Step 8: Recovery

Objectives:

At the end of this episode, I will be able to:

Understand what recovery is.

Explain what Step 8, Recovery, of the IH&R process is.

Identify what the process flow for Recovery should be for the IH&R team.

Define the actions that should be taken during recovery by the IH&R team.

External Resources:

Step 8 Recovery

What is the process flow for Recovery? -

1. After eliminating the root cause(s) of the incident from all the systems and resources, the IH&R team must restore the affected systems, services, resources, and data through recovery.

2. The IH&R team will check to determine what data was lost/affected, and restore it completely from backup media.

3. The IH&R team must take steps to ensure that the backup(s) do not have traces of malware or attack vectors before restoring.

4. After recovering all the lost data, IH&R team must restart all the processes, services and systems that were affected.

The actions to be performed in recovery stage are:

```
▪ Rebuilding the system by installing a new O/S
▪ Restoring user’s data from trusted backups
▪ Examining the protection and detection methods
▪ Examining security patches and system logging information
```

What are Recovery / Remediation Plans? -

Recovery plans are developed for specific departments within an organization to allow them to recover from incidents.

The purpose of recovery planning is to prepare an organization to survive in the event of an incident and continue its normal business operations.

Recovery planning is required for the following reasons:

```
▪ Helps to ensure critical business operations continue during and after an
```

incident
▪ Facilitates making quick and effective decisions during an incident
▪ Identifies and prioritizes the important business and support functions
▪ Provides effective supervision of recovery tasks
▪ Protects confidential information of an organization