Security Governance
Master of Science in Cyber Security

AA 2024/2025

INCIDENT MANAGEMENT

Definitions

An **incident** is an event that could lead to loss of, or disruption to, an organization's operations, services or functions.

Incident management is the process aimed at identifying, analysing, and correcting hazards to prevent a future re-occurrence.

OBSERVATION: Without effective incident management, an incident can disrupt business operations, information security, IT systems, employees, customers, or other vital business functions

What is a Cyber Security Incident?

Any malicious act (or suspicious event) that:

- *Compromises (or was an attempt to compromise) the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset or*
- *Disrupts (or was an attempt to disrupt) the operation of a Critical Cyber Asset*

An incident is the act of violating an explicit or implied security policy (according to NIST Special Publication 800-61). These include but are not limited to:

- *attempts (either failed or successful) to gain unauthorized access to a system or its data*
- *unwanted disruption or denial of service*
- *the unauthorized use of a system for the processing or storage of data*
- *changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent*

Incident Management

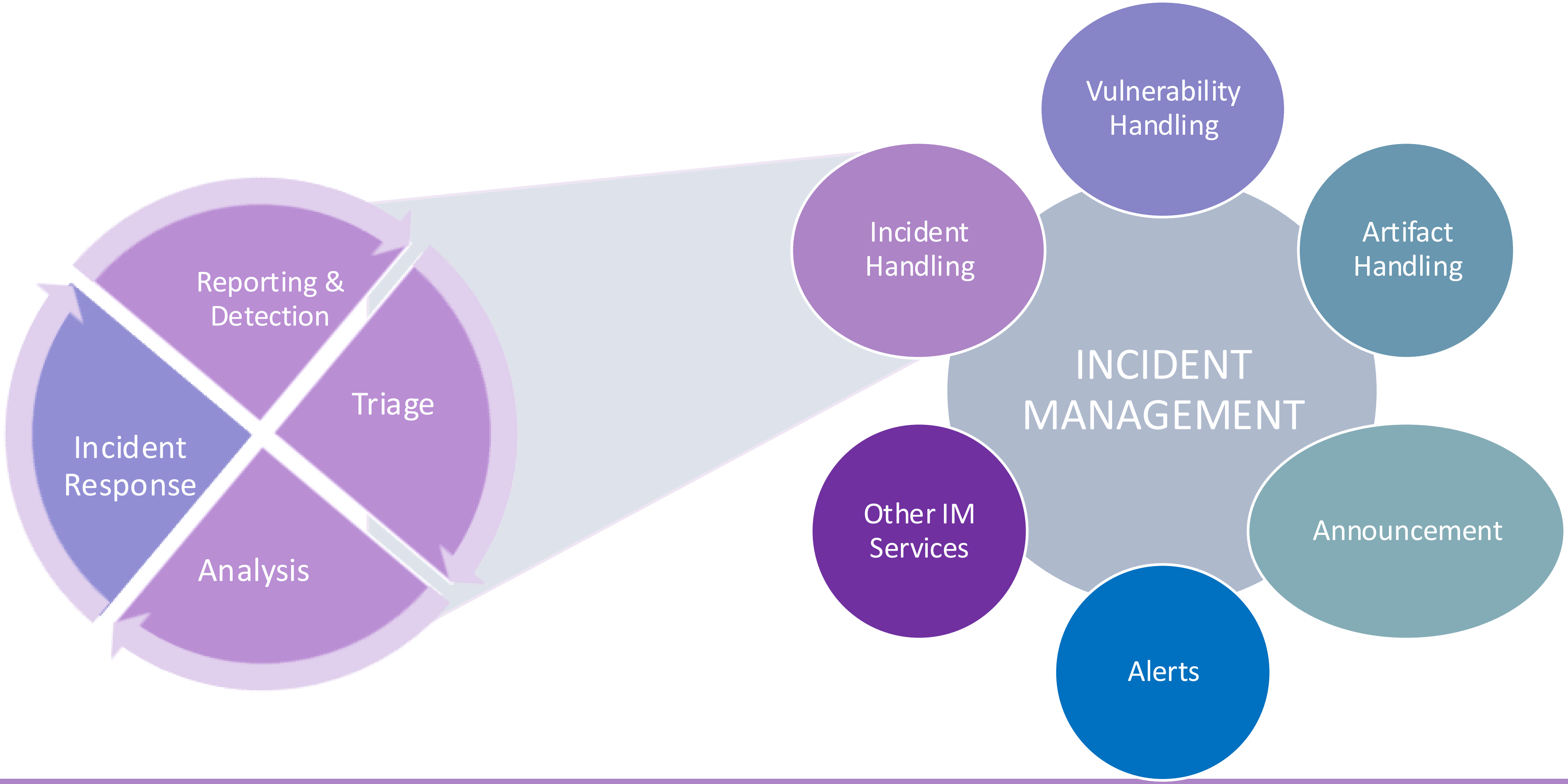
Incident management seeks to **prevent** such incidents from happening.

When they do happen, incident management aims to **contain** and resolve them, and use the lessons learnt for the next time.

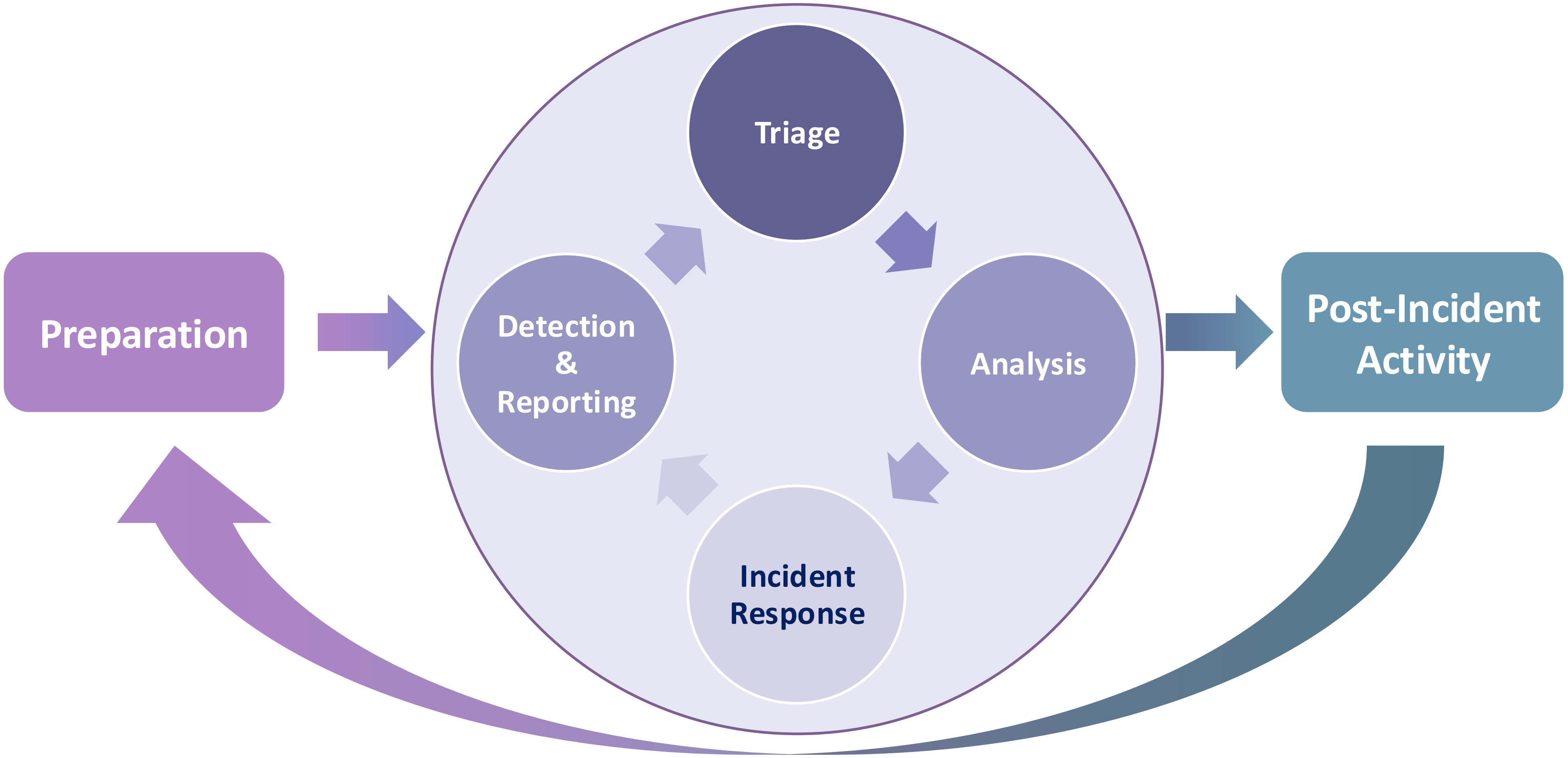
Therefore incident management serves the primary process and the organisation as a whole

The IT department may implement it, but it directly concerns the management of the organisation

Incident Management Decomposition



Incident Handling Life Cycle



Preparation

Incident response methodologies typically emphasize preparation

- establishing an incident response capability to timely respond to incidents is fundamental but…
- … preventing incidents by ensuring that systems, networks, and applications are sufficiently secure is also paramount

Preparation is composed of two main activities

- Preparing to handle Incidents
- Preventing Incident

Preparing to Handle Incidents

In order to handle incidents efficiently and effectively there is the need to define

- *Communication and Facilities*
  - Contact Information, Incident reporting mechanism, Issue tracking system, Smartphones, war room, Secure storage facility, etc…
- *Analysis Hardware and Software tools*
  - Digital Forensics workstation, Laptops, Removable media, etc…
- *Incident Analysis Resources*
  - Documentation, cryptographic hashes, list of critical assets
- *Incident Mitigation Software*
  - Clean OS and application for restoration

Preparing to Handle Incidents

Many incident response teams create a jump kit

- a portable case that contains materials that may be needed during an investigation

The jump kit should be ready to go at all times

A jump kit typically includes:

- a laptop, loaded with appropriate software (e.g., packet sniffers, digital forensics)
- backup devices
- blank media
- basic networking equipment and cables.

Because the purpose of having a jump kit is to facilitate faster responses, the team should avoid borrowing items from the jump kit

Preventing Incidents

Keeping the number of incidents reasonably low is very important to protect the business processes of the organization

If security controls are insufficient, higher volumes of incidents may occur, overwhelming the incident response team

This can lead to slow and incomplete responses, which translate to a larger negative business impact (e.g., more extensive damage, longer periods of service and data unavailability).

Preventing Incident

Fundamental activities to prevent incidents are

- Risk Assessment
- Host Security
- Network Security
- Malware Prevention
- User Awareness and Training

Detection and Analysis

Incidents can occur in countless ways, so it is infeasible to develop step-by-step instructions for handling every incident

Organizations should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors

Different types of incidents merit different response strategies

Attack Vectors

The most common attack vectors that every company should be ready to handle are

- External/Removable Media
- Attrition (e.g., brute force attacks)
- Web
- Emails
- Impersonation
- Improper Usage
- Loss or Theft of Equipment
- …

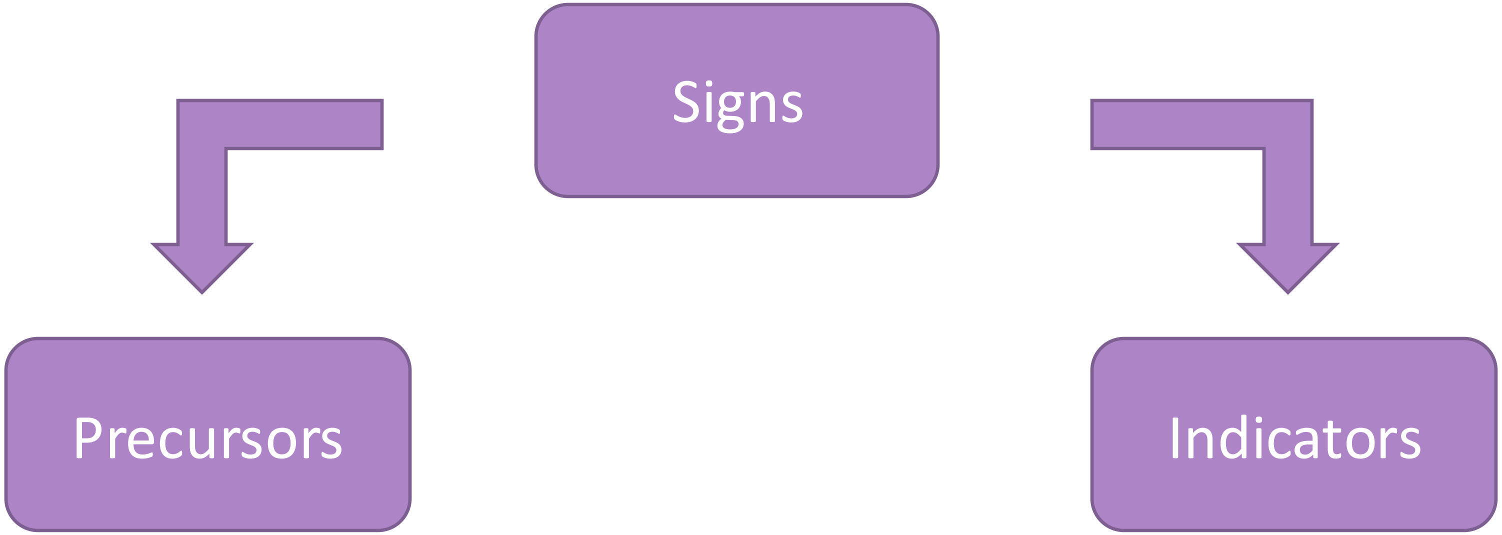
Signs of an Incident

In order to effectively respond to an incident it is fundamental to detect and classify it

Challenges:

1. Detection can rely on many different means, with varying levels of detail and fidelity
2. The volume of potential signs of incidents is typically high
3. Deep, specialized technical knowledge and extensive experience are necessary for proper and efficient analysis of incident-related data

Signs of an Incident



Signs

Precursors

Indicators

It is a sign that an incident may occur in the future

It is a sign that an incident may have occurred or may be occurring now

Sources of Precursors and Indicators

Common Sources of precursors and indicators are

Alerts	IDPSs
	SIEMs (Security Information and Event Management)
	Antivirus and antispam software
	File Integrity Checking software
	Third party monitoring services
Logs	Operating system, service and application logs
	Network device logs
	Network Flows
Publicly Available Information	Information on new vulnerabilities and exploits
People	People from within the organization
	People from other organizations

Incident Analysis

Incident detection and analysis is deeply impacted by several factors

- Accuracy (False Positive)
- Huge amount of events/alerts to analyse
- Indicators may follows from different root causes (not necessarily related to an incident)
- Many incidents are not associated with clear symptoms

Suggestion: build a team of highly experienced and proficient staff members who can analyse the precursors and indicators effectively and efficiently and take appropriate actions

10 Recommendations for Incident Analysis

1. Profile Networks and Systems
2. Understand Normal Behaviors
3. Create a Log Retention Policy
4. Perform Event Correlation
5. Keep All Host Clocks Synchronized
6. Maintain and Use a Knowledge Base of Information
7. Use Internet Search Engines for Research
8. Run Packet Sniffers to Collect Additional Data
9. Filter the Data
10. Seek Assistance from Others

Incident Documentation

In case of suspect of an incident running, it is fundamental to start to record facts related to the possible incident

- Timeline
- Supporting tools should be adopted
- Preserving integrity and confidentiality of collected data is important

Incident Prioritization

Handling should be prioritized based on the relevant factors, such as

- Functional Impact of the Incident
- Information Impact of the Incident

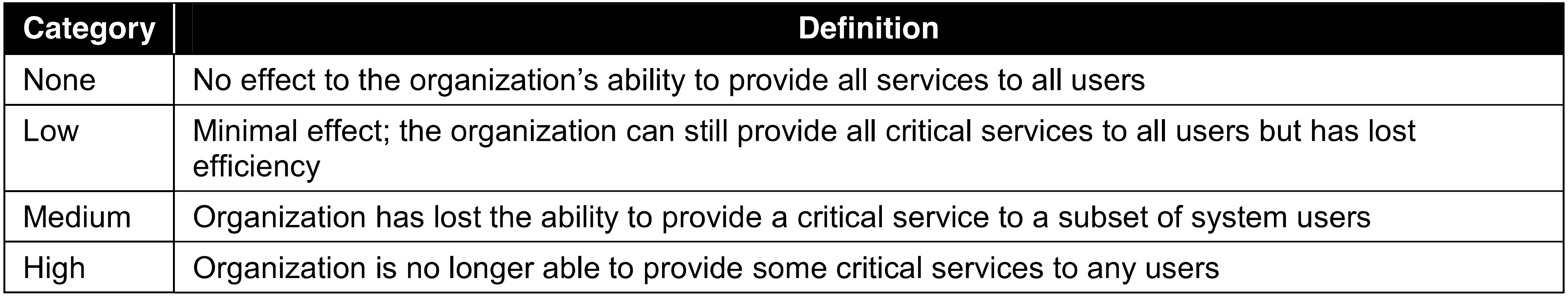
Business Impact

- Recoverability from the Incident

An organization can best quantify the effect of its own incidents because of its situational awareness

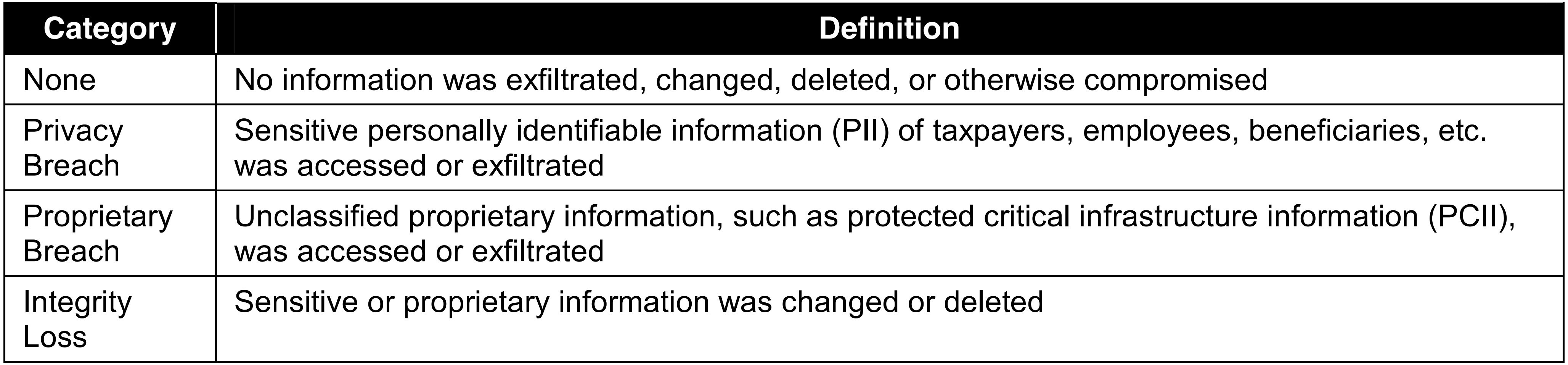
Rating incidents can be helpful in prioritizing limited resources

Example of Functional Impact Categories



Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Example of Information Impact Categories



Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Example of Recoverability Effort Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Incident Notification

Incidents should be notified to the appropriate individuals so that all who need to be involved in the response will play their roles

- Notification list and procedures should be specified in the security policies
- Multiple Communication strategies should be defined to be fault tolerant

Choosing a Containment Strategy

Containment is important before an incident overwhelms resources or increases damage

Containment provides time for developing a tailored remediation strategy

An essential part of containment is decision-making

- e.g., shut down a system, disconnect it from a network, disable certain functions
- Such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident

Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly

Choosing a Containment Strategy

OBSERVATION: Containment Strategies are incident dependent!

Criteria for determining the appropriate strategy include:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (e.g., network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (e.g., partial containment, full containment)
- Duration of the solution (e.g., emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution)

Evidence Gathering and Handling

Gathering evidence during an incident has two main purpose:

- to resolve the incident
- for legal proceedings

In such cases, it is important to clearly document how all evidence (including compromised systems) has been preserved

Identifying the Attacking Hosts

WARNING: Identifying an attacking host can be a time-consuming and futile process that can prevent a team from achieving its primary goal i.e., minimizing the business impact

the most commonly performed activities for attacking host identification are

- Validating the Attacking Host’s IP Address
- Researching the Attacking Host through Search Engines
- Using Incident Databases
- Monitoring Possible Attacker Communication Channels

Eradication and Recovery

Eradication may be necessary to

- eliminate components of the incident
- disable breached user accounts
- identify and mitigate all vulnerabilities that were exploited

Eradication and Recovery

In recovery, administrators

- restore systems to normal operation
- confirm that the systems are functioning normally
- remediate vulnerabilities to prevent similar incidents

Recovery may involve

- restoring systems from clean backups
- rebuilding systems from scratch
- replacing compromised files with clean versions
- installing patches
- changing passwords
- and tightening network perimeter security (e.g., firewall rulesets, boundary router access control lists)

Lessons Learned

One of the most important parts of incident response is also the most often omitted: **learning and improving**

Questions to be answered include:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyse, and mitigate future incidents?

Reference

- NIST SP 800-61, Revision 2 Computer Security Incident Handling Guide - Recommendations of the National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf