CHAPTER 1

INTRODUCTION

CHAPTER 1

INTRODUCTION

The main focus of disaster recovery planning is to ensure that there is a recovery capability in the event of a sudden, severe and unplanned disruption in an organization. The planning must ensure continuity of all the critical functions with minimum disruption and recover quickly during such calamity. The elements of a comprehensive and complete disaster recovery planning must include risk analysis and business impact analysis in order to recommend a suitable disaster recovery strategy.

Risk analysis on the system may ease the identification of risks, vulnerabilities and exposures of the organization's asset. Risk is a measure of the cost of a realized vulnerability that incorporates the probability of disaster occurrence. Whilst vulnerability is defined as the weakness in the disaster recovery safeguard.

Computers and networks become an integral part of daily operation for most of the business, education and government organizations. Thus, it is a dependable system for most of the organizations. Dependability is defined as the trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers.[1]The most significant attributes of dependability are reliability, availability, safety and security. Reliability deals with continuity of service, availability with readiness for usage, safety with avoidance of catastrophic consequences on the environment, and security with prevention of unauthorized access or handling of information. [2]

One of the most essential assets in these organizations is data. Any data loss can be devastating and may impair the performance of critical tasks with resulting loss of productivity, revenue, and even customers and market share. Besides, in a distributed computing system, the data are spread out over a network. Hence, the vulnerabilities of data assets are increased compared to a centralized computing system. The probability of disaster occurrence is also significantly higher, especially in a less secured client-server environment.

Thus, disaster recovery strategies are vital to protect data assets from a catastrophic event. Consequently, data backup strategy is defined as the activity of copying files or databases to an off-site so that they will be preserved in case of equipment failure or other catastrophe. Restoration is the reverse activity that involves retrieval of backed up file from the off-site storage.

Local and remote data backup system is the designed strategy based on the risk analysis and case study in a business organization. In the local area network, distributed local data backup system is proposed so that the storage devices are distributed throughout the network. Whilst, this system also support remote data backup by using the File Transfer Protocol (FTP). Data could be backed up to or restored from the FTP server over a wide area network. Therefore, this dissertation studies on disaster recovery planning focusing on developing strategies of local and remote data backup in a network-computing system.

1.1 PROBLEM STATEMENT

It may be readily noticeable that there has been an increased dependency on the computer and communications technologies since its introduction to business data processing in the mid-1950s. Some of the organizations typically banking systems need highly dependable computing system in order to perform critical task. Çonsequently, there should be a proactive preparation to mitigate effects of disasters on these technologies. Hence disaster recovery planning may ensure the survival of business continuity in the face of disaster.

Furthermore, there are many lack tested disaster recovery programs for the distributed computing systems typically the lack standard back up procedures. A survey from Comdisco[3], one of the world's leading providers of solutions that help organizations reduce technology cost and risk, shows that the disaster recovery planning has not kept pace with the rapid movement of critical data from the centralized system into the new environment in distributed systems. Hence, most organizations' distributed environments are at significant risk in the event of a disaster. This vulnerability index of Comdisco in 1997 surveyed more than 200 of the largest computer users in the U.S., Canada and United Kingdom, and reveals some eye-popping statistics,

"Overall, only 12 percent of companies have an effective disaster recovery program in place for their enterprise computing systems. The vast majority of companies, 82 percent, has ineffective recovery programs for their enterprise wide computing environments and is extremely vulnerable in the event of a disaster affecting their computer systems." [3]

1.2 DISSERTATION OBJECTIVES

Even though several of backup strategies are implemented in the network-computing system, vulnerabilities to data loss still exist. Therefore, the objectives of this dissertation are to:

i) Determine all possible disasters that may attack the network-computing environment through risk analysis.

ii) Perform a case study on the disaster recovery planning in a selected business organization and provide sufficient solutions for vulnerabilities found.

iii) Design the local and remote data backup strategy, based on the observation and analysis, necessary to recover data assets after occurrence of disaster.

iv) Develop the local and remote data backup system as a part of the disaster recovery planning for data asset.

v) Test the developed local and remote data backup system.

vi) Discuss on strengths and drawbacks of the implemented strategy.

1.3 SCOPES OF THE DISSERTATION

This dissertation focuses on developing the data backup strategy in disaster recovery planning. As a result, the scopes of dissertation are to:

1. Review on the techniques in disaster recovery planning, threats, vulnerabilities and data backup strategies in order to gain knowledge to fulfill the objectives of this dissertation.
2. Conduct the study on management of network and data warehousing techniques in order to design an efficient backup system.
3. Perform a case study on the disaster recovery planning on a selected business organization and design an appropriate backup system.
4. Conduct the study of windows socket network programming and review all of FTP commands.
5. Develop local and remote data backup system performed on Windows 98 platform.
6. Develop the local data backup module where data can be stored in any media storage devices, including the magneto-optical storage and magnetic disk drives, that resided in the LAN.
7. Build a remote data backup module where data will be transferred over the WAN using FTP. Therefore, this module would communicate with the FTP server that will establish both the control and data connection. After the authentication of user name and password, data can be backed up to the remote FTP server for off-site storage.

1.4 SIGNIFICANCE OF THE DISSERTATION

The target audiences of this dissertation are network administrators who have a great concern on the risk of data loss. Therefore, it will offer great benefits to most organizations, which operates on a distributed computing environment embraced from Local Area Network (LAN) to Wide Area Network (WAN). Besides, the case study, discussion and analysis on various data backup strategies can be used as guidelines in disaster recovery planning.

1.5 METHODOLOGY

The procedures that have been followed up to accomplish this dissertation is as illustrated in Figure 1.1, Overall Dissertation Process. Generally, it can be divided into four stages. They are problem statement, literature review and analysis, observation and design plus implementing and testing.

The main problem is viewed in the perspective of how to develop an effective data backup strategy in disaster recovery planning. Thus, as reviewed, there are three courses that must be taken into account. They are off-site storage, backup site and risk analysis on users' requirements.

After the literature review, the process is continued to perform a case study on a selected business organization. Risk analysis is implemented on the backup strategy of the target organization. This includes identification of threats and vulnerabilities in the existing data backup strategies of the organization. Consequently, local and remote data backup system is designed as the solution for the vulnerabilities found.

The final section of the dissertation process is the implementation of proposed strategy. This involves the development of local and remote data backup system. After conducting system coding and testing, this is followed by the discussions on the achievement and future enhancement of the implemented strategies.

1.6 REFERENCES

Literature review on disaster recovery planning, data backup strategies, fault tolerance system, distributed computing network system, descriptions and implementation of FTP, security issues, threats, vulnerabilities and risk analysis on various system had been performed. These literatures include references from books, magazines, journals, RFCs, and other resources available in Internet.

1.7 DISSERTATION ORGANIZATION

Chapter 2: Literature Review

This chapter covers an overview on a disaster recovery planning. The discussion revolves around the strategies of disaster recovery and backup system. In the local and remote data backup system, data storage devices have been reviewed. Besides, it also involves the data backup strategies and comparison of backup system in both of the local and remote data backup system. In order to develop a remote data backup system, perspective, model and commands of File Transfer Protocol (FTP) have been studied. Eventually, the synthesis of local and remote data backup system is taken into account.

Chapter 3: The Need of Risk Management in Disaster Recovery Planning

Chapter 3 focuses on risk management on the network ,computing system. The need for risk management in disaster recovery planning is discussed. Risk management, which involves risk analysis, risk assessment and identification of systems requirements, is discussed in this chapter. In addition, risk analysis, which covers identification and prioritization of assets, threats and vulnerabilities, are also performed. These supplement the needs to design a dynamic data backup strategy.

Chapter 4: Observation and Design of Data Backup Strategy in a Business Organization

Chapter 4 involves case study on a business organization with local area network environment. Risk analysis is implemented on the existing backup strategy in the organization, which include identification of threats and vulnerabilities. Based on the analysis, a local and remote data backup strategy is designed with the discussion of its features. This designed strategy has solved the existing vulnerabilities in the risk analysis of the business organization.

Chapter 5: Implementation of Local and Remote Data Backup System

This chapter highlights the implementation aspect of this dissertation. Concept of local and remote data backup system is discussed. The modules in this system include local data backup module, remote data backup and restore module, scheduled and incremental backup module and log files module. Their algorithm and implementation have been taken into account.

Chapter 6: Testing and Results

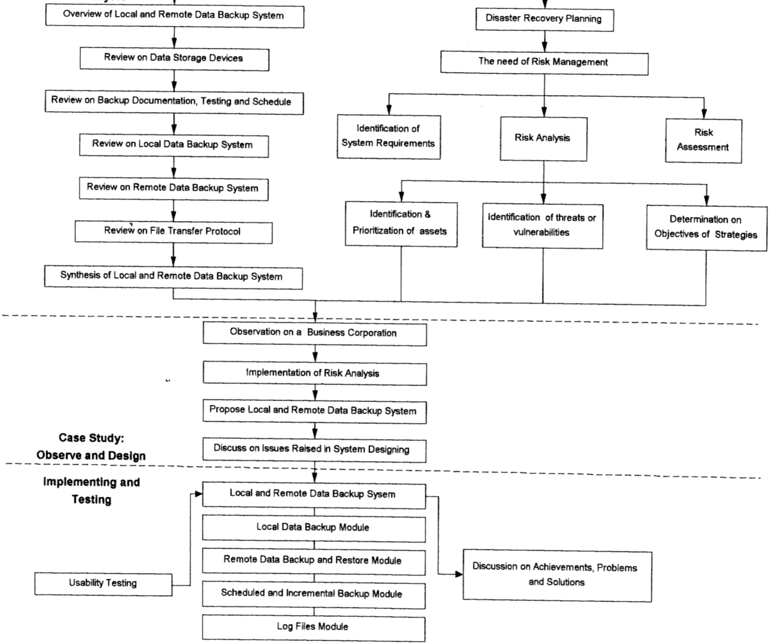
Chapter 6 investigates the usability and functionality testing of the proposed local and remote data backup system. This involves a mock disaster where deletion of data file is performed. Testing results and discussions of each module in the system are included in this chapter. Eventually, the evaluations, strengths and drawbacks of the local and remote data backup system are also discussed.

Chapter 7: Conclusion and Future Enhancement

This final chapter concludes the overall presentation of the dissertation. It includes achievements, system constrains, and discussions about the future enhancement on this dissertation.

Appendix A: User Manual for Local and Remote Data Backup System

This appendix shows the user manual of local and remote data backup system. It includes steps to perform setup in each menu.


Overview of Local and Remote Data Backup System
Review on Data Storage Devices
Review on Backup Documentation, Testing and Schedule
Review on Local Data Backup System
Review on Remote Data Backup System
Review on File Transfer Protocol
Synthesis of Local and Remote Data Backup System
Disaster Recovery Planning
The need of Risk Management
Identification of System Requirements
Risk Analysis
Risk Assessment
Identification & Prioritization of assets
Identification of threats or vulnerabilities
Determination on Objectives of Strategies
Case Study: Observe and Design
Observation on a Business Corporation
Implementation of Risk Analysis
Propose Local and Remote Data Backup System
Discuss on Issues Raised in System Designing
Implementing and Testing
Local and Remote Data Backup Sysem
Local Data Backup Module
Remote Data Backup and Restore Module
Scheduled and Incremental Backup Module
Log Files Module
Usability Testing
Discussion on Achievements, Problems and Solutions