UNIT II

PEOPLE MANAGEMENT-HUMAN RESOURCE SECURITY

Disaster management

What Is a Disaster Recovery Plan?

- Disaster recovery plan is an organization's set of procedures and responsibilities in the event of an unforeseen disaster such as a ransomware attack or equipment damage.
- For example, event of ransomware attack, your disaster recovery plan will help your organization improve recovery time to resume daily business operations.
- Disaster recovery plan usually is organized by type of disaster, and has instructions thatcan be easily followed by anyone within the organization.
- Instructions should be accessible without specialized department knowledge or training.

The benefits of having a strong disaster recovery plan include:

- Reduced financial and reputational losses from an unplanned attack
- Reduced interruption of daily operations
- Internal staff trained in emergency procedures
- Quick return of services to endpoint users

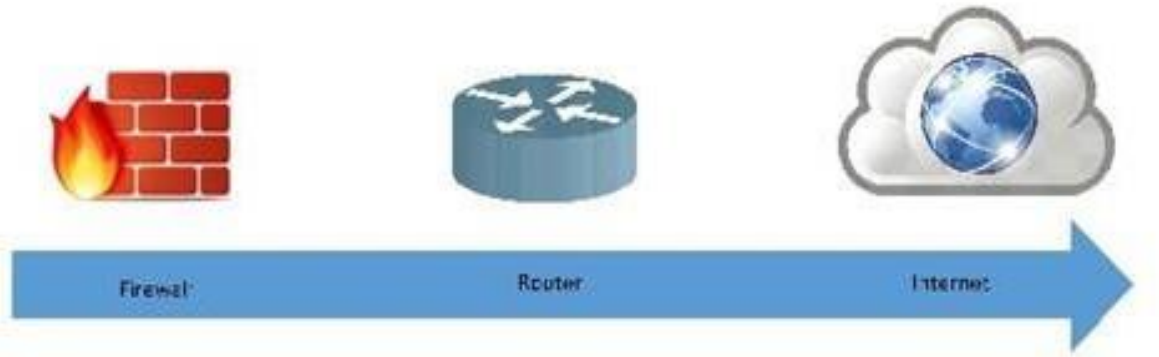
Requirements to Have a Disaster Recovery Plan

- 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
Payroll system	8 hours	Server damaged	We take backup daily	Restore the backupsin the Backup Server

- 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.

- Devices that Help us with Network Security
- Firewalls − They can be software or applications which operate at the network level.
- They protect Private networks from external users and other networks. Generally, they are a compound of programs and their main function is to monitor the traffic flow from outside to inside and vice versa.
- Their position is generally behind a router or in front of the router depending on the network topologies.



What Is an Incident Response Plan?

- An incident response plan is an organization's set of procedures and responsibilities in the event of a cyber-related disruption such as a phishing attack or a data breach.
- plan will help your incident response team reduce company-wide downtime.

A thorough incident response plan will address the following:

- Actions and procedures for each step of response to an incident
- Each department's roles and responsibilities
- Key stakeholders who act as leadership during an incident
- A communication plan for the incident response team and other departments
- Guidance on any legally required disclosure to the public or regulatory authorities
- Metrics for capturing the effectiveness of the incident response
- An incident response plan should also include a business impact analysis.
- A business impact analysis identifies which business operations could be disrupted by an incident and what the overall effect on the organization would be.
- This analysis can help you to prioritize which business processes require the most resources for resuming operations the fastest.