Computer Security - Disaster Recovery

Disaster recovery is generally a planning process and it produces a document which ensures businesses to solve critical events that affect their activities. Such events can be a natural disaster (earthquakes, flood, etc.), cyber–attack or hardware failure like servers or routers.

As such having a document in place it will reduce the down time of business process from the technology and infrastructure side. This document is generally combined with Business Continuity Plan which makes the analyses of all the processes and prioritizes them according to the importance of the businesses. In case of a massive disruption it shows which process should be recovered firstly and what should be the downtime. It also minimizes the application service interruption. It helps us to recover data in the organized process and help the staff to have a clear view about what should be done in case of a disaster.

Requirements to Have a Disaster Recovery Plan

Disaster recovery starts with an inventory of all assets like computers, network equipment, server, etc. and it is recommended to register by serial numbers too. We should make an inventory of all the software and prioritize them according to business importance.

An example is shown in the following table –

Systems	Down Time	Disaster type	Preventions	Solution strategy	Recover fully
Payroll system	8 hours	Server damaged	We take backup daily	Restore the backups in the Backup Server	Fix the primary server and restore up to date data

You should prepare a list of all contacts of your partners and service providers, like ISP contact and data, license that you have purchased and where they are purchased. Documenting all your Network which should include IP schemas, usernames and password of servers.

Preventive steps to be taken for Disaster Recovery

- The server room should have an authorized level. For example: only IT personnel should enter at any given point of time.
- In the server room there should be a fire alarm, humidity sensor, flood sensor and a temperature sensor.

These are more for prevention. You can refer the following image.

Fire Sensor

Temperature and Humidity

Flood sensor

- At the server level, RAID systems should always be used and there should always be a spare Hard Disk in the server room.

- You should have backups in place, this is generally recommended for local and off-site backup, so a NAS should be in your server room.
- Backup should be done periodically.
- The connectivity to internet is another issue and it is recommended that the headquarters should have one or more internet lines. One primary and one secondary with a device that offers redundancy.
- If you are an enterprise, you should have a disaster recovery site which generally is located out of the city of the main site. The main purpose is to be as a stand-by as in any case of a disaster, it replicates and backs up the data.