, Nov 9, 1998), corporate losses for the year exceeded US$135 million, and more than US$50 million of the amount was because of unauthorised insider access.

Of course last but not least of the list is the natural disaster, it can earth-quake, which happened in Gujarat, India or hurricane.

Because of the possibility of disaster occurring, there is a need of disaster recovery plan. Disaster recovery began in the late seventies as a method of protecting large computer data centre installations from unlikely events like earthquakes, hurricane, etc. For a business struck by disaster, whether it be a natural causes like a flood or earthquake or unnatural cause like fire, explosion, equipment failure or theft, important survival of a company is preparedness. To be prepared is not just by having a plan and documenting them; in fact it involves a lot of process. According to Ronald A. Cuccaro, in his article "Expecting the

Unexpected Part of the Unexpected", said that, the most important part of establishing a comprehensive disaster recovery program should be adopting the philosophy that you can best protect your firm not just by assuming that you're covered, but by digging deeper into potential problems and exposures and by expecting the unexpected part of the unexpected.

The history of Titanic depicts a good example of fault tolerance and disaster recovery. It provides a classic example of where people have tendency to have too much confidence in the ability to prevent disaster from affecting the operations and not adequately prepared to recover should the disaster break through those preventive measures. In Titanic, there were not enough of lifeboats because she was thought to be unsinkable. The lifeboats were just then thought as decoration purposes only.

In the Information Technology Age, computer systems are vulnerable to various threats, which may lead to loss of data and / or system failures. Information is money. When system fails, it means system unavailable for use. As the result, firms cannot perform its operation or can only perform manually. This means volume of business is less and would lose business if not careful. Customers are dissatisfied as the manual way might be of inconvenience to them, eventually loosing customers. Customers are business and business is money. On top of that, system restoration costs time and money. The cost of failure in recovers might be dependent to the damage occurred. Unless there is adequate backup, information in corporate database may not be able to be restored. Without these data, a company might be in a difficult position to resume its business. Even though some firms may insure their properties, but filing claims need evaluation of the damages and there is high tendency of disputes in the amount that the insurer will pay. Restoring a system is expensive and time consuming.

There is tangible and intangible cost in restoring computer system. Hence, a company must do all that it can to minimise the consequences of all forms of threats. Business Disaster Recovery Plan looks into the cause and effect of security risks. It looks into preventive actions as well as contingency actions. For instance, 'system failures', preventive action looks into what actions are needed to prevent the system from failing and contingency action is about, if the system failed, what are the steps needed to bring up the system in minimal time and cost.

In today's highly competitive edge, companies are struggling to stay on top by finding ways to limit expenses and increase profits. None of the company can afford the loss of property and productivity from destruction caused by disaster. When Information Technology is involved, there is definitely an involvement of Disaster Recovery.

Hence, backup and safe storage of information is fundamental to the reliability and recoverability of each system and its supported businesses. In the event of information corruption or loss, disk hardware failure or site disaster, the backup information is often the link to recovery. Backup and recovery standards define requirements which must assist in providing for a timely recovery of critical business activities when an outage or a disaster occurs. This would helps an organisation to ensure that their business has a continuity plan to resume.

The main objective of Disaster Recovery Planning is to ensure the continuity of business and operations in the event of unanticipated disruption. Disaster recovery is needed in an organisation, no doubt about that. It is an ideal situation if all the systems in an organisation have their disaster recovery. It is actually a myth. The main question is to what extend is the investment? What is the reality on the investment behind Disaster Recovery in an organisation? The rule of thumb is, the cost of the recovery plan should not exceed the benefit derived.

1.2 Research Questions

The research questions identified below are based on the purpose and significance of the study as explained above:

- What is the new insight of Business Continuity of an organisation?
- How do we develop an effective Disaster Recovery Process?
- How do we apply the theory into a practical in MCSB Systems Berhad?

1.3 Scope of Study

The scope of study will be focussing on business information only, which is directly involve with the recoverability of data of an organisation to ensure the continuity of business if similar facilities were to put in place.

Through this study, a clear understanding of business impact analysis would make possible determination of criticality of business information in an organisation. A step by step disaster recovery planning process will be followed to ensure the business continuity implementation will be done successfully if disaster ever occurred. In the later chapter of the thesis, the concept above would be applied to MCSB Systems Berhad.

This paper will discuss the new insight into Business Continuity. It will also recommend the most appropriate Disaster Recovery Plan and Standard Operating Procedure that need to be adopted by MCSB Systems to ensure the continuity of business after disasters.

Disaster Recovery Management and Business Continuity is a very large topic of discussion. It could be from the point of discussion of end-to-end of the topic, from management of employees to management of business information. At the same time, there are limitations of the study in term of time, resources as well as literature.

1.4 Organization of the Study

The study is broken into five chapters.

In Chapter 1, an introduction of the thesis will be emphasised. In this chapter too, the purpose and significance of the study will be discussed.

Chapter 2 will focus on the literature review of the topics. Focuses on the theoretical aspects of business continuity. Among the areas touched includes examples of disasters all around the globe. This chapter also looks into the lesson learned from some of the disasters that happened in the world.

In Chapter 3, Disaster Recovery Process methodology is highlighted. It identified the mission critical of the organisation. It also explained step by step process plans to ensure information in an organisation is protected against the effects of a disaster. Business Impact Analysis (BIA) helps to access the critical systems and data in an organisation. BIA is the underpinning of a disaster recovery plan that would focuses on what business is needed in order to survive should a disaster to strike. BIA is able to assess current organisation vulnerabilities as well as site risk assessment. This is to access infrastructure as well as environment risks and define the minimum acceptable levels of outputs. Upon knowing the critical systems in an organisation, an organisation would be able to select recovery option and strategy method. Policy can be drawn to establish the backup and records retention plan.

In Chapter 4, the methodology in chapter 3 is applied with respect to MCSB Systems Berhad.

The last chapter would then summarise the findings of this thesis and recommendations for future research.