Understanding Information Security Incidents

- Information Security Incidents: a network or host activity that impacts the security of information stored on network devices or systems with respect to confidentiality, integrity, and availability.
- Information Security Incident Types:
  - Malicious code or Insider threat Attacks: generated by malicious programs such as viruses, Trojan horses, and worms.
  - Unauthorized Access: refers to the process of obtaining illegal access to systems or network resources to steal or damage information.
  - Unauthorized Usage of Services: an attacker uses another user's account to attack the system or network.
  - Email-based Abuse: an attacker creates a fake website mimicking a legitimate website and sends website links to users to steal sensitive information such as user credentials, bank account details, and credit card details.
  - Espionage: involves stealing proprietary information of any organization and passing it to other organizations with the motive of negatively impacting the organization's reputation or for some financial benefit.
  - Fraud and Theft: involves theft or loss of assets or equipment that contains confidential information.
  - Employee Sabotage and Abuse: Actions performed by an employee to abuse computer systems include removing hardware or services of a system.
  - Network and Resource Abuses: an attacker uses a network and resources to obtain critical organization details, or in some scenarios make the network services or resources unavailable to legitimate users by flooding servers or applications with traffic.
  - Resource Misconfiguration Abuses: an attacker exploits resource misconfiguration such as vulnerable software configurations, open proxy

servers or anonymous FTP servers, misconfigured web forms or blog sites, and so on.

- Signs of an Incident: include the alerts, warnings, reports, complaints, and issues that represent an ongoing or completed security attack on an organization or its resources.
  - Precursor: indicate the possibility of the occurrence of a security incident in future.
  - Indicator: a sign representing that the incident has probably occurred or is currently in progress.
- Sources of Precursors and Indicators:
  - IDPS: used to detect suspicious events and log details related to the incidents, such as date and time of detection, type of incident, and source and destination IP addresses.
  - Security Incident and Event Management (SIEM) tools: similar to IDPS systems but collect the log data from multiple sources, analyze the log data, and generate alerts based on the analysis.
  - Antivirus/Antispam Software: detects malware, alerts administrators or users to it, and prevents it from infecting hosts.
  - File Integrity Checking Software: detects and alerts when critical system files are modified.
  - Third-Party Monitoring Services: as fraud detection systems, will notify an organization if any of the IP addresses or domain names belonging to the organization are misused to perform attacks on other organizations.
  - OS, Service, Network, and Application Logs: can be analyzed and correlated to detect suspicious events and generate alerts on security incidents.
- Cost of an Incident: refers to the sum of the total amount lost due to the attacks and the amount spent on recovering from the incidents
  - Tangible Cost: refers to the organization's direct expenditure due to an incident. Can be quantified and identified.
  - Intangible Cost: refers to expenditures that the organization cannot calculate directly or value accurately. Difficult to identify and quantify.