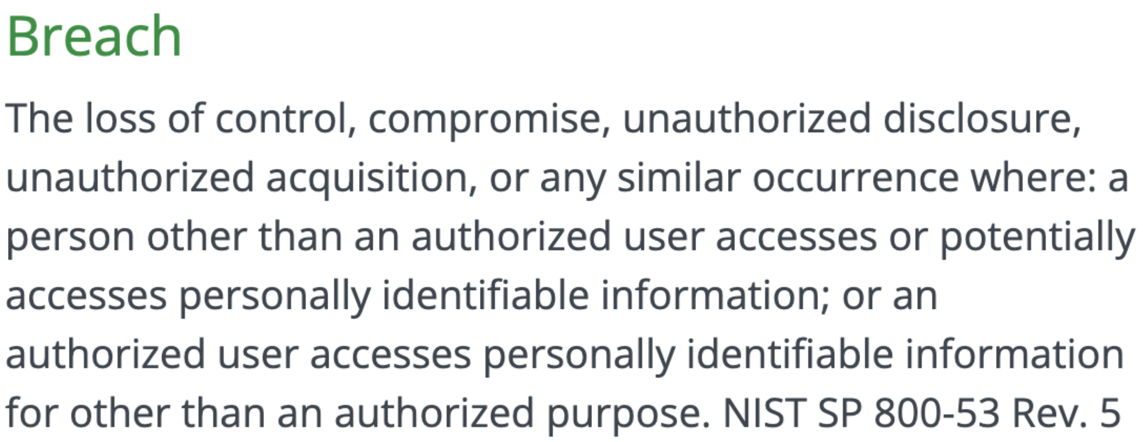
Cybersecurity Fundamentals

Module 2 : Incident Response, Business Continuity and Disaster Recovery Concepts

INCIDENT TERMINOLOGY : BREACH



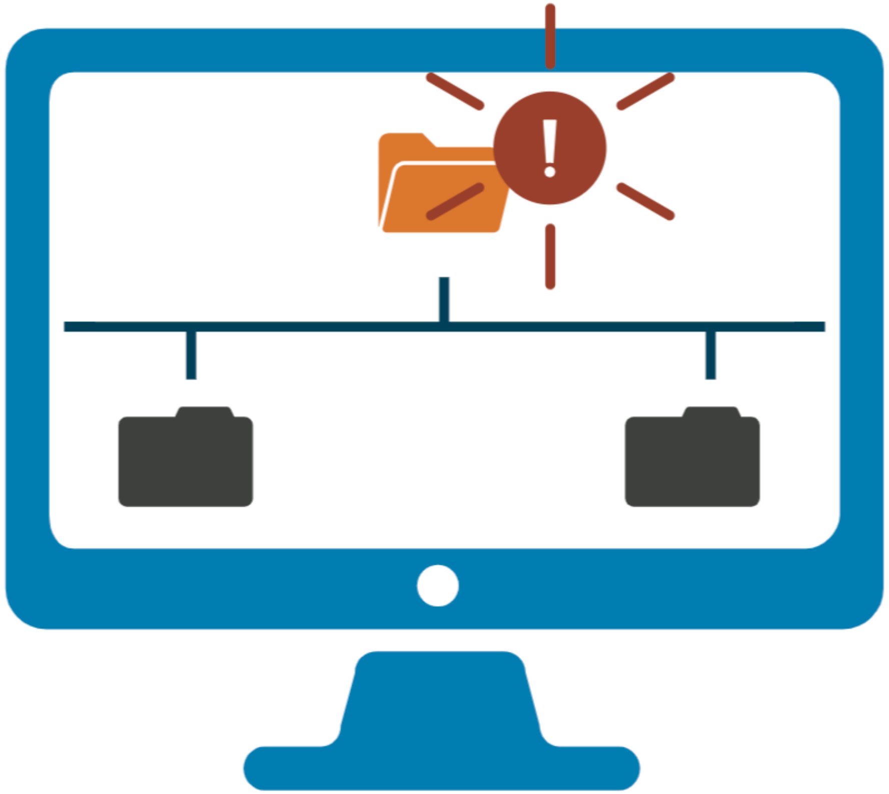
Breach

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses personally identifiable information; or an authorized user accesses personally identifiable information for other than an authorized purpose. NIST SP 800-53 Rev. 5

INCIDENT TERMINOLOGY : EVENT

Event

Any observable occurrence in a network or system. NIST SP 800-61 Rev 2



INCIDENT TERMINOLOGY : EXPLOIT

Exploit

A particular attack. It is named this way because these attacks exploit system vulnerabilities.

INCIDENT TERMINOLOGY : INCIDENT

Incident

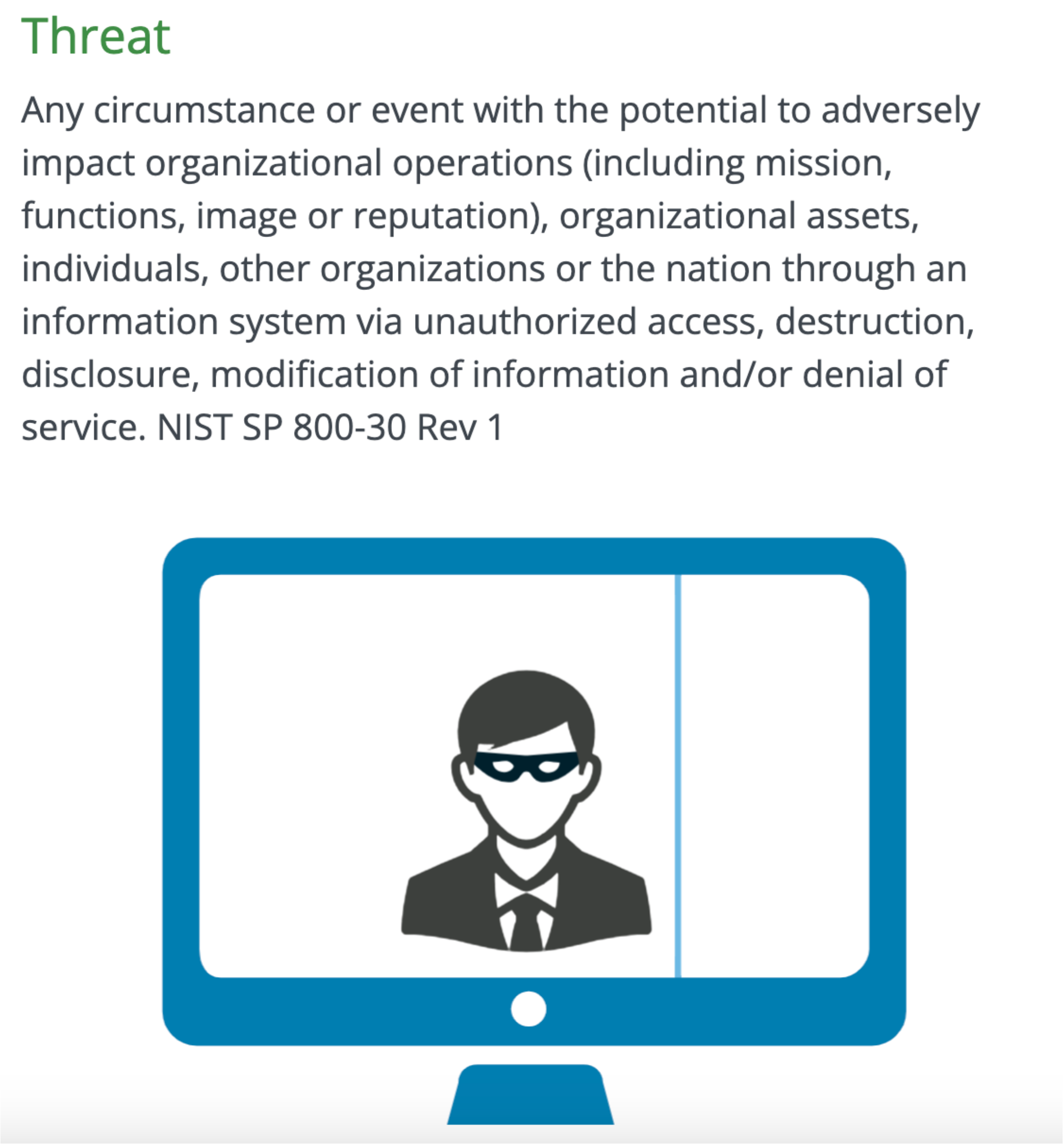
An event that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system or the information the system processes, stores or transmits.

INCIDENT TERMINOLOGY : INTRUSION

Intrusion

A security event, or combination of events, that constitutes a deliberate security incident in which an intruder gains, or attempts to gain, access to a system or system resource without authorization. IETF RFC 4949 Ver 2

INCIDENT TERMINOLOGY : THREAT



Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations or the nation through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service. NIST SP 800-30 Rev 1

INCIDENT TERMINOLOGY : VULNERABILITY

Vulnerability

Weakness in an information system, system security procedures, internal controls or implementation that could be exploited by a threat source. NIST SP 800-30 Rev 1

```
*****.***** = ******() {
  *** ***** = *****.***********('*****');
  **(****** === '*****/*******-******.***') {
    *********.***********('***','******/********.***');
  } **** {
    *********.***********('***','*****/******-****.***');
  }
}
```

INCIDENT TERMINOLOGY : ZERO DAY

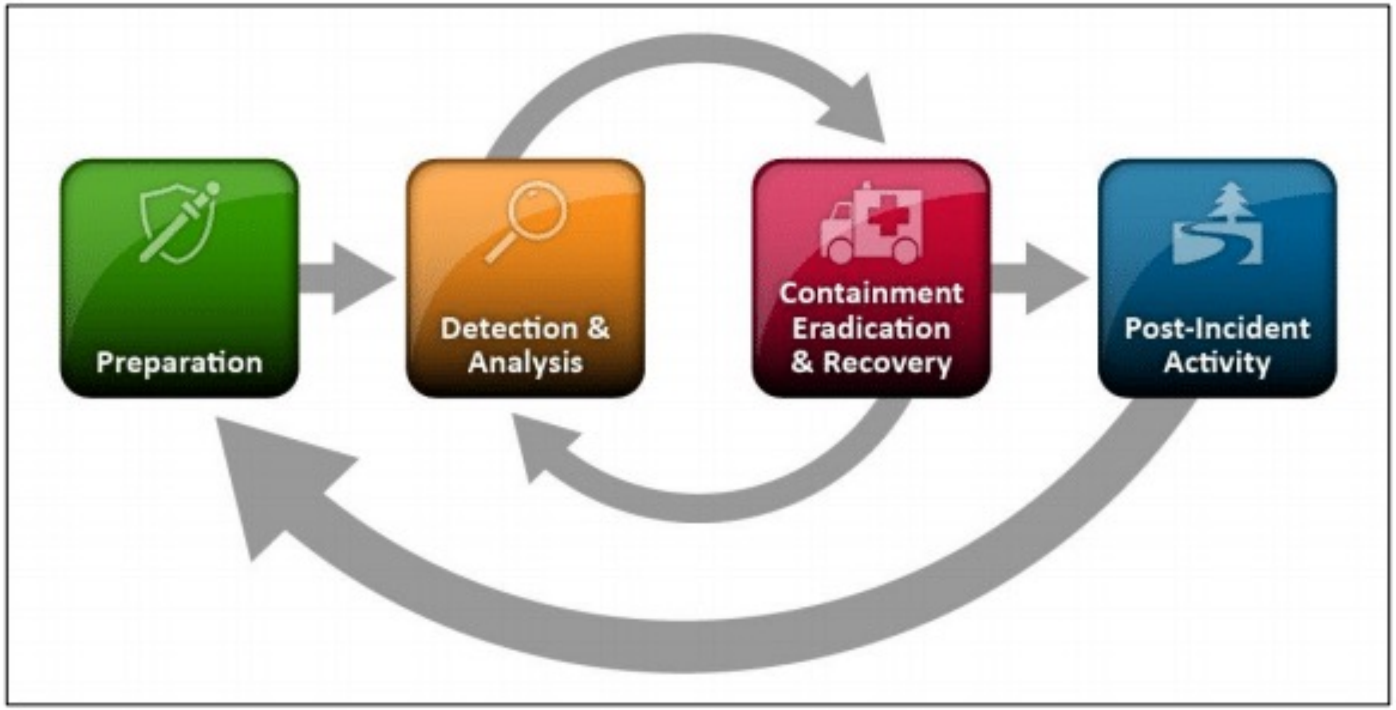
Zero Day

A previously unknown system vulnerability with the potential of exploitation without risk of detection or prevention because it does not, in general, fit recognized patterns, signatures or methods.

THE GOAL OF INCIDENT RESPONSE

- it is inevitable that adverse events will happen that have the potential to affect the business mission or objectives.
- The priority of any incident response is to protect life, health and safety. When any decision related to priorities is to be made, always choose safety first.
- The primary goal of incident management is to be prepared. Preparation requires having a policy and a response plan that will lead the organization through the crisis.
- Every organization must have an incident response plan that will help preserve business viability and survival.
- The incident response process is aimed at reducing the impact of an incident
- incident response planning is a subset of the greater discipline of business continuity management (BCM)

COMPONENTS OF THE INCIDENT RESPONSE PLAN



PREPARATION

- Develop a policy approved by management.
- Identify critical data and systems, single points of failure.
- Train staff on incident response.
- Implement an incident response team. (covered in subsequent topic)
- Practice Incident Identification. (First Response)
- Identify Roles and Responsibilities.
- Plan the coordination of communication between stakeholders.

DETECTION AND ANALYSIS

Monitor	Monitor all possible attack vectors.
Analyze	Analyze incident using known data and threat intelligence.
Prioritize	Prioritize incident response.
Standardize	Standardize incident documentation.

CONTAINMENT

GATHER EVIDENCE.

CHOOSE AN APPROPRIATE CONTAINMENT STRATEGY.

IDENTIFY THE ATTACKER.

ISOLATE THE ATTACK.

ERADICATION

Identify and mitigate all vulnerabilities that were exploited.

Remove malware, inappropriate materials, and other components.

If more affected hosts are discovered (for example, new malware infections), repeat the detection and analysis steps to identify all other affected hosts, then contain and eradicate the incident for them.

RECOVERY

- Removing malicious content from infected systems

- Rechecking, testing, and verifying all components for functionality

- Enacting extreme care during the recovery and restoration process so information systems are reliable once more

- Implementing a systematic approach to testing, monitoring, and validating data systems to avoid future compromise

- Designing procedures that help return information systems to full functionality (e.g., establishing an agreed-upon timeframe to restore data systems for use)

- Creating a written record of platforms and processes for testing and verification of restored systems to provide guidelines for managing another intrusion should it occur

POST-INCIDENT ACTIVITIES

IDENTIFY EVIDENCE THAT MAY NEED TO BE RETAINED.

DOCUMENT LESSONS LEARNED.

INCIDENT RESPONSE TEAM

Computer Incident Response Team (CIRT)

Computer Security Incident Response Team (CSIRT)

Responsibilities :

Determine the amount and scope of damage caused by the incident.

Determine whether any confidential information was compromised during the incident.

Implement any necessary recovery procedures to restore security and recover from incident-related damage.

Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

INCIDENT RESPONSE TEAM MEMBERS

- Representative(s) of senior management
- Information security professionals
- Legal representatives
- Public affairs/communications representatives
- Engineering representatives (system and network)

THE IMPORTANCE OF BUSINESS CONTINUITY

to sustain business operations while recovering from a significant disruption.

Key part : communication

COMPONENTS OF BUSINESS CONTINUITY PLAN

List of the BCP team members, including multiple contact methods and backup members

Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)

Notification systems and call trees for alerting personnel that the BCP is being enacted

Guidance for management, including designation of authority for specific managers

How/when to enact the plan

Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

THE GOAL OF DISASTER RECOVERY

the Disaster recovery plan (DRP) guides the actions of emergency response personnel until the end goal is reached—which is to see the business restored to full last-known reliable operations.

Disaster recovery refers specifically to restoring the information technology and communications services and systems needed by an organization, both during the period of disruption caused by any event and during restoration of normal services.

COMPONENTS OF DISASTER RECOVERY PLAN

- Executive summary providing a high-level overview of the plan
- Department-specific plans
- Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
- Full copies of the plan for critical disaster recovery team members
- Checklists for certain individuals:
    - Critical disaster recovery team members will have checklists to help guide their actions amid the chaotic atmosphere of a disaster.
    - IT personnel will have technical guides helping them get the alternate sites up and running.
    - Managers and public relations personnel will have simple-to-follow, high-level documents to help them communicate the issue accurately without requiring input from team members who are busy working on the recovery.