INCIDENT AND INCIDENT RESPONSE METHODOLOGY

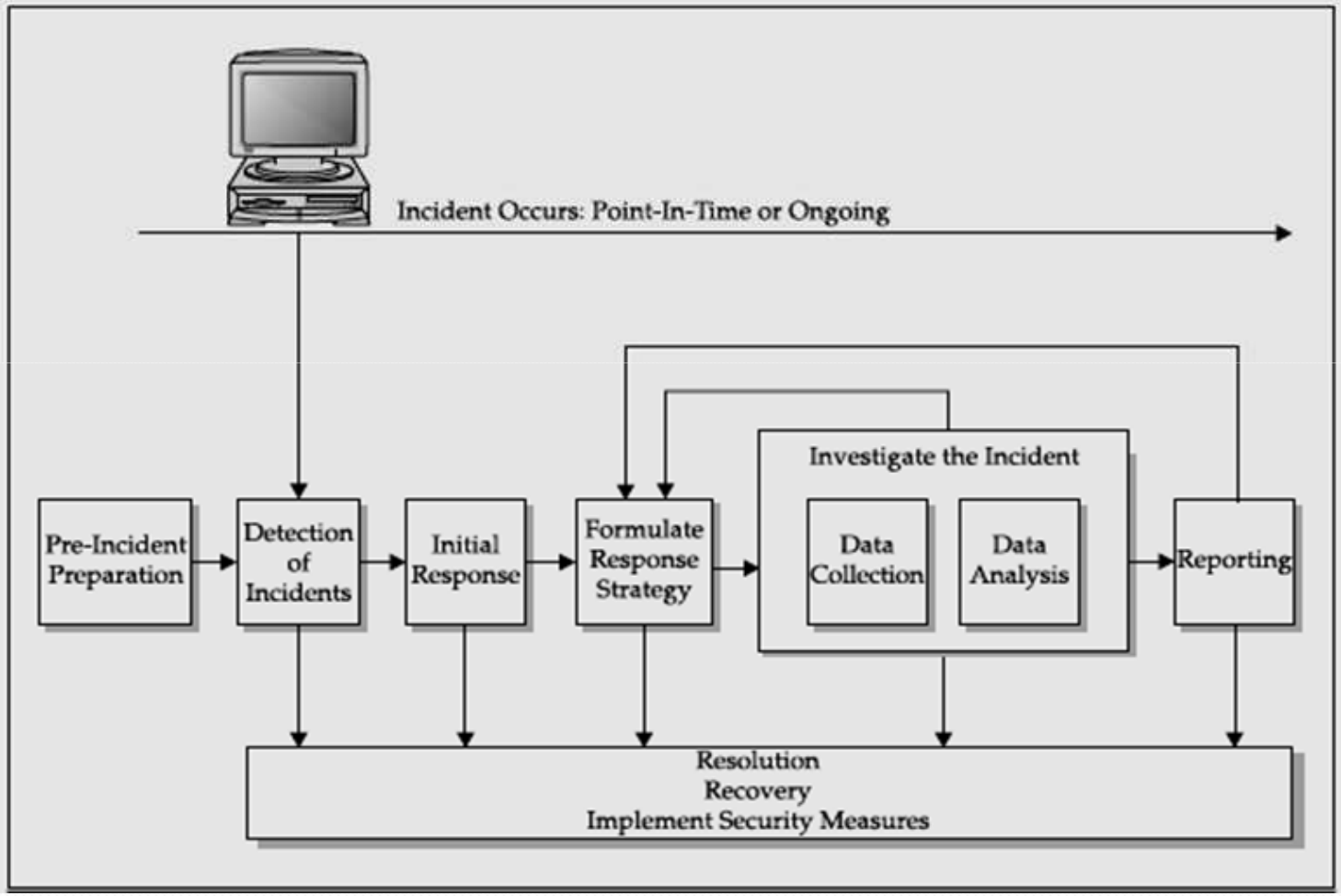
WHAT IS A COMPUTER SECURITY INCIDENT

- *Any unlawful, unauthorized, or unacceptable* action that involves a computer system or a computer network
- Events
  - Theft of trade secrets
  - Email spam or harassment
  - Unauthorized or unlawful intrusions into computing systems
  - Embezzlement
  - Possession or dissemination of child pornography
  - Denial-of-service (DoS) attacks
  - Tortious interference of business relations
  - Extortion
  - Any unlawful action when the evidence of such action may be stored on computer media such as fraud, threats, and traditional crimes

Incident Response Methodology

- Seven major components of incident response:
  - **Pre-incident preparation**
  - **Detection of incidents**
  - **Initial response**
  - **Formulate response strategy**
  - **Investigate the incident**
  - **Reporting**
  - **Resolution**

Incident Response Methodology



Components of incident response

Incident Response Methodology

- **Pre-incident preparation**
- It is necessary for successful incident response.
- Necessary actions need to be taken to prepare an organization and CSIRT before an incident occurs.
- Computer Security Incident Response Team (CSIRT)
- Incident response is reactive in nature
- Pre-incident preparation is only a proactive measure
- Preparation will involve obtaining the necessary tools, developing techniques to respond to incident and taking actions on the systems and networks that will take part during an incident.

Incident Response Methodology

- **Pre-incident preparation**
  - **Preparing the Organization**
    - It involves developing strategies that will be employed by organization for incident response
      - Host-based security measures implementation
      - Network-based security measures implementation
      - End users training
      - Employing an intrusion detection system (IDS)
      - Strong access control
      - Timely vulnerability assessments
      - Taking backups on a regular basis

Incident Response Methodology

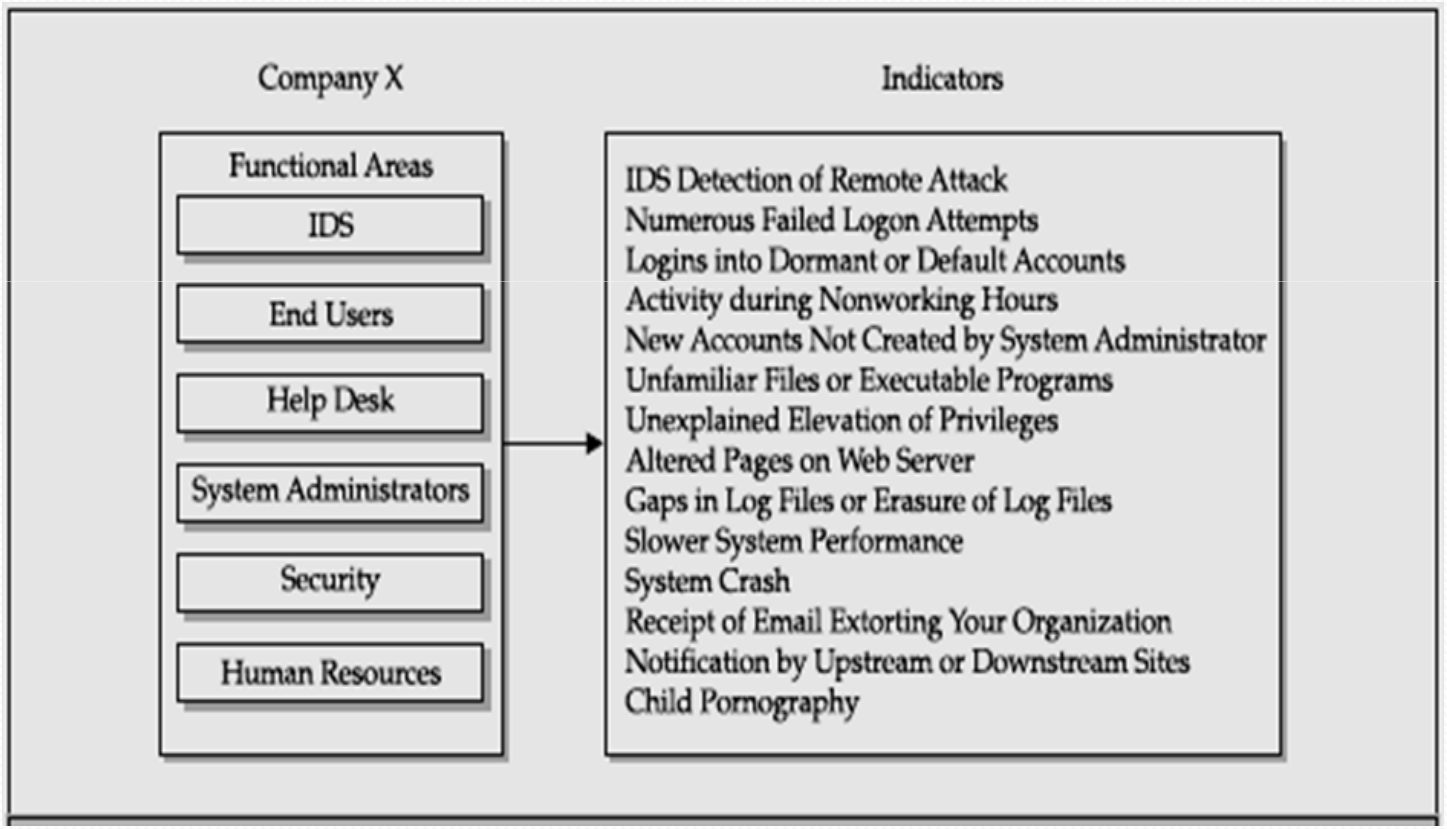
- **Pre-incident preparation**
  - **Preparing the CSIRT**
    - The hardware/ software/ documentation needed to investigate computer security incidents must be collected
    - Policies and operating procedures to implement response strategies must be framed
    - Employees need to be trained for incident response

Incident Response Methodology

- **Detection of incidents**
- Detection is very important for successful response.
- It is one of the most decentralized phases
- It is identified when someone suspects that an **unauthorized, unacceptable, or unlawful event** has occurred in an organization
- Incident occurred may involve an organization's computer networks or data-processing equipment**.**
- It is necessary to prepare initial response **checklist** to make sure to record facts.

Incident Response Methodology

- **Detection of incidents**



Incident Response Methodology

- **Initial Response**
- Initial investigation starts at this phase.
- It involves assembling the CSIRT, collecting data, determining the type of incident and assessing the impact.
- It documents the steps that must be taken to prevent reactions and panic when an incident is detected.
- It helps to implement a methodical approach.
- Data is collected without touching the system.

Incident Response Methodology

- **Initial Response**
- Task to be performed for data collection are Interviewing system administrators/business unit personnel, reviewing intrusion detection reports and network-based logs to identify an incident has occurred and reviewing the network topology and access control lists.
- IR team must verify that an incident has actually occurred or not, which systems are directly or indirectly affected which users are involved, potential business impact and initiate network monitoring. Information collected in this phase is used to begin the next phase, developing a response strategy.

Incident Response Methodology

- **Formulate a Response Strategy**

- The main goal of this phase is to *determine the best response* strategy *for an incident*. *I*t should consider the political, technical, legal, and business factors that surround the incident. Appropriate response strategy *must be selected and management approval needs to be obtained.*
- **Considering the Totality of the Circumstances**
- **Considering Appropriate Responses**

Incident Response Methodology

- **Formulate a Response Strategy**
  - Taking Action
  - Organization need to take disciplinary action against an employee or respond to a malicious act by an outsider. Action can be filing civil or criminal complaint, or.
    - Legal Action
      - File a civil complaint
      - Notify law enforcement
    - Administrative Action
      - Disciplining or terminating employees by any actions like letter of reprimand, immediate dismissal, mandatory leave, reassignment of job duties, temporary reduction in pay or withdrawal of certain privileges.

Incident Response Methodology

- **Investigate the incident**
- Investigator performs a thorough collection of data.
- Then review the data collected to determine what / when / where the incident happened, who did it, how it can be prevented in the future. Investigation is conducted by reviewing host-based evidence, network-based evidence and evidence gathered via traditional, nontechnical investigative steps

Incident Response Methodology

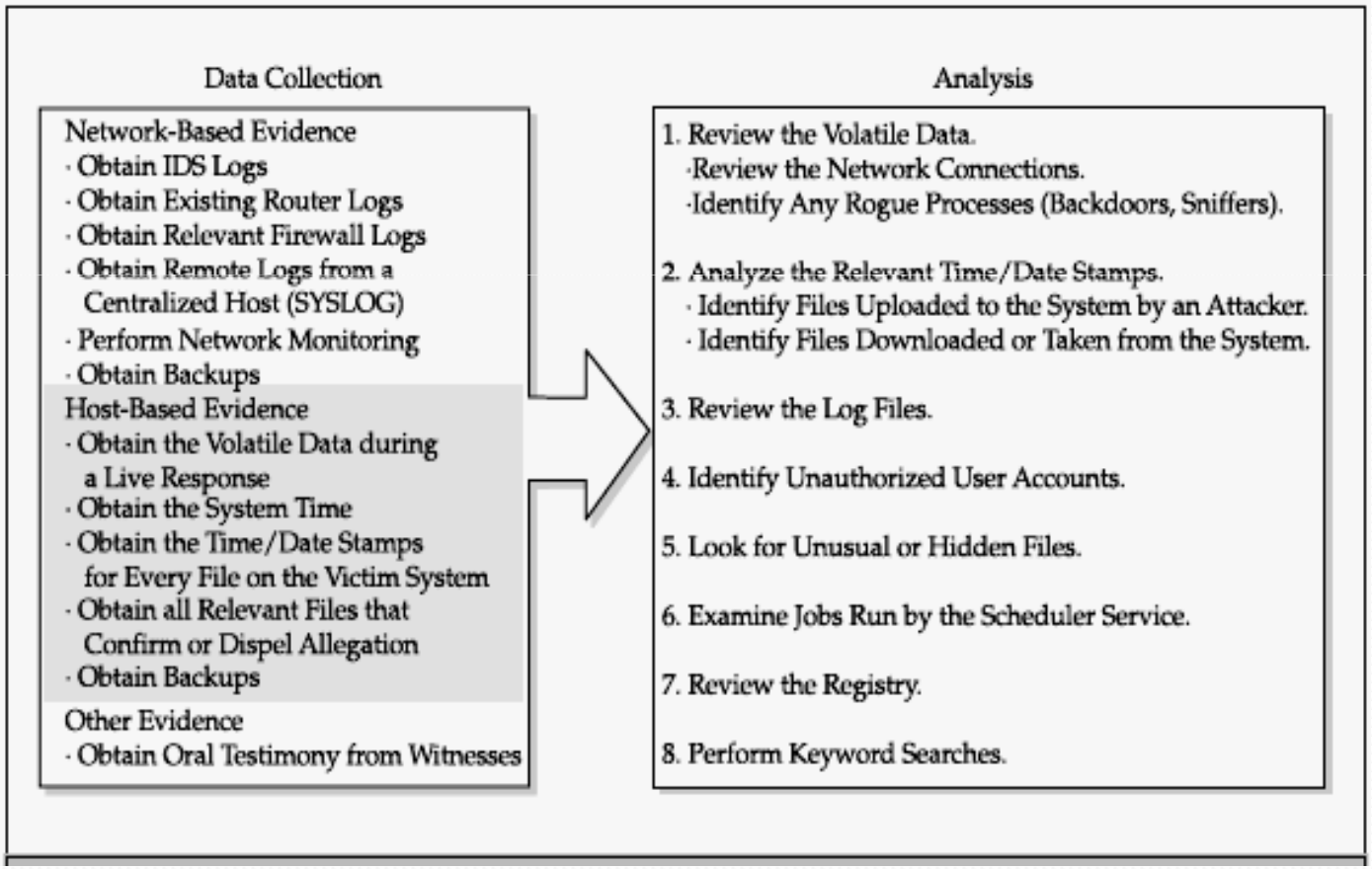
- **Investigate the incident**
- People cause incidents using things to destroy, steal, access, hide, attack, and hurt other things. Key task of the investigator is to determine which things were harmed by which people.
- This is difficult more difficult in computer crime as people are using encryption, steganography, anonymous email accounts, fakemail, spoofed source IP addresses, spoofed MAC addresses, masquerading as other individuals, and other means to mask their true identity.
- This makes identifying the attacker a time consuming task.

Incident Response Methodology

- **Investigate the incident**
-
- Investigation can be divided into two phases:
  - **Data collection**
  - **Forensic analysis**
-

Incident Response Methodology

- **Investigate the incident**



Incident Response Methodology

- **Reporting**
- Create reports that accurately describe the details of an incident. Report should be understandable to decision makers, must withstand legal scrutiny, produced in a timely manner.
- Guidelines to for reporting phase:
  - Document immediately
  - Write concisely and clearly
  - Use a standard format
  - Use editors

Incident Response Methodology

- **Resolution**
- The goal is to implement host-based, network-based, and procedural countermeasures. To prevent an incident from causing further damage and to return organization to a secure, healthy operational status.