12.1.2 Incident Response Process Facts

This lesson covers the following topics:

- Security incident
- Incident response process

Security Incident

A security incident is an event or series of events that are a result of a security policy violation. The incident may or may not have adverse effects on an organization's ability to proceed with normal business. It is important to organizations that security incidents are recognized and dealt with appropriately. The following table describes types of security incidents.

Type	Description
Employee errors	Unintentional actions by an employee that cause damage or leave network systems vulnerable to attack.
Unauthorized act by an employee	Intentional actions by an employee to do harm to a company's network or data. Also known as an insider threat.
External intrusion attempts	Intentional actions by a threat actor who is not employed by or associated with an organization in an attempt to exploit attack vectors. The intent of the threat actor is to harm an organization or profit from access to an organization's resources.
Virus and harmful code attacks	Tools used by threat actors to disrupt company business, compromise data, or hurt the company's reputation
Unethical gathering of competitive information	This is also known as corporate espionage. The goal is to obtain proprietary information in order to obtain a competitive advantage or steal clients.

Incident Response Process

Incident response is the action taken to stop an incident in process, collect all data relative to an incident, and implement the appropriate response. An incident response process helps an organization to prevent additional damage from an incident, collect data to be used in the prosecution of the threat actor, and mitigate the damage of an incident. An incident response process should:

- Define what is considered an incident.
- Identify who should handle the response to the incident. This person is designated as the first responder.
- Describe what action should be taken when an incident is detected.
- Provide a detailed outline of steps to efficiently and effectively handle an incident while mitigating its effects.
- Explain how and to whom an incident should be reported.
- Explain when management should be notified of the incident and also outline ways to ensure that management is well-informed.
- Be legally reviewed and approved.

- Be fully supported by senior management and administration with appropriate funding and resources such as camera equipment, forensic equipment, redundant storage, standby systems, and backup services.