Step 4: Notification

Objectives:

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

Understand what the process flow for notification is.

Explain what Step 4, Notification, of the IH&R process is.

Identify what information elements/items should be communicated about the incident as part of the notification phase.

Define what methods can be used for secure communication between IH&R team members.

External Resources:

Step 4 Notification

What is the process flow for notification? -

Communication plays a major role in swiftly responding to an incident. It helps in reducing the impact of an incident by facilitating better coordination between different stakeholders.

Incident handlers must communicate the severity of an incident to management in order to secure approval for performing incident response procedures.

Communications should include the initial processes performed to assess the situation, detection methods applied, impacted resources, and management strategy.

NOTE: The IH&R team may need to discuss the incident with the organization's legal representative to file a lawsuit against the perpetrators, if necessary.

Incident handlers may also need to communicate with an external party after approvals from management if they need external support for handling the incident.

After controlling and mitigating the incident, the incident response team can disseminate the details of the incident and lessons learned throughout the organization to create/raise awareness.

Who ya' gonna call? -

The IH&R team should have a list of contacts who have a role to play in the incident response process.

They must notify all these contacts after classifying and prioritizing the incident to gain permission and perform other incident response functions as needed.

What are you gonna tell 'em ? -

The IH&R team should communicate the following details about the incident, as they will help with containment and eradication:

```
▪ Impact on business and services
▪ Scope of attack including the resources, accounts, devices, and other
components compromised
▪ Information /data at risk
▪ Level of incident severity
▪ Urgency for recovery
▪ Resources available
▪ (Exact) time of detection for incident activity
▪ Network location of the activity
▪ Attack vectors and source(s)
▪ Vulnerabilities or configuration flaws exploited
▪ Indicators of Compromise (IoCs)
▪ Methods used for detection
▪ Suggestions regarding containment and eradication
```

How are you gonna tell 'em? -

During the incident response process secure communication between different teams is essential.

```
▪ Secure Communication Channels
▪ Out-of-Band Communication Channels
```