CHAPTER 3

THE NEED OF RISK MANAGEMENT IN DISASTER RECOVERY PLANNING

CHAPTER 3

THE NEED OF RISK MANAGEMENT IN DISASTER RECOVERY PLANNING

3.1 INTRODUCTION

In a network computing system, data assets are vulnerable to various types of risks, threats and disasters. These phenomena become worst when the network embraces a local area network to an international network. Therefore, there is a need of risk management in disaster recovery planning for a network computing system.

Hence, this chapter focuses on risk management on the network computing system. Risk management, which involves risk analysis, risk assessment and identification of systems requirements, is discussed in this chapter. These supplement the needs to design a dynamic data backup strategy.

3.1.1 THE NETWORK COMPUTING SYSTEM

Computing system could be generally classified into centralized systems and distributed systems. Centralized systems or the mainframe type technologies are usually used in banking system because of its powerful security features. Thus, it supports mission-critical systems where there are needs in consistency of data and satisfactory performance in workload management.

On the other hand, distributed systems operate in a seamless and less protected networks. These distributed workstation types of technologies evolve in a fast pace because of their effectiveness in resource sharing, its high performance in low cost and its extensibility of system size. Besides, it offers a better fault tolerance system and provides functionality not less than that expected from a single computer. However, management of such a decentralized computing environment is much more complex than that of a centralized mainframe environment.[11]

3.1.2 DEFINITION OF DISTRIBUTED COMPUTING SYSTEMS

Distributed systems are defined as:

"A distributed system consists of a collection of autonomous computers linked by a computer network and equipped with distributed system software. Distributed system software enables computers to coordinate their activities and to share the resources of the system - hardware, software and data. Users of a well-designed distributed system should perceive a single, integrated computing facility even though it may be implemented by many computers in different locations."[12]

In other words, distributed systems can be viewed as a client and server architecture where the information system is composed of several server functions that provide services to a large numbers of client functions. These application design approach can be executed in various hardware or interconnected platform.

3.1.3 VULNERABILITIES IN DISTRIBUTED COMPUTING SYSTEMS

However, there is an evidence, based upon Comdisco's 1997 Vulnerability Index survey about more than 200 organizations in the U.S., Canada and United Kingdom, where the organizations' distributed environments are at significant risk in the event of a disaster. [1]The Vulnerabilities Index Score on Data Center, Local Area Networks (LANs) and Wide Area Networks (WANs) is shown in following figure, where 0 is least vulnerable and 100 is completely vulnerable.

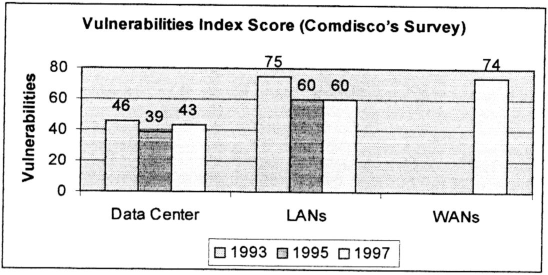

Figure 3.1 Vulnerabilities Index Score from Comdisco's Survey [1]

In fact, as illustrated in the figure 3.1, stability of Vulnerability Index in LANs and Data Centers has been maintained over the year from 1993 to 1997. However, the average Vulnerability Index for the WANs was 74, compared to an average Index of 60 for LANs and 43 for Data Centers. Hence, with the migration of computing away from centralized data centers to a wide distributed system, enterprises are increasingly vulnerable. The risks encountered includes[13]:

- Loss of data in multiple database
- Loss of multiple servers
- Loss of interdependent functions at many points
- Loss of application systems at many points
- Loss of a wide variety of ever-changing technology

Therefore, an appropriate disaster recovery planning should be analyzed and implemented in an efficient way in order to overcome the challenging vulnerabilities faced in distributed system.

3.2 THE NEED OF RISK MANAGEMENT

Based on the definition of Gail S. Howell in [21], risk management is a process that consists of five parts:

- An assessment of the value of an asset
- Identification of the threat to that asset
- Definition of the vulnerabilities of the asset
- Identification of security countermeasures that could nullify/reduce the threat to the asset
- Analysis of the cost/benefits of employing the countermeasures

In other words, the risk management process encapsulates two key components. Firstly, the structured risk analysis determining the existing and risk assessment recommending levels of risk to the assets. Secondly, the identification of system requirements that could reduce the threat, regarding to the cost-effective analysis.

3.2.1 RISK ANALYSIS

In disaster recovery planning, risk analysis is the proper methodological instrument for assessing the needs of system by identifying risks and exposures. Generally, risk analysis consists of three main objectives. [10] Firstly, identifying and prioritizing the assets and functions according to time sensitivity and criticality. Secondly, identifying possible threats or vulnerabilities to these assets and functions. Finally, setting objectives for any strategies developed in the disaster recovery planning in order to eliminate or minimize the impact of risks.

3.2.1.1 IDENTIFICATION AND PRIORITIZATION OF ASSETS

Listing inventory of assets that are going to be protected is the initial step of addressing the issue of risk analysis. The assets may include hardware, software, telecommunications components, physical devices, data and other documentation and records. Subsequently, this is followed by the prioritization on the inventory lists according to the criticality, vitality and time sensitivity. The equivalence of these measurements is the ability of the system to cope with the interruption of asset in term of tolerance. In the context of data processing, assets may be defined on the spectrum of tolerance as depicted in Table 3.1.[10]

Table 3.1 Spectrum of Tolerance[10]

	Features of Assets	**Restoration Process**
Critical	Tolerance to interruption is very low and the cost of interruption is very high. The functions of system terminate until the replacement of interrupted assets.	Require rearrangement of whole system to the backed up form.
Vital	Tolerance to interruption is slightly higher and somewhat lower costs than critical assets provided that restoration is completed within a certain timeframe. The functions of interrupted asset can be performed manually for a brief period of time.	Require a considerable amount of "catching up" to restore data to a useable form.
Time Sensitive	The functions of interrupted asset can be performed manually for an extended period of time.	Require considerable "catching up" once restored
Non-Critical	May be interrupted for an extended period of time with little or no cost.	Require little or no "catching up" when restored

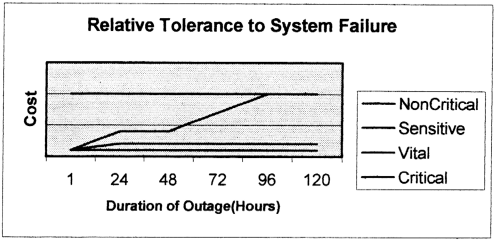

Figure 3.2 Relative Tolerance to System Failure [10] p. 36

3.2.1.1.1 IDENTIFICATION AND PRIORITIZATION OF DATA

However, the main concern of asset in current dissertation is the availability of data that are stored on a network environment. This may comprise of the financial, statistical, payroll, personnel, planning, operations, tactical, defense, trade secrets and others information of an organization. With the identification of dedicated assets, prioritization based on their functions shall be analyzed as shown in Table 3.2.

Table 3.2 Analysis on prioritization of various kinds of data assets

Examples of data assets in network	**Prioritization**
General data related to organization's critical mission	Critical
Transactions:	
Related data in transactions	Critical
Data in security services such as authentication PIN, secret keys and other passwords.	Critical
Finance Department:	
Book Keeping	Time Sensitive
Collection of Debit and Invoice Generation	Vital
Project Planning	Time Sensitive
Human Resource and Administration Department:	
Generally the staffing and payroll data as well as other maintenance, such as salary scheme, general office maintenance.	Non-Critical

3.2.1.2 RISK IDENTIFICATION

The objective of risk identification is to identify all possible risks in timely and proactive manner. Risk Identification methods should have the following attributes:

1. All areas of the disaster recovery planning should be examined in a systematic manner;
2. The risks should be proactive rather than reactive;
3. The risk information should be synthesized from all available sources of risk information.

3.2.1.2.1 THREATS AND VULNERABILITIES

Accordingly, possible threats or vulnerabilities to the data assets are to be analyzed. A threat is defined as a person, thing, event or idea, which poses some danger to an asset in term of confidentiality, integrity, availability and legitimate use. While, risk is defined as a measure of the cost of vulnerabilities or the cost of weakness in safeguards. [14]

Threats, both natural and human risks can pose serious impact on data center operation. They can be classified as follows:

- Natural disaster like fire, water, earthquake, storms;
- Environmental facilities failure involving electric power;
- Network mechanical breakdown or software failure;
- Vandalism, sabotage, rioting, terrorism, labor disputes;
- Network threats involving accidental or deliberate destruction by intruders or hackers.

3.2.1.2.2 NATURAL DISASTERS

Natural disaster may be the worst disaster of the all that happened in a particular region. Environmental facilities failure typically outage of electric power, destruction of data center, breakdown of network and the loss of life may cause by the acts of God. In the case of the earthquake that devastated the island of Taiwan on September 21, 1999, numerous homes and businesses were destroyed. To date, over 100,000 people are left homeless; over six thousand homes were completely wiped out.[15] Additionally, many organizations have to postpone their production because of the inadequate power supplies and destruction of computer facilities including the primary data center. Numerous businesses in the computer and network industry were affected as a result.

3.2.1.2.3 DEFICIENCY ON NETWORK MANAGEMENT

Another originator of the failure of network environmental facilities, thus hardware or software, may be the deficiency on management or on system maintenance. Poor management of resources typically data center is one of the obvious vulnerabilities. As indicated by Patrick Kelly while analyzing company disaster preparedness plans, data center that has been managed in a way of "single point of failure" is just similar as putting all their eggs in one basket and watch them. [16] Consequently, these have significantly increased the vulnerabilities of system and decreased the survivability in case of a major disaster.

3.2.1.2.4 DEFICIENCY ON SYSTEM MAINTENANCE

System maintenance, in the other hand, is an approach that should be exercised to ensure the continuity services of the hardware and software. Computer machine, storage and backup medium, interface and communication equipment plus other hardware devices are subject to failure. Beside, defects in the operating system and programs must be also taken account.

3.2.1.2.4.1 Y2K CRISIS

A significant example of preventive maintenance is the Y2K crisis where every date-sensitive hardware and software that will roll over from "99" to "00" must be maintained by [17]:

- Testing and fixing every line of computer code that contains a date field;
- Repairing every data interface;
- Rewriting every date field in every corporate database file;
- Replacing every electronic component containing an embedded microchip that reads dates.

Obviously, any inadequate maintenance planning on Y2K compliance may cause various kinds of damage especially on the date dependence system. Dates give better representation of the demographic patterns in most of the organization operation. Computer programs expect to locate the data records containing the dates in the correct place. Beside, non-programmable microcircuits in the embedded chips that are hard-wired into other pieces of equipment may include date calculation in their programming logic. Hence, the inaccuracy ordering of dates that arise from Y2K crisis may practically affect most of the organizations and systems as summarized in Table 3.3.

Table 3.3 Possible Y2K Crisis Vulnerabilities in various Systems and Organizations[17]

Systems and Organizations	**Possible Vulnerabilities in Y2K Crisis**
Banking, finance	Calculation of interest, mortgages, loans, current accounts, fixed deposit accounts, savings accounts, customer profiles and vaults control;
Security system	Sending and receiving units, video and surveillance systems.
Construction and building	Commence and completion, booking, sales and purchase, project management;
Retail and distribution	Shelf life, invoice, payments, inventory, delivery, promotion and seasonal;
Shipping and transportation	Shipping dates, arrival dates, fleet management, port facilities, bonded warehouse and storage time and cost;
Infrastructure	Telecommunications equipment including satellites, repeaters, cellular phones, pager and call management system; Medical devices and equipment including monitoring system, dialysis chemotherapy, laboratory, radiology and radiation equipment;
Utilities and distribution	Power generation, monitoring and control equipment and grid date sensitive;

3.2.1.2.5 NETWORK SECURITY THREATS

Network threat is another issue of vulnerabilities typically to the information technology and the Internet dependence systems. As this dependency on information technology becomes more critical in completing mission; destruction, manipulation or denial of access of information resources could be a disaster. Potential enemies may devastate a corporation's assets using tools as simple as a modem and following paragraph indicates the evidences.

"... *News reports are filled with stories of hackers attacking agencies such as the CIA and NASA. Recently, a hacker in the UK stole proprietary data from the Rome Air Development Facility through the Internet. Both the Social Security Administration and the Justice Department had to shut down compromised web sites. Langley Air Force Base and several government and academic sites were victims of an e-mail attack, shutting down e-mail for hours... "[18]*

In essence, the network related security risks could be categorized into theft of confidential or secret information, theft of assets plus other hacking and malicious damages, which involve data interception or modification, unauthorized access to networked resources and misrepresentation of identity. Consequently, the issues of data corruption, inaccessible to resource, loss of sales and loss of customer confidence may be arisen. Table 3.4 illustrates the typical threats associated with the applications in network security requirements.

Table 3.4 Typical threats associated with the applications in network security requirement [14]p. 31

Requirement	Threats
Banking:	
Protect against fraudulent or accidental modification of transactions	Integrity violation
Identify retail transaction customers	Masquerade, repudiation
Protect PINs from disclosure	Eavesdropping
Ensure customers' privacy	Eavesdropping
Electronic Trading:	
Assure source and integrity of transactions	Masquerade, integrity violation
Protect corporate privacy	Eavesdropping
Provide legally-binding electronic signatures on transaction	Repudiation
Government:	
Protect against unauthorized disclosure or manipulation of unclassified but sensitive information	Masquerade, authorization and integrity violation, eavesdropping
Provide electronic signatures on government documents	Repudiation
Public Telecommunications Carriers:	
Restrict access to administration functions to authorized individuals	Masquerade, authorization violation
Protect against service interruptions	Denial of service
Protect subscribers' privacy	Eavesdropping
Corporate/Private Network:	
Protect corporate/individual privacy	Eavesdropping
Ensure message authenticity	Masquerade, integrity violation

3.2.1.2.5.1 COMPUTER VIRUS CRISIS

Computer virus crisis is one of the most vulnerable disasters faced in the distributed computing systems. In general, these malicious programs that replicate themselves can cause various types of damage or perform undesired or unintended operations. Trojan Horse, worms, viruses and bombs are included in this class that might make random changes to data files, encrypt or distort the data, physically damage the storage devices and copy data for illegal access.[19]

In fact, the Chernobyl virus recently demonstrated how easy it is to disrupt a system and cause millions of dollars worth of damage. Besides this notorious virus, there are plentiful of them that are vulnerable to various areas of the international infrastructure. For example, there are viruses that will overheat the Central Processing Unit by locking it in a divide by a zero loop for a sufficient amount of time. In addition, some viruses may attack the Domain Name Service (DNS) by shuffling the directory systems in the resolution tables, so that fault matching of the IP numbers occurs.

"*...The Chernobyl virus wreaked havoc in the Middle East and Asia as well as some European countries. This virus, which was set to activate on the anniversary of the Chernobyl incident, attempts to corrupt the data on the hard drive, while at the same time tampering with the boot up (BIOS) program, with-out which the computer can not be turned on. South Korea for instance, estimates that up to 15 percent of all its computers may have been affected causing damage of up to $250 million. Other areas of the world also suffered extensive damage...* "[20]

Furthermore, if several of the malicious viruses were to attack simultaneously, a catastrophe may break out in the system, which require days and months to clean up and, in some cases, rebuild the system. The only way to mitigate possible attacks is through heightened awareness and constant vigilance.

3.2.2 RISK ASSESSMENT

Risk assessment or prioritization is one of the essential processes in the continuous and iterative risk management. The objective of Risk Prioritization is to prioritize the identified risks for mitigation. Both qualitative and quantitative methods can be used to categorize the risks as to their relative severity and potential impact on the assets. [22] To effectively compare identified risks, and to provide a proactive perspective, the risk prioritization method should consider the following factors:

1. The probability of the risk occurring;
2. The consequence of the risk;
3. The cost and resources required mitigating the risk.

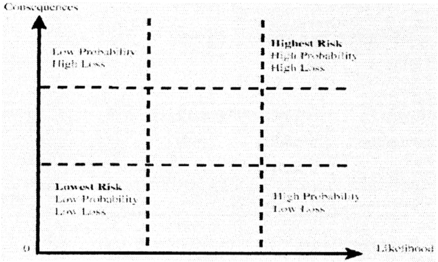

Figure 3.3: Risk is a function of likelihood of loss and expected consequences of loss.[23]

As illustrated in figure 3.1, the simple framework for assessing risk is based on the likelihood or probability of loss and consequences of loss. Whence, any risk can be assigned a position somewhere on this two-dimensional scale.

3.2.2.1 METHODOLOGY OF RISK ASSESSMENT

Hence, in a distributed network system, the risk assessment on the data assets may generally be determined by adding the sum of the Probability multiplied by the weighting and the Business Impact multiplied by the weighting plus the Cost of Recovery multiplied by the weighting. Based on the source [5]p.58, a sample risk prioritization will be done depicted in Table 3.5 where the rating of weight is from 1 (low) to 5 (high) where Composite shows the weight of possible risk. Hence, in the case of Table 3.5, Hardware Failure in the system has the highest priority in the occurrence of risk while the risk of Chemical Spill has the lowest.

Table 3.5 A Sample Risk Prioritization

Disaster	**Factor Risk**	**Probability (0.5)**	**Business Impact (0.3)**	**Costs of Recovery (0.2)**	**Composite**
General	Riot	1	3	3	2
	War	1	4	4	2.5
	Bomb Threat	1	3	3	2
	Loss of Key Staff	3	3	2	2.8
Natural	Earthquake	1	4	4	2.5
	Floods	2	3	3	2.5
	Typhoon	1	4	4	2.5
	Major Building Fire	2	4	4	3
Regional	Fire	2	4	4	3
	Power Failure	2	2	2	2
	Chemical Spill	1	2	2	1.5

Security	Virus Infection	3	3	3	3
	Unauthorized Access	2	3	3	2.5
System	Hardware Failure	2	5	4	3.3
	Software Failure	2	3	3	2.5
	Communication Failure	3	3	3	3
Man Made	Human Error	3	2	2	2.5
	Cable Cut	2	4	3	2.8
	Explosion	1	4	4	2.5

3.2.3 IDENTIFICATION OF SYSTEM REQUIREMENTS

Based on the risk analysis that has been accomplished on the previous sections, the requirements or objectives of the disaster recovery planning could be set in order to eliminate or minimize the impact of risks.

3.2.3.1 PREVENT DATA LOSSES

In a distributed system where data have been identified as the main asset to be protected, the main concern in a disaster recovery planning is to prevent the loss of data. Consequently, the planning also protects against malfunctions of application systems and minimizes the downtime of computer network.

3.2.3.2 MINIMIZING NETWORK DOWNTIME

In fact, the impact of network downtime, which may be caused by the failure of database, ranges from a minor inconvenience to an inability to perform organization's critical tasks with resulting loss in productivity, revenue, and even customers and market share. One survey on downtime reported industry average numbers of $80,000 per hour, four hours average downtime and nine occurrences per year for a loss of nearly $3 million per organization per year. [24]

3.2.3.3 FAULT TOLERANT SYSTEM

Moreover, the requirements must involve a good designed fault tolerant information system, which allow applications to continue processing without impacting the user, application, network, or operating system in the event of a failure. [25] Redundancy of components is usually implemented to provide continuous processing in the event of a component failure. Mission critical applications such as data servers and network servers need a higher level of fault tolerance, these systems must satisfy the following requirements:

1. The system must uniquely identify any single error or failure;
2. The system must be able to isolate the failure and operate without the failed component;
3. The failed system must be repairable while it continues to perform its intended function;
4. The system must be able to be restored to its original level of redundancy and operational configuration.

In short, single points of failure must be minimized in the fault tolerant information systems. Similarly, physical facilities must be duplicated as redundancies for the disaster recovery planning. Using alternative power sources and RAID disk subsystems to protect the system from being brought down by the failure of either a disk drive or power supply may be a good option.

3.2.3.4 MONITORING SYSTEM

Besides, a monitoring system that provides continuous monitoring of critical equipment and assets should be implemented. This monitoring system will receive alarms at a response center where an operator follows a predetermined set of instructions to notify responsible individuals. [31]

To this end, the requirements of the strategies in disaster recovery planning are:

1. Preventing Data Losses
2. Minimizing Network Downtime typically from the fault of database
3. Well Designed Fault Tolerant System equipped with supportive facilities and administrators
4. Monitoring System considering the risks being analyzed