PROPOSAL OF DISASTER RECOVERY PLAN

Universiti Teknologi Malaysia

PROPOSAL OF DISASTER RECOVERY PLAN

1.0 EXECUTIVE SUMMARY

A common occurrence problem in companies engaged in networking and security is that the infrastructure and devices used to store data are outdated. When I interviewed a database staff member, he told me that this problem made them more difficult and required more maintenance time. Besides, the second problem faced is high cost and unreliable human sources. Information technology (IT) is the company's most valuable asset, not only hardware but also software. Without well-maintained IT, companies will not be able to achieve optimal operations. That's because it requires high enough expense for maintenance, regular inspections to make the company's IT operating system run optimally, and these things usually absorb a large enough budget for the company (which may be an established company).That is not a big problem. In contrast, the startup company sees it as a fatal problem and may threaten their financial situation. Coupled with the lack of reliable human resources, this will increase the company's costs in providing staff training due to IT training does requires a lot of costs. Therefore, many companies have begun to open their doors to external IT outsourcing and maintenance.

Also, data security is the third IT problem most often faced by large companies. Even if large companies have their own data centers, they still consider various methods to prevent their company data from being lost, damaged, or hacked. One of the reasons IT companies are very vulnerable to be attacked as some companies use counterfeit or pirated software, especially companies that use Internet networks and do not have the latest security system protection, may cause leakage data or cyberattack.Therefore, companies engaged in the IT field (especially the network and security field) must carry out regular maintenance. Not only that, the problem that large companies may face at any time is the existence of disasters. These disasters are natural disasters and disasters caused by a human fault (human error). In other words, companies are not hacked by hackers but because of their IT technical errors or natural disasters that cause damage to the company. These disasters not only affect the company's data but also causing an effect on computer networks and internet networks. These disasters are not allowed in resulting the company's IT activities paralyzed, especially since the company involves the lives of many people, such as companies engaged in telecommunications, banking, media, and other sectors. In short, these companies should have disaster recovery capabilities. Therefore, when facing any disaster, the company can speed up recovery and ultimately suppress the company's budget.

2.0 PROJECT BACKGROUND

The increase in the number of unplanned incidents such as natural disasters, power outages, cyberattacks, and other disruptive events has made it difficult for IT companies to deal with them. So, we created this IT recovery and services project to help companies in a hard time dealing with these things, especially for small companies.

3.0 OBJECTIVES OF THE PROJECT

The purpose of designing a disaster recovery plan is to minimize downtime and data loss. Our motto is to protect the company under any circumstances (especially when the computer operation and service are improper). There are many other goals, such as:

i. Reduce Overall Risk

The primary goal of a disaster recovery plan is to reduce the company's overall risk. Therefore, our disaster recovery plan is concise but complete. It will identify all loopholes that may jeopardize your company. So, ensuring that your company returns to a fully operational state after the sudden disaster.

ii. Maintain

The disaster recovery plan that is prepared by us has already undergone a few tests and is full of the current scale. That means it willhelp your company to recover rapidly when encountering the problem. In short, the company's disaster recovery plan will be reviewed and maintained annually by our team to ensure that new aspects of the business are covered, and the plan has to be examined at least every two years.

iii. Presenting to owner and investor

Once developed and tested, we will present our disaster recovery plan to the owner and board of directors and record any feedback to ensure all the useful comments are covered in the revised plan.

iv. Comply with regulations

This is a customized disaster recovery plan. We will consider all government regulations to ensure that your company can operate normally without violating any government regulations.

v. Rapid response

Our disaster recovery plan is written and developed to respond quickly to any disasters. It is particular for your company only. As mentioned, time is your greatest enemy after the disaster

attacks, so we make sure copies of your plan for recovery are stored electronically and hard copies. Therefore, you can access it every day. Within reach of any hour of the day or night.

4.0 TEAM MEMBERS

The following are the roles needed to build our disaster recovery company or team

i. Project manager
Creating a comprehensive continuity plan and a continuous process and will also be responsible for managing schedules and budgets.

ii. Crisis Management Team
This team will be led by organization's Chief of Operations (COOP). It will consist of the senior executive and they will be responsible for making all critical decisions regarding the response to a crisis.

iii. Administrative Support Team
The team will be led by the head of the organization's administration and is made up of staff representatives of facilities, human resources, and administrative supporters. Their primary responsibility is to provide constant support to crisis management teams and other teams especially when the restoration process requires initiation.

iv. Damage Assessment Team
The team is responsible for initial damage assessment activities have on the structures, environmental support equipment, computer hardware, software, data communication capabilities, and other special equipment.

v. Recovery Coordination Team
The team is important to coordinate all activities and communication between the technical area and the user area. This team will assist the crisis management team with a detailed plan or in formulating alternative actions if needed.

vi. Human Resource Support Team
They are here to quickly deal with all issues related to employees in the organization, and if needed, they can add additional temporary staff, start the home treatment center plan, and coordinate with company insurance and legal representatives.

vii. Site Restoration Team
This team will follow the damage assessment team to see if rescue operations are possible, and coordinate efforts to return the business unit and technology group/operation to a primary or alternative permanent location.

viii. Transportation Support Team
This team will coordinate accommodation for personnel as well as for the shipments of equipment and supplies, as well as prints if necessary, at alternative locations. This group will also facilitate food shipments for alternative locations if needed.

ix. System Restoration Team

This team will help restore the wired and wireless network infrastructure.

5.0 DETAILS OF PROPOSED ACTIVITIES/SOLUTIONS

The 11 September 2001 attacks on the World Trade Center indirectly raised awareness and triggered revisions to the DR planning approach. And specific disaster recovery procedures for each time-critical IT system must be developed by a team with expertise in a specific business and technical environment. So, we will start by dividing the team and reviewing the personnel who will join, which will take 1-2 days, then we will start looking for investors and presenting our project, which will take 1 week. Next, we will start buying the required inventory, which will take 3 days. Then we will start advertising and marketing our services, until an indefinite time. And if someone needs our services, we will immediately start the project.

6.0 EXPECTED DELIVERABLES

It is hoped that our project can be useful for IT companies that need our services and can provide the best service we can provide for companies that need our services, and our project will be the best in the field of disaster recovery.

7.0 EXPECTED IMPACTS

We hope that our project can create a good impression on companies and groups. This is because the requirements for disaster recovery plans are increasing in our market and more and more companies need disaster recovery services as protection for their companies. Therefore, our project will be one of the best investments for its company in the future, in which we will provide customers with the best services to win the trust of customers, and they are satisfied with our services. Also, we always expand the scope of the market to include higher profits and train and develop the talents of new workers who will be successors to future projects, because this is the company's most valuable asset, that is, young talents.

8.0 RISKS

There are a lot of risks and mistakes that may occur involved in our project, such as:

i. Failure To Identify and Understand Dependencies in Both Help and Restoration
IT faces the challenge of meeting the growing expectations of the latter user to access critical applications while managing increasingly complex infrastructure.

ii. Shortage of Understanding of Software Compatibility Issues
Many software compatibility issues can make data can not be covered. Conflicting software can cause the recovery to fail. Resolving these errors can be tricky, requiring hours of troubleshooting to identify and fix the errors.

iii. Inadequate testing
Time and resources are urgently needed to conduct disaster recovery testing. Recovery testing can be expensive and deprive valuable IT resources of value-added activities.

iv. A Miscariage to Protect Against Corrupted Data and Malwave

There are multiple backups of data damages that could lead to recovery failures - solar flares that are suddenly extinguished, XFS system problems and files, to multiple hardware failures and human errors. Failure to detect malware in the backup environment continues to be one of the most common causes of disaster recovery failure.

vi. Failure to follow media management best practices
One of the most common reasons why the seemingly perfect reserves could not be recovered was the mishandling of the backup media or archivist - tape, removable hard drives, etc. Though tape and discs media are relatively low in technology, they are highly manual and require disciplined compliance with best practices. Simple human error such as lack of recording or archive drives can make recovery impossible.

9.0 SUMMARY

Nowadays, infrastructure is an increasingly complex combination of virtual structures, structures, clouds, and environments. Protecting a critical operation running in this environment requires fundamental changes from a server level backup to planning that centers on holistic restoration. By determining and working from an understanding of the disaster recovery needs of the entire infrastructure, it can save time, reduce critical risk, and eliminate the failure of nightmare recovery.