Ch.11 summary By @MHazazi

What Is an Incident?

- Incident preparedness includes having **policies**, **strategies**, **plans**, and **procedures**
- IS incident is an adverse event that threatens business security and/or disrupts service
- Every organization should be prepared to respond to the following attacks:

1) Intentional unauthorized access or use
Occurs when an insider or an intruder gains logical or physical access without permission

2) Denial of service (DoS) attacks
Prevents normal authorized functionality of the organization's networks, systems, application

3) Malware
Code that is secretly inserted into program with the intent of gaining authorized access or causing harm

4) Inappropriate usage
Occurs when authorized user performs actions that violate company policy, agreement, law, or regulation

Incident Severity Levels

	Level 1	Level 2	Level 3
Explanation	cause significant harm to the business, customers, or the public	unauthorized access to noncritical systems or information	situations that can be contained and resolved by the information system custodian, data/process owner, or HR personnel
Response Time	Immediate	Within 4 hours.	Within 24 hours
Internal Notification	CEO COO CISO Legal counsel Designated incident handler	COO CISO Legal counsel Designated incident handler	CISO Designated incident handler
Examples	- compromise of protected customer information. - Theft or loss of device contains protected information. - DOS	- Inappropriate access to legally protected or proprietary information. - Malware detected on multiple systems. - Warning signs and/or reconnaissance detected related to a potential exploit. - Notification from a third party of an imminent attack	- Malware detected and/or suspected on a workstation or device, with no external connections identified. - User access to content or sites restricted by policy. - User's excessive use of bandwidth or resources.

How Are Incidents Reported

- Employees report all actual and suspected incidents
- The employee who discovers an incident may not be trained or an IT technician
- Company encourage employee to report anything

What Is an Incident Response Plan

- Composed of policies, plans, procedures, and people
- **incident response plan (IRP)** is a roadmap of reporting, responding, and recovery actions
- Incident response procedures are detailed steps needed to implement the plan
- **IRP Activities:**

1. **Preparation**
   developing internal incident response capabilities, establishing external contracts and relationships, defining legal and regulatory requirements, training personnel, and testing plans and procedures

2. **Detection and investigation**
   establishing processes and a knowledge base to accurately detect and assess precursors and indicators

3. **Initial response**
   incident declaration, internal notification, activation of an incident response team, and/or designated incident handlers, and prioritization of response activities

4. **Containment**
   steps necessary to prevent the incident from spreading, and as much as possible limit the potential for further damage

5. **Eradication and recovery**
   elimination of the components of the incident

6. **Notification**
   notify state and federal agencies, affected parties, victims, and the public-at-large

7. **Closure and post-incident activity**
   incident recap, information sharing, documentation of “lessons learned,”

8. **Documentation and evidence-handling requirements**
   recording of facts, observations, participants, actions taken, forensic analysis, and evidence chain of custody

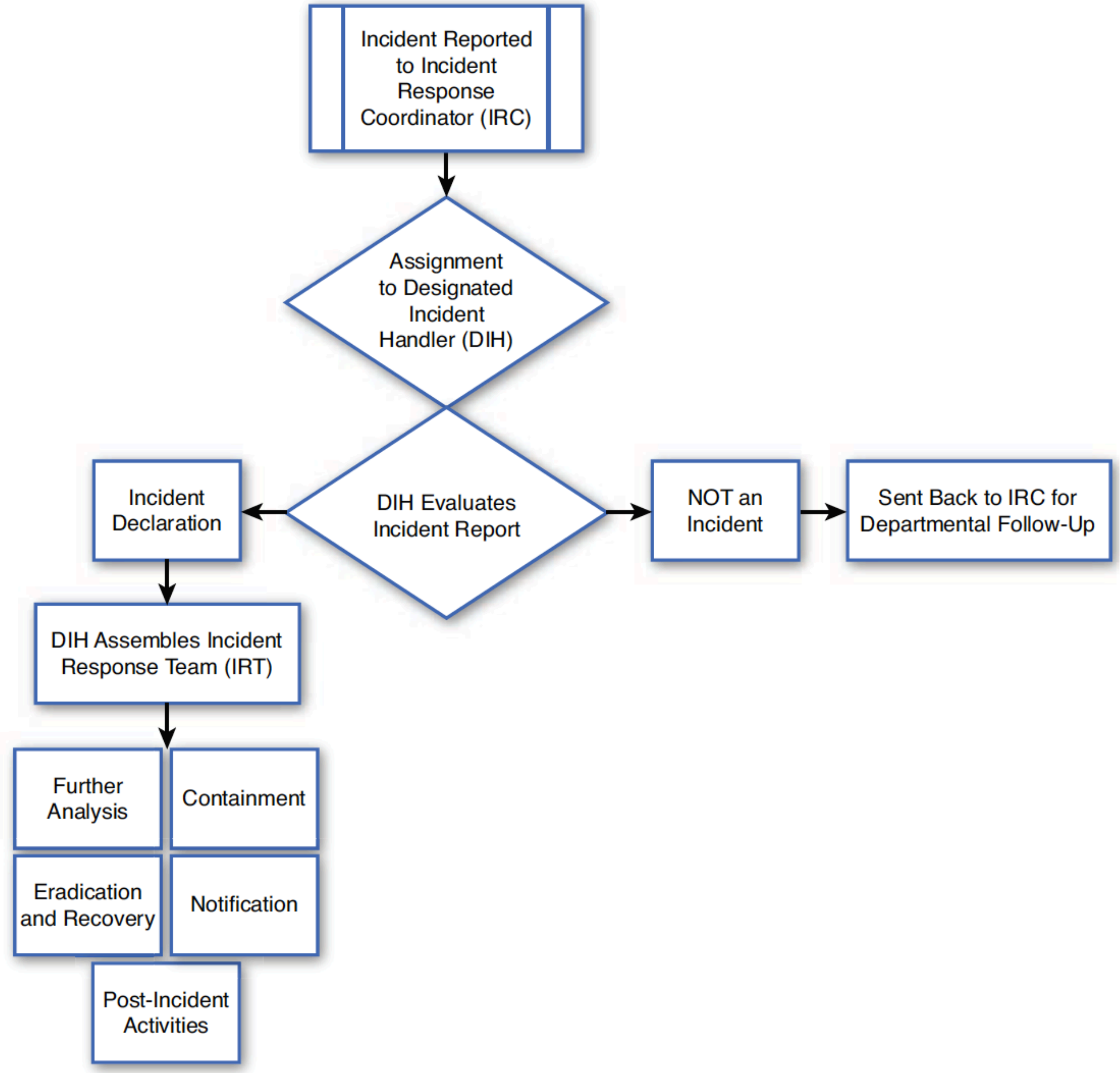
Key Incident Management Personnel

- **Incident response coordinator (IRC)**
  - Central point of contact for all incidents
  - Verifies and logs the incident

- **Designated incident handlers (DIHs)**
  - Senior-level personnel who have crisis management and communication skills, experience, and knowledge to handle an incident

- **Incident response team (IRT)**
  - Trained team of professionals that provide services through the incident lifecycle

- **incident response roles and responsibilities.**


Incident Reported to Incident Response Coordinator (IRC)
Assignment to Designated Incident Handler (DIH)
DIH Evaluates Incident Report
Incident Declaration
NOT an Incident
Sent Back to IRC for Departmental Follow-Up
DIH Assembles Incident Response Team (IRT)
Further Analysis
Containment
Eradication and Recovery
Notification
Post-Incident Activities

Investigation and Evidence Handling

- Incidents should be thoroughly documented

- Depending on the incident it may be necessary to contact local, state, or federal law enforcement
  - The IRT team should be acquainted with applicable law enforcement representatives

- Incident handlers that perform forensic analysis should be familiar with forensic principles, guidelines, procedures, tools, and techniques

- **The process of digital forensic includes:**
  - Collection = identify, label, record, and acquire data from the possible sources of relevant data
  - Examination = forensically processing large amounts of collected data to get particular data
  - Analysis = analyze the results of the examination
  - Reporting = reporting the results of the analysis

- Chain of custody applies to physical, digital, and forensic evidence
  - It is used to prove that evidence has not been altered

- Evidence should be stored in a secure location

Data Breach Notification Requirements

- **Federal requirements that address the protection of personally identifiable information (PII)**
  - Gramm-Leach- Bliley Act (GLBA)
  - Health Information Technology for Economic and Clinical Data Act (HITECH)
  - The Federal Information Security Management Act (FISMA)
  - Federal Education Rights and Privacy Act (FERPA)