SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

M3.5 - Cybersecurity Operations and Management

Contents (1/2)

Contents (2/2)

Contents

Technical Vulnerability

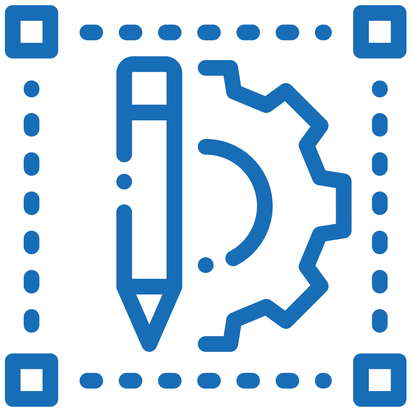
GENERAL DEFINITION

A **hardware, firmware, communication, or software flaw that leaves an information processing system open to potential exploitation** either externally or internally, resulting in risk for the system.

Technical Vulnerability Management

GENERAL DEFINITION

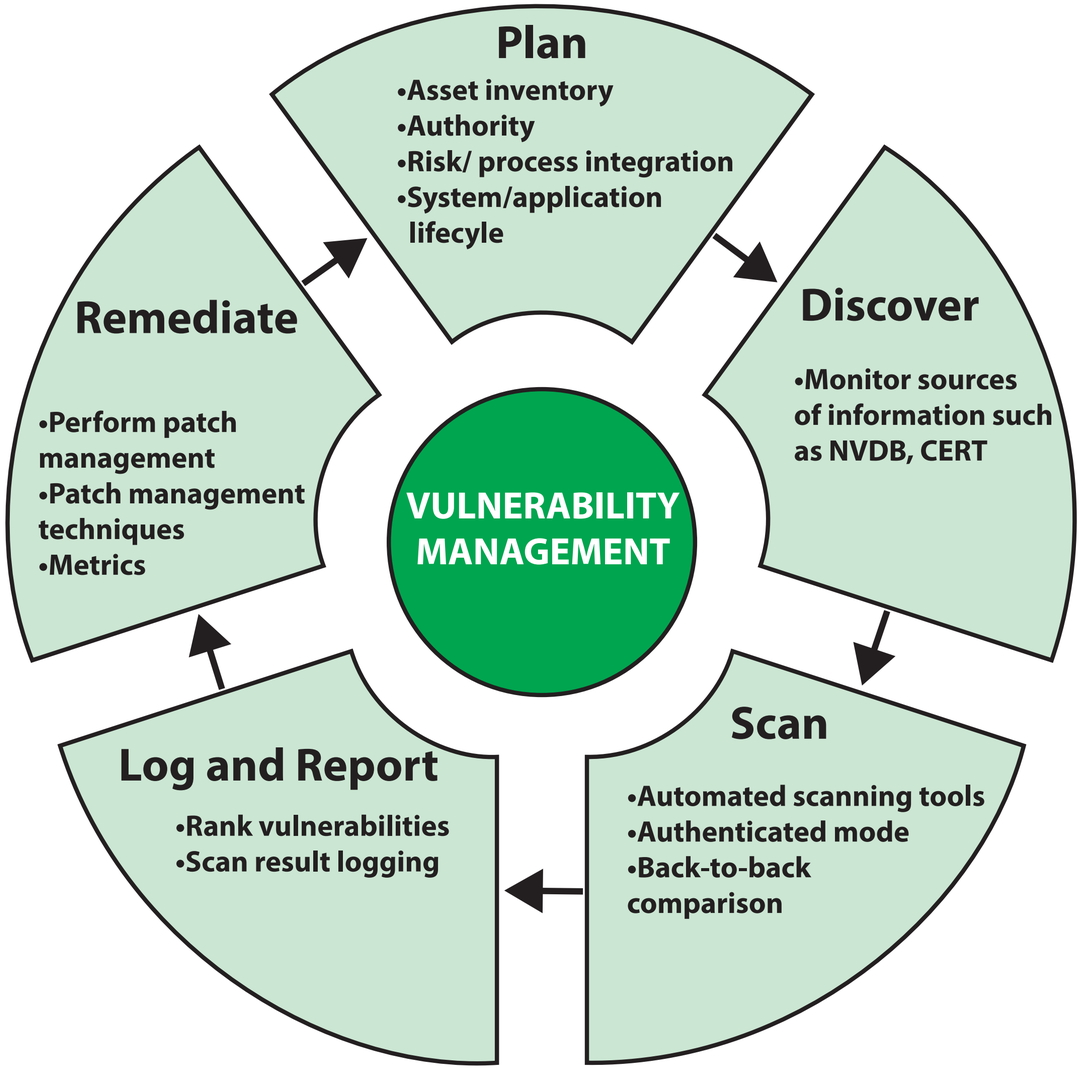
- Technical vulnerability management, usually referred as vulnerability management, is a security practice specifically **designed to proactively mitigate or prevent the exploitation of technical vulnerabilities** that exist in a system or an organization
- The process **involves the identification, classification, remediation, and mitigation of various vulnerabilities** in a system
- It is an integral part of cybersecurity and is practiced together with risk management as well as other security practices



Vulnerability Management Steps

PROCESS

Five key steps involved in vulnerability management



Plan Vulnerability Management (1/2)

VULNERABILITY MANAGEMENT STEPS

Effective **management of technical vulnerabilities** begins with planning. **Key aspects of the planning process** include the following:

1. **Risk and process integration:**

   Technical vulnerability review is an operational aspect of an overall information security risk management strategy. A vulnerability **analysis** must consider the **relative risk impacts**, including those related to the potential for operational disruption. These risks must also have a **clear reporting** path that allows for appropriate management awareness of risk factors and exposure. Vulnerability management should also provide input into change management and incident management processes.

2. **Integration with asset inventory:**

   Asset identification is an integral part of risk assessment. The resulting asset **inventory** allows for action to be taken once a technical vulnerability is reviewed and a mitigation strategy agreed on. By integrating the asset inventory with the vulnerability management system, an enterprise can **prioritize high-risk systems where the impact of technical vulnerabilities can be greatest**.

Plan Vulnerability Management (2/2)

VULNERABILITY MANAGEMENT STEPS

3. **Establishment of clear authority to review vulnerabilities:**

   Because probing a network for vulnerabilities can disrupt systems and expose private data, an **enterprise needs to have in place a policy and approval from top management before performing vulnerability assessments**. The enterprise's acceptable use policy must have users and system managers consent to vulnerability scanning as a condition of connecting to the network. Awareness training should clarify that the main purpose of seeking vulnerabilities is to defend against attacks. There is also a need for policies and **ethical guidelines for those who have access to data from vulnerability scans**. These individuals need to understand the appropriate action when illegal materials are found on their systems during a vulnerability scan.

4. **System and application life cycle integration:**

   The review of vulnerabilities must be **integrated in system release and software development planning** to ensure that potential weaknesses are identified early to both lower risks and manage costs of finding these issues prior to identified release dates.

Discovery Known Vulnerability

VULNERABILITY MANAGEMENT STEPS

The **discover step** involves **monitoring sources of information** about **known vulnerabilities** to hardware, software, and network equipment.

Key sources of information include the following:

- **NIST** National Vulnerability Database (**NVDB**), Common Vulnerability Scoring System (**CVSS**), and Common Vulnerabilities and Exposures (**CVE**)

- **Computer emergency response team** (**CERT**)
  - A team that **collects information about system vulnerabilitie**s and disseminates it to systems managers
  - Local (inside the organization) or national CERT

- **Packet storm** **https://packetstormsecurity.com/**:
  - Provides information and tools to help mitigate both personal data and physical loss on a global scale

- **Security Focus**:

  This site maintains two important resources.
  - **BugTraq** is a high-volume, full-disclosure mailing list for detailed discussion and announcement of computer security vulnerabilities.
  - **The SecurityFocus Vulnerability Database** provides security professionals with up-to-date information on vulnerabilities for all platforms and services

- **Internet Storm Cente**r (**ISC**) **https://isc.sans.edu/**:

  Maintained by the SANS Technology Institute, the ISC provides a free analysis and warning service to thousands of Internet users

Scan for Vulnerability (1/2)

VULNERABILITY MANAGEMENT STEPS

- Enterprises need to **regularly scan software, systems, and networks** for vulnerabilities and proactively address those that are found
- The Center for Internet Security (CIS) **recommends the following scanning** regimen:
  - **Run automated vulnerability scanning tools against all systems on the network on a weekly** or more frequent basis and deliver a prioritized lists of the most critical vulnerabilities to each responsible system administrator
  - **Perform vulnerability scanning in authenticated mode**, either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested
  - Compare the results from back-to-back vulnerability scans to **verify that vulnerabilities were addressed**, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk

Scan for Vulnerability (2/2)

VULNERABILITY MANAGEMENT STEPS

There are **two challenges involved in scanning** that an enterprise needs to address:

- **Scanning can cause disruptions.** The scanning process can **impact performance**. This is especially true with **legacy systems**, which can have problems even with simple network port scans. IT operations staff need to be in the loop. Make them aware of the importance and relevance of scans. Also, timing needs to be resolved to ensure that **scanning does not conflict with regular maintenance schedules**.

- **Scanning can generate huge amounts of data and numerous false positives.** Technical vulnerability management practices produce very large data sets. Accordingly, use frequent follow-up evaluations to validate the findings. Reviewing all these vulnerabilities is infeasible. Develop a vulnerability prioritization plan before initiating a large number of scans.

The vulnerability prioritization plan must be aligned with the IT infrastructure and application plan to support the overall IT strategic plan; there should not be too much focus on legacy infrastructure and legacy applications that may be retired shortly.

Log and Report

VULNERABILITY MANAGEMENT STEPS

- When a vulnerability **scan is completed**, the **organization should log the results** so that personnel can verify the activity of the regular vulnerability scanning tools
- Discovered **vulnerabilities should be ranked** reflecting:
  - The **skill required to exploit** the vulnerability
  - The **availability of the exploit** to potential attackers
  - The **privilege gained upon successful exploitation**
  - The **risk and impact of this vulnerability** if exploitation is successful
- The **reporting process includes keeping track of the number and risk levels** of vulnerabilities discovered over time and the effectiveness of remediation efforts in removing vulnerabilities
- Event logs be correlated with information from vulnerability scans

Performing Patch Management

VULNERABILITY MANAGEMENT STEPS

Issues to consider related to **performing patch management**:

1. The **relationship between timing, prioritization, and testing**

2. **Availability of resources involved in testing** need to be taken into account

3. **The impact of a patch** on operational systems

4. **Special care** should be taken **if multiple automated means of patching are used** (self-patching software, third-party services, and network-based capability)

Security Event Logging

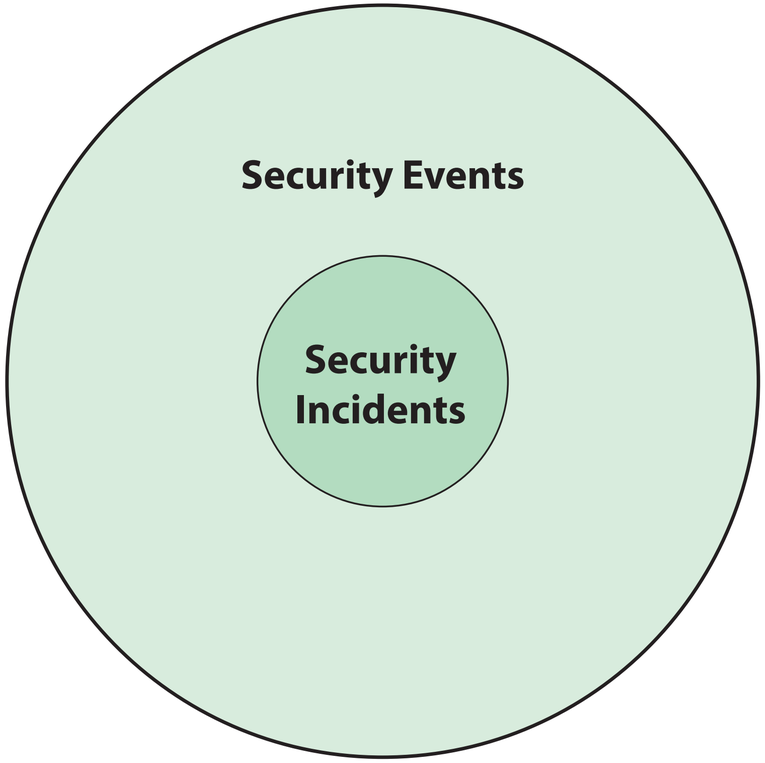
In the **information security field, a distinction** is commonly made between **events** and **incidents**:

Security event

An **occurrence** considered by an organization to have **potential security implications** to a system or its environment. **Security events identify suspicious or anomalous activity**. Events sometimes provide indications that incident are occurring

Security incident

An **occurrence** that actually or **potentially puts in danger the confidentiality, integrity, or availability of an information system**; or the information the system processes, stores, or transmits; or that **constitutes a violation** or **imminent threat of violation** of security policies, security procedures, or acceptable use policies

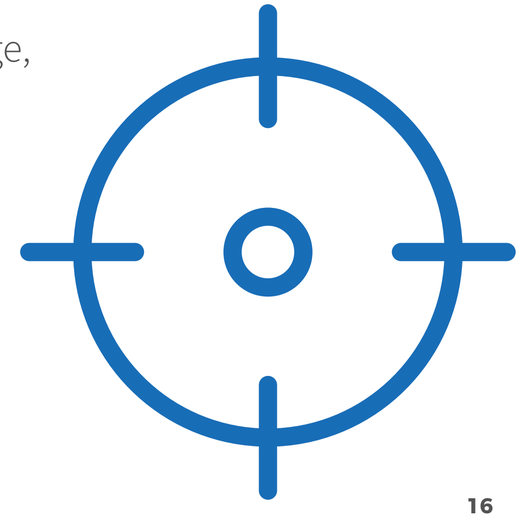


Security Event Logging Objectives

- The **objectives of security event logging** are:
  - To **help identify threats** that may lead to an information security incident
  - Maintain the integrity of important security-related information
  - **Support forensic investigations**

- **Effective logging enables an enterprise to review events, interactions, and changes that are relevant to security**

- **With a record of events** such as **anomalies**, unauthorized access attempts, and excessive resource usage, an **enterprise can perform an analysis to determine the cause**



Log

GENERAL DEFINITION

A record of the **events occurring** within an organization's **systems** and **networks**

Potential Security Log Sources

A wide **variety of sources of security events can be logged**, including the following:

- Server and workstation operating **system logs**
- **Application logs** (for example, web server, database server)
- **Security tool logs** (for example, antivirus, change detection, intrusion detection/ prevention system)
- **Outbound proxy logs** and end-user application logs
- **Firewalls and other perimeter security devices for traffic** between local user and remote database or server (referred to as north–south traffic)
- Security devices between data center storage elements that communicated across a network, which may involve **virtual machines and software-based virtual security capabilities**

What to Log for Security Aspects?

Potential **security related events that could be logged**:

Operating system logs

Successful user logon/logoff; **failed user logon**; user account change or deletion; service failure; password changes; **service started or stopped**; object access denied; object access changed

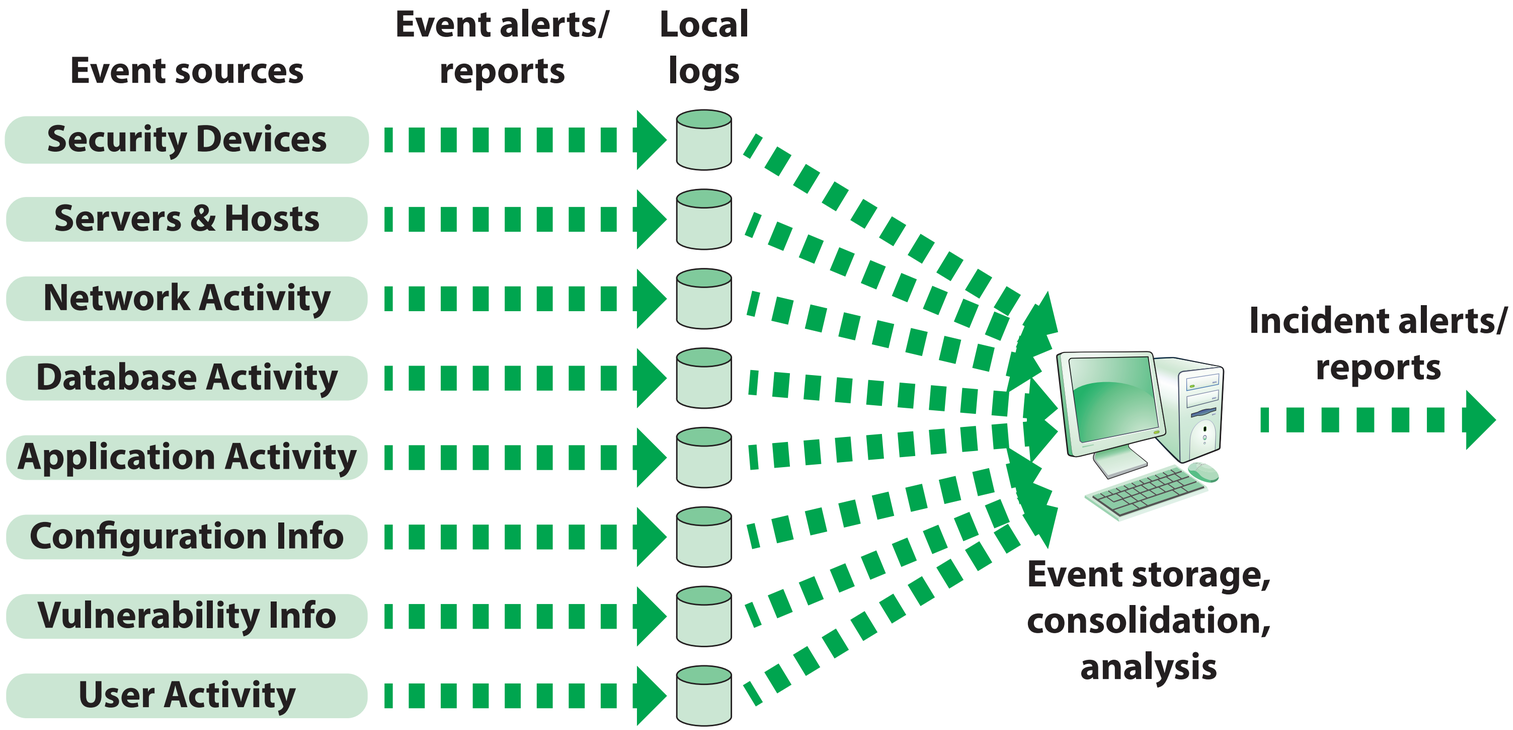
Network device logs

Traffic allowed through firewall, **traffic blocked by firewall**; bytes transferred; protocol usage; detected attack activity; user account changes; **administrator access**

Web servers

Excessive access attempts to nonexistent files; **code seen as part of the URL**; attempted access to extensions not implemented on the server; web service stopped/started/failed messages; **failed user authentication**; invalid request; internal server error

Security Event Management (SEM)



Security event management (SEM) is the **process** of identifying, gathering, monitoring, analyzing, and reporting security-related events. **The objective of SEM is to extract from a large volume of security events those events that qualify as incidents.** SEM takes data input from all devices/nodes and other similar applications, such as log management software. The collected events data is **analyzed with security algorithms and statistical computations** to trace out any vulnerability, threat, or risk

SEM Functions (1/2)

- The first phase of event management is the **collection of event data** in the form of logs
- As event data are generated, they are **generally stored in logs local to the devices that generate them**
- A number of steps need to be taken at this point:
  - **Normalization**:
    For effective management, the log data needs to be in a **common format** to enable further processing
  - **Filtering**:
    This step includes **assigning priorities** to various types of events
  - **Aggregation**:
    The IT facility of a large enterprise generates millions of events per day; it is possible to aggregate them **by categorie**s into a more manageable amount of data

SEM Functions (2/2)

The objective of the next steps is to **analyze the data and generate alerts** of security incidents

Pattern matching

- It is important to look for data patterns within the fields of stored event records. **A collection of events with a given pattern can signal a security incident**

Scan detection

- Often, an **attack begins with a scan of IT resources by the attacker,** such as port scans, vulnerability scans, or other types of pings. A **substantial number of scans being found from a single source** or a small number of sources can signal a security incident

Threshold detection

- A straightforward form of analysis is the detection of a threshold being crossed. For example, if the number of occurrences of a type of **event exceeds a given threshold in a certain time period,** that constitutes an incident

Event correlation

- Correlation consists of using multiple **events from a number of sources to determine that an attack or suspicious activity** occurred
- Another aspect of correlation is to **correlate particular events with known system vulnerabilities**, which might result in a high-priority incident

Threat Intelligence

GENERAL DEFINITION

Threat intelligence, also known as **cyber threat intelligence (CTI)**, or cyberintelligence, is the **knowledge established as a result of analyzing information about potential or current attacks that threaten an organization**

The information is **taken from a number of internal and external sources**, including application, system, and network logs; security products such as firewalls and intrusion detection systems; and dedicated threat feeds

Threat Sources

GENERAL DEFINITION

Adversarial:

Individuals, groups, organizations, or states **that seek to exploit** the organization's dependence on cyber resources

Accidental:

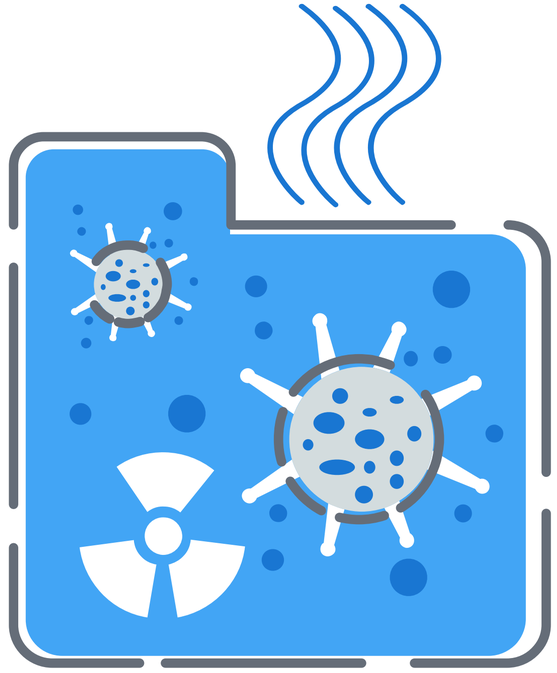
Erroneous actions taken by individuals in the course of executing their everyday responsibilities

Structural:

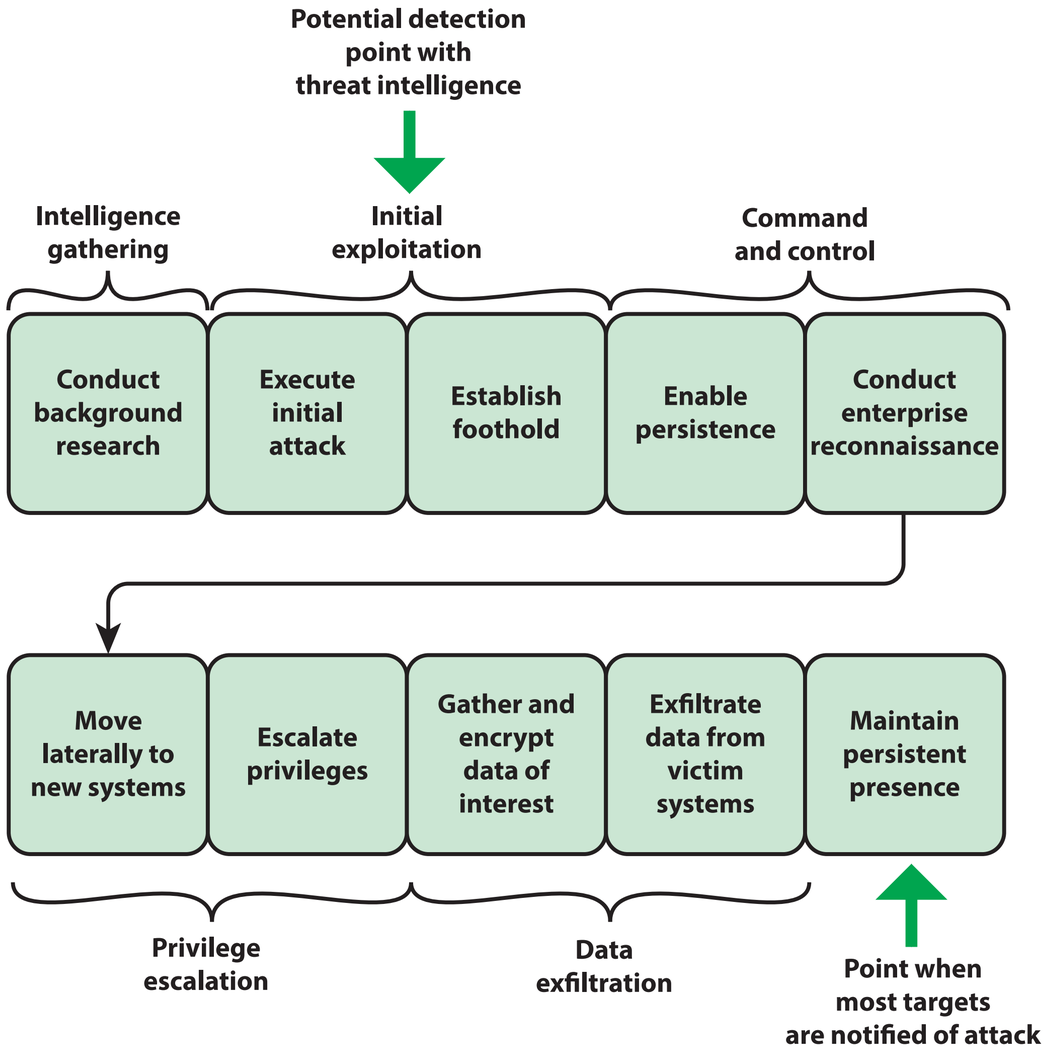
Failures of equipment, environmental controls, or **software due to aging**, resource depletion, or other circumstances that exceed expected operating parameters

Environmental:

Natural disasters and **failures of critical infrastructures** on which the organization depends, but which are outside the control of the organization



Potential Benefits of Threat Intelligence



The **primary purpose** of **threat intelligence is to help organizations understand the risks** of the most common and severe external threats, such as advanced persistent threats (APTs), exploits, and **zero-day threats**. Although threat actors also include internal (or insider) and partner threats, the emphasis is on the types of external threats that are most likely to affect a particular organization's environment.

Threat intelligence includes in-depth information about specific threats to help an organization protect itself against the types of attacks that could do them the most damage.

Threat intelligence enables a security team to become aware of a threat well **before the point of typical notification**, which is often after the real damage is done. Even if an early opportunity is lost, **threat intelligence reduces the time it takes to discover that an attack** has already succeeded and therefore speeds up remediation actions to limit the damage.

Gathering Threat Intelligence

External Sources

Subscribe to a regular feed of threat data from a threat intelligence subscription service

Cyberintelligence vendors whose services can be employed

Many of the sources of vulnerability information, such as CERTs, are useful sources of threat intelligence

Another useful source of threat intelligence is information sharing and analysis centers (ISACs)

Internal Sources

Event logs from technical infrastructure, such as operating system logs

Alerts from security systems such as **firewalls**, malware protection, DLP, network-based intrusion detection systems (NIDSs), gateway proxy servers, and physical security systems

Direct feeds from security event management utilities, such as those produced by security event logging software or a security information and event management (SIEM) system

Dedicated teams that perform information security–related activities

Business support functions

Threat Analysis

Threat analysis includes the **task of describing the type of possible attacks**, potential attackers, and their methods of attack and the consequences of successful attacks

It **involves** the following:

- **Identifying** the vulnerabilities of the system
- **Analyzing the likelihood** of threats aimed at exploiting these vulnerabilities
- **Assessing the consequences** that would occur if each threat were to be successfully carried out
- **Estimating the cost** of each attack
- Costing out potential **countermeasures**
- **Selecting the security mechanisms** that are justified (possibly by using cost/ benefit analysis)

An organization should carry out **this analysis as a regular part of risk management**

Security Information and Event Management (SIEM)

GENERAL DEFINITION

An **application** or set of tools that **provides the ability to gather security data from information system components** and present that data as actionable information via a **single interface**

- One of the **most important incident management tools** is a **SIEM system**
- Capabilities of a typical **SIEM include**:
  - Data collection
  - Data aggregation
  - Data normalization
  - Correlation
  - Alerting
  - Reporting/compliance
  - Forensics
  - Retention
  - Dashboards

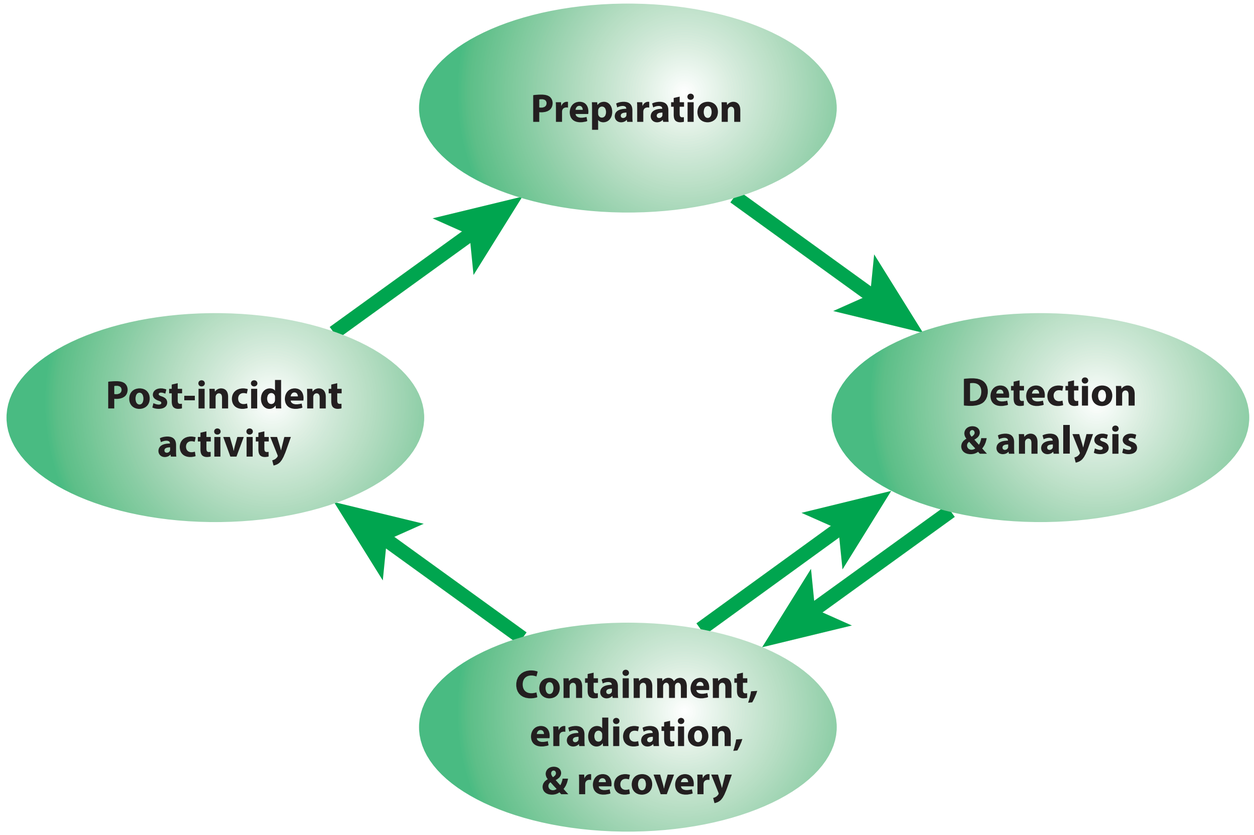
Incident Management Policy

- It is essential that an **incident management policy be established** for **appropriate incident management**

- The policy should also cover **the strategy for dealing with incidents**, including the following topics:

  - **Identification of an incident and response** (for example, shutdown, containment, quarantine)
  - **Acquisition** of volatile and static data
  - **Retention** and analysis of data
  - **Remediation**
  - **References to law** enforcement
  - Handling of forensic data
  - **Escalation** of incidents
  - **Reporting** of findings
  - **Definition of the learning process** from incidents to upgrade systems and processes

Incident Response Life-Cycle



- Many organizations **react in an ad hoc manner** when a security incident occurs.
- **Because of the potential cost of security incidents, it is cost-beneficial to develop a standing capability for quick discovery and response to such incidents.**
- This capability also serves to support the analysis of past security incidents **with a view to improving the ability to prevent and respond to incidents**.

Preparation for Incident Response

INCIDENT RESPONSE LIFE-CYCLE

Making the right planning and implementation decisions is key to establishing a successful incident response program

Tasks involved in preparing for incident response include:

- Develop an organization-specific definition of the term incident so that the scope of the term is clear
- Create an **incident response policy**
- Develop incident response and reporting procedures
- Establish **guidelines** for communicating with external parties
- Define the services that will be provided by the incident response team (IRT)
- Select an organizational structure and staffing model for incident response
- **Staff** and **train** the IRT
- Establish and maintain **accurate notification mechanisms**
- Develop **written guidelines for prioritizing incidents**
- Have a **plan** for the collection, formatting, organization, storage, and retention of incident data

Analysis

INCIDENT RESPONSE LIFE-CYCLE

- **Once an incident is detected**, it is appropriate to move immediately to the next phase of the life cycle, which deals with **removing the threat and recovery from any damage**.

- Typical **actions** include:
  - Determine the **magnitude** of the impact
  - Assess the **severity**
  - Assess the **urgency** of the event

- The **analysis also needs to determine whether immediate action is needed to remove the vulnerability or to block the action that enabled the incident to occur**

Containment

INCIDENT RESPONSE LIFE-CYCLE

- Most incidents require **some sort of containment**
- The objective is **to prevent the spread of the effects of the incident** before they overwhelm resources or in some other way increase damage
- Strategies for **dealing with various types of incidents must be planned well in advance**
- The nature of the strategy and **the magnitude of resources devoted to containment depends on criteria developed** ahead of time
  - Examples of criteria include **potential damage to and theft of resources**, the need to preserve evidence, the effectiveness of the strategy, the time and resources needed to implement the strategy, and the duration of the solution

Recovery

INCIDENT RESPONSE LIFE-CYCLE

During **recovery**, IT personnel **restore systems to normal operation to the extent possible and, if applicable, harden systems to prevent similar incidents**.

Possible **actions** include the following:

- **Restoring** systems with clean versions from the latest backup
- **Rebuilding** systems from scratch
- **Replacing** compromised files with clean versions
- **Installing** patches
- Changing passwords
- **Locking network perimeter security** (for example, firewall rule sets)

Incident Handling Checklist

INCIDENT RESPONSE LIFE-CYCLE

Detection and Analysis	
1.	Determine whether an incident has occurred
1.1	Analyze the precursors and indicators
1.2	Look for correlating information
1.3	Perform research (e.g., search engines, knowledge base)
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
3.	Report the incident to the appropriate internal personnel and external organizations
Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence
5.	Contain the incident
6.	Eradicate the incident
6.1	Identify and mitigate all vulnerabilities that were exploited
6.2	Remove malware, inappropriate materials, and other components
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
7.	Recover from the incident
7.1	Return affected systems to an operationally ready state
7.2	Confirm that the affected systems are functioning normally
7.3	If necessary, implement additional monitoring to look for future related activity
Post-Incident Activity	
8.	Create a follow-up report
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)

Emergency Classification

INCIDENT RESPONSE LIFE-CYCLE

Security incident emergencies must be handled with a greater sense of urgency than other security incidents.

An emergency response may make an **emergency fix to temporarily eliminate ongoing damage until a more permanent response is provided.** Implementing an emergency fix can also require that an information security officer be temporarily given access privileges not normally authorized.

Classification scheme for security incidents suggested in ISO 27035:

Emergency

- Severe impact
- These are incidents that act on especially important information systems and result in especially serious business loss or lead to especially important social impact

Critical

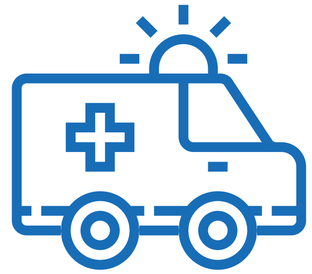
- Medium impact
- These are incidents that act on especially important information systems and result in serious business loss or lead to important social impact

Warning

- Low impact
- These are incidents that act on especially important information systems and result in minor business loss or lead to considerable social impact

Information

- No impact
- Result in minor business loss or no business loss or lead to minor social impact or no social impact



Example of Incident Category and Severity Class

	Severity Class			
Incident category	**Information**	**Warning**	**Critical**	**Emergency**
Technical attacks	Failed attempts	Single ordinary (user compromise)	Multiple (user compromise) (Application privileged access compromise)	Mass (Application privileged access compromise)
Technical attacks		Annoyance (scratch the surface)	Disturbance (throughput impact)	Unavailability (stop in service)
Malware	Single known (detected and blocked by antivirus protection)	Single unknown	Multiple infections Server infections	Mass infections

Threat and Incident Management Best Practices

The SOGP breaks down the best practices in the **threat and incident management category into two areas**.

The **areas** and topics are as follows:

Cybersecurity resilience:

The objective of this area is to **manage threats and vulnerabilities** associated with business applications, systems, and networks by scanning for technical vulnerabilities, maintaining up-to-date patch levels, performing continuous security event monitoring, **acting on threat intelligence, and protecting information against targeted cyber attacks**

Topics include:

- Technical vulnerability management
- Security event logging
- Security event management
- Threat intelligence
- Cyber attack protection

Security incident management:

The objective of this area is to **develop a comprehensive and documented strategy for managing security incidents**, which is supported by a process for the identification, response, recovery, and post-implementation review of information security incidents

Topics include:

- Security incident management framework
- Security incident management process
- Emergency fixes
- Forensic investigations

Contents

Physical and Infrastructure Security

GENERAL DEFINITION

We must distinguish **three elements** of information system security:

Logical security:

Protects computer-based data from software-based and communication-based threats.

Physical security:

Also called **infrastructure security** . Protects the information systems that contain data and the people who use, operate, and maintain the systems. Physical security also must **prevent any type of physical access or intrusion** that can compromise logical security.

Premises security:

Also known as **corporate or facilities security**. Protects the **people** and **property** within an entire area, facility, or building(s), and is usually required by laws, regulations, and fiduciary obligations. Premises security provides **perimeter security, access control**, **smoke and fire detection**, fire suppression, some environmental protection, and usually surveillance systems, alarms, and guards.

Physical Threats

GENERAL DEFINITION

There are a **number of ways in which such threats can be categorized**. It is **important to understand the spectrum of threats to information systems** so that responsible administrators can ensure that prevention measures are comprehensive.

We can organize the **threats into the following categories**:

- **Environmental** threats
- **Technical** threats
- **Human-caused** threats

Technical Threats

GENERAL DEFINITION

Electrical power is essential to run equipment

- **Power** utility problems:
  - Under-voltage - dips/brownouts/outages, interrupts service
  - Over-voltage - surges/faults/lightening, can destroy chips
- **Electromagnetic interference (EMI):**
  - **Noise** along a power supply line, motors, fans, heavy equipment, other computers, cell phones, microwave relay antennas, nearby radio stations
  - Noise can be transmitted through space as well as through power lines
  - Can **cause intermittent** problems with computers

Physical Security Prevention and Mitigation Measures

Standards including **ISO 27002** *"Code of practice for information security management"* and **NIST SP 800-53** *"Recommended Security Controls for Federal Information Systems"* **include lists of controls relating to physical and environmental security**

- One prevention measure is the use of **cloud** computing
- **Inappropriate temperature and humidity**
  - Environmental control equipment, power supply
- **Fire and smoke**
  - Alarms, preventative measures, fire mitigation
  - Smoke detectors, no smoking
- **Water**
  - Manage lines, equipment location, cutoff sensors
- **Other threats**
  - Appropriate technical counter-measures, limit dust entry, pest control

Mitigation Measures of Technical Threats

- Uninterruptible power supply (UPS) for each piece of critical equipment
- **Critical equipment should be connected to an emergency power source** (like a generator)
- To **deal with electromagnetic interference (EMI)** a combination of filters and shielding can be used

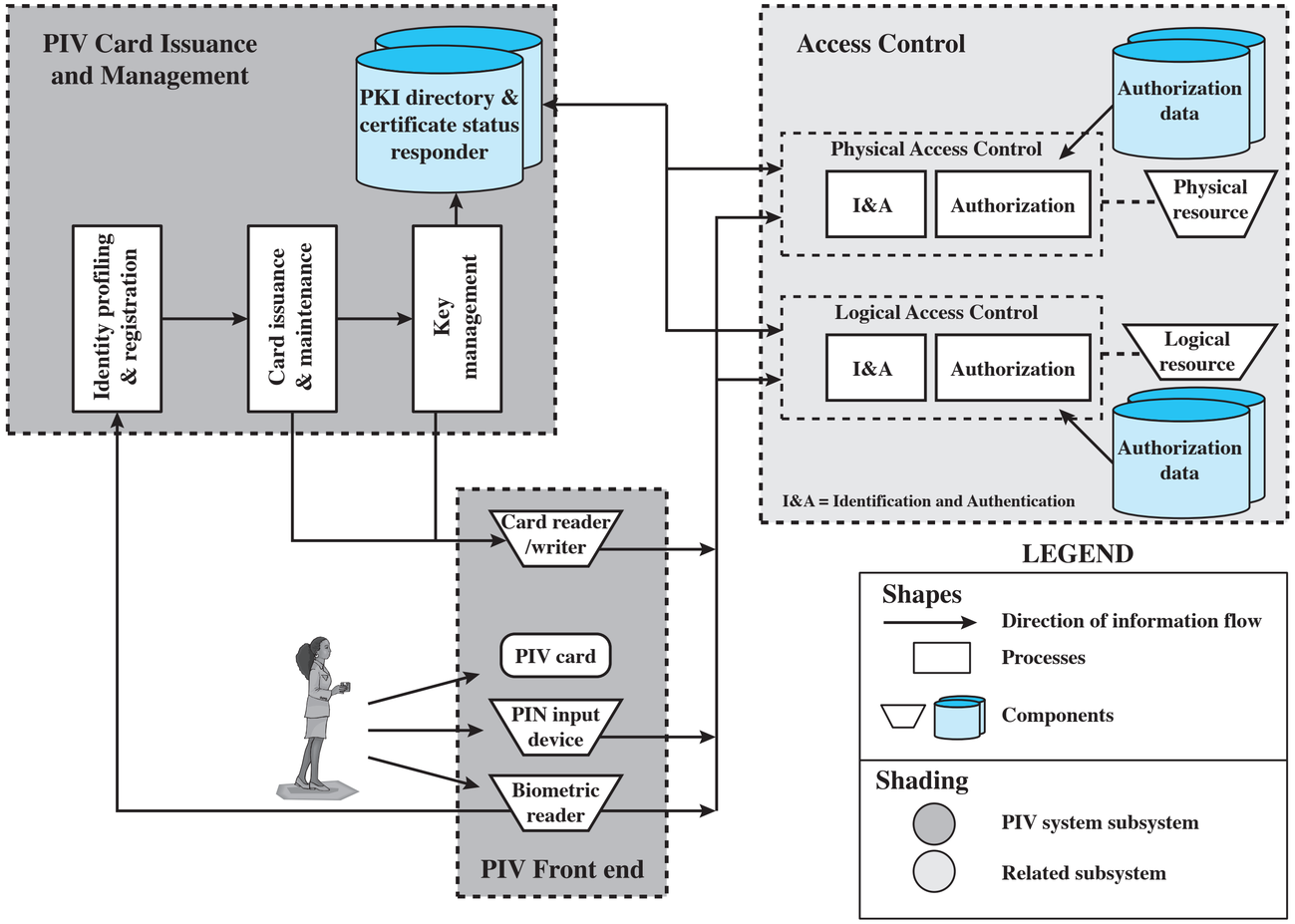
Recovery from Physical Security Breaches

- Most essential element of recovery is **redundancy**
  - Provides for recovery from loss of data
  - Ideally all important data should be available off-site and updated as often as feasible
  - Can use batch encrypted remote backup
  - **For critical situations a remote hot-site that is ready to take over operation instantly can be created**
- Physical equipment **damage recovery**
  - Depends on nature of damage and cleanup
  - **May need disaster recovery specialists**

Physical and Logical Security Integration

- Physical security involves numerous detection and prevention devices
- More effective if there is a central control
- **Integrate automated physical and logical security functions**
  - Use a single ID card
  - Single-step card enrollment and termination
  - Central ID-management system
  - Unified event monitoring and correlation
- For the **integration of physical and logical access control** to be practical, **a wide range of vendors must conform to standards that cover smart card protocols,** authentication and access control formats and protocols, database entries, message formats, and so on. An important step in this direction is FIPS 201-2 *"Personal Identity Verification (PIV) of Federal Employees and Contractors"* issued by NIST in 2013.

Personal Identification Verification System Model

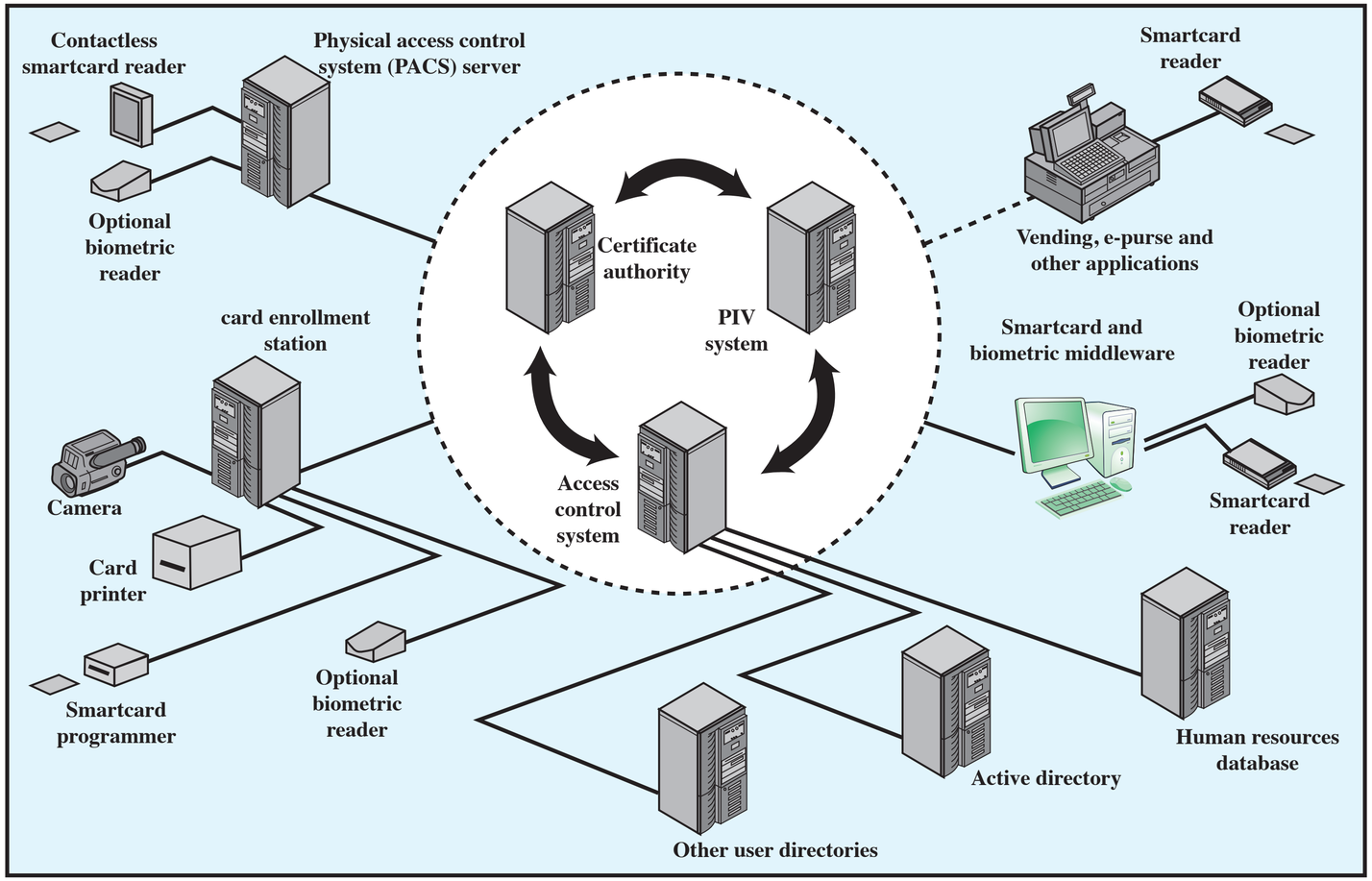


The **Personal Identification Verification (PIV) front end defines the physical interface to a user who is requesting access to a facility**, which could be either physical access to a protected physical area or logical access to an information system. **The PIV front end subsystem supports up to three factor authentication**; the number of factors used depends on the level of security required. The front end makes use of a **smart card**, known as a PIV card, which is a dual-interface contact and contactless card.

The other major component of the PIV system is the PIV **card issuance and management subsystem**. This subsystem includes the components responsible **for identity proofing and registration**, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure [PKI] directory, certificate status servers) required as part of the verification infrastructure.

The PIV system interacts with an **access control subsystem**, which includes components **responsible for determining a particular PIV cardholder's access to a physical or logical resource**.

Example of Convergence of Physical and Logical Security



If the **integration of physical and logical access control** extends beyond a unified front end to an integration of system elements, a **number of benefits grow**, including the following:

- **Employees gain a single, unified access control authentication device**; this cuts down on misplaced tokens, reduces training and overhead, and allows seamless access.
- A single logical location for employee ID management reduces duplicate data entry operations and allows for immediate and real-time authorization revocation of all enterprise resources.
- **Auditing and forensic groups have a central repository for access control investigations**.
- Hardware unification can reduce the number of vendor purchase-and-support contracts.
- Certificate-based access control systems can leverage user ID certificates for other security applications, such as document e-signing and data encryption.

Contents

Business Continuity Concepts

GENERAL DEFINITION

- **Business:** the operations and services performed by an organization in pursuit of its objectives, goals, or mission.
- **Business continuity: The capability of an organization to continue delivering products or services at acceptable predefined levels following a disruptive incident.** Business continuity embraces all the operations in a company, including how employees function in compromised situations.
- **Business continuity management (BCM):** A holistic management **process that identifies potential threats to an organization and the impacts to business operations those threats**, if realized, might cause, and that provides a framework for **building organizational resilience with the capability of an effective response** that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities.
- **Business continuity plan (BCP):** The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
- **Business continuity program:** An ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.

Business Continuity Objectives

GENERAL DEFINITION

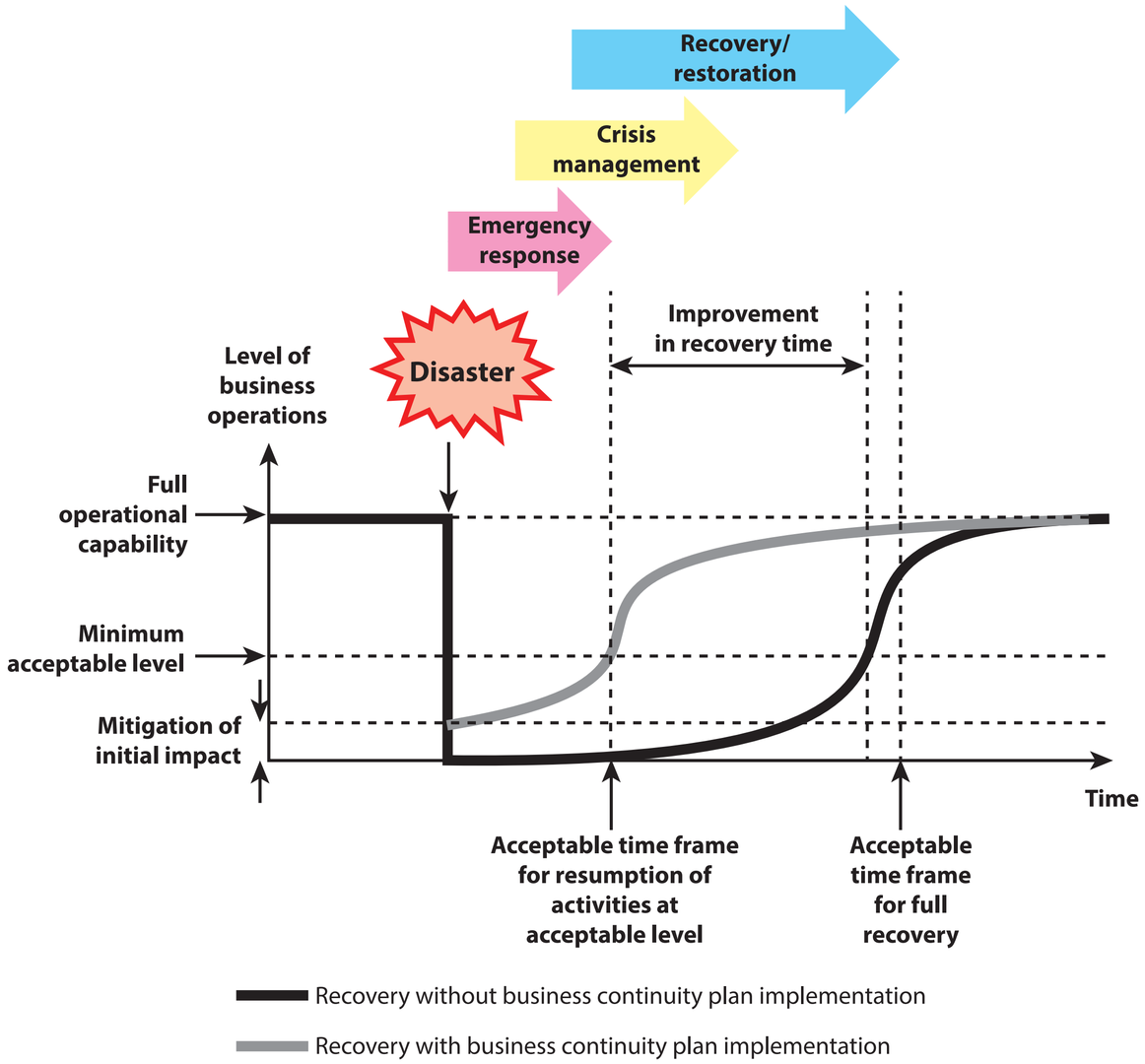
Enterprises **engage business continuity planning to reduce the consequences of any disruptive event** to a manageable level

Continuity of Operations (COOP)

An effort in an organization to **ensure that it can continue to perform the essential business functions during a wide range of emergencies**, including localized acts of nature, accidents, and **technological or attack-related emergencies**.

Business Continuity Management

GENERAL DEFINITION



In essence, **business continuity management is concerned with mitigating the effects of disasters.** There are the two ways in which business continuity management achieves that mitigation. The relative distances depicted in the figure imply no specific time scales. **The gray curve** shows the pace of recovery from a **disaster with** a business continuity plan in place, and **the black curve** shows the typical recovery pace **without** a business continuity plan.

When a disaster occurs, **the worst-case scenario is that it has the potential to bring some business processes or functions to a complete halt**. A business continuity plan includes resilience properties and quick or instantaneous switchover mechanisms that mitigate this initial impact.

A **business continuity plan** also calls for the implementation of capabilities and procedures that result in more rapid restoration of operational capability.

Essential Components for Maintaining Business Continuity

An **organization's resilience is directly related to the effectiveness of its business continuity capability**.
The following key components that are essential to maintaining business continuity:

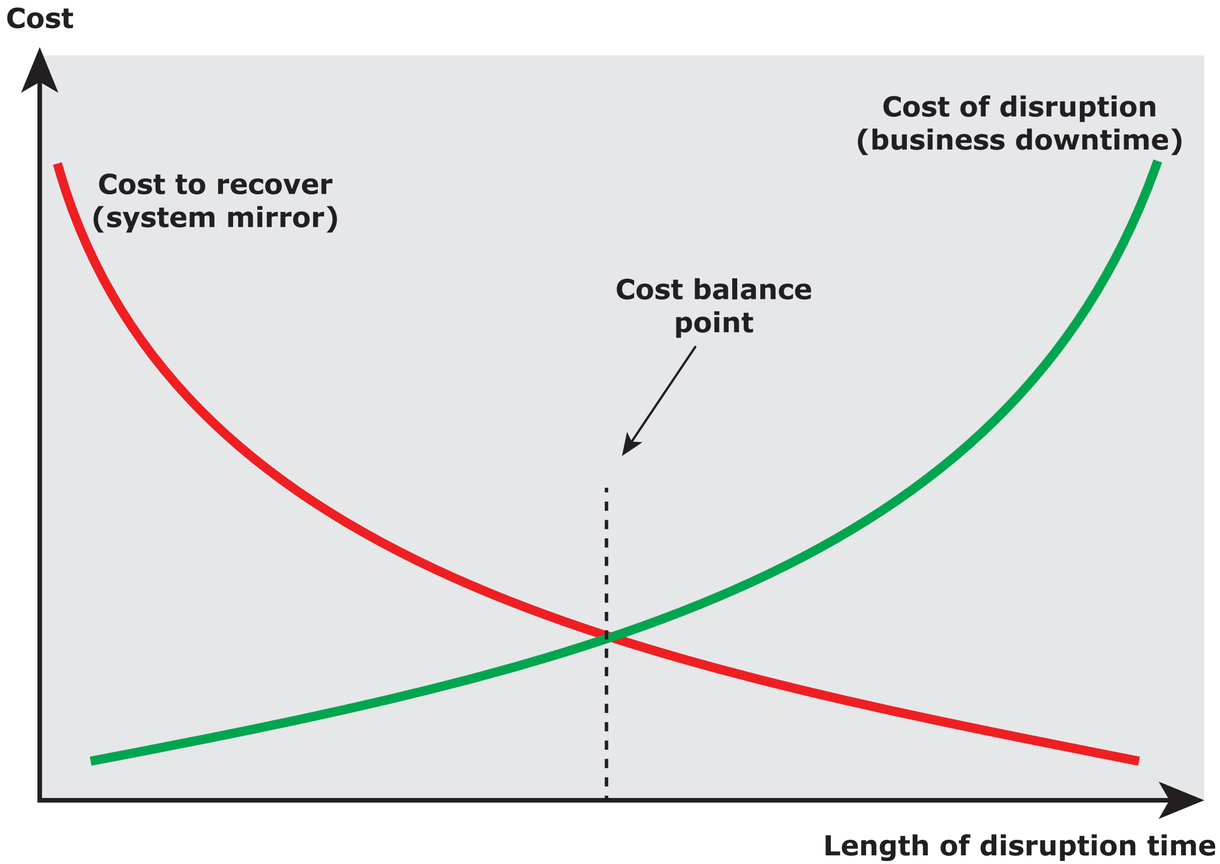
- **Management:** Continuity of **management is critical to ensure continuity** of essential functions. An organization should have a **detailed contingency plan** that indicates a clear line of succession so that designated backup individuals have the authority needed to maintain continuity when key managers are unavailable.

- **Staff:** There is a twofold requirement with respect to staff. First, **all staff should be trained** on how to maintain continuity of operations (COOP) or restore operations in response to an unexpected disruption. Second, the organization should develop guidelines for vertical **training** and cross training so that staff can take on functions **of peers** and those above and below them in the reporting hierarchy, as needed.

- **ICT systems:** A top priority following a disruption is communications, both internal and external. Communication systems and technology should be interoperable, robust, and reliable. An organization should **identify critical IT systems and have backup** and rollover capabilities tested and in place

- **Buildings and equipment:** This component includes the buildings where essential functions are performed. **Organizations should have separate backup locations available** where management and business process functions can continue during disruptions that in some way disable the primary facility. This component also covers essential equipment and utilities.

Cost Balancing for Business Continuity Management



A **business continuity strategy** involves considering the costs/benefits of any proposed strategy.

There is a trade-off that management needs to consider.
The cost of disruption derives from the business impact analysis and risk assessment. Against that is the **cost of resources** to implement a business continuity program. Typically, the longer a disruption continues, the more costly it becomes for the organization. But the shorter the RTO, the more costs are incurred. For example, for **short recovery times, an organization may require a mirror data site that is always active and updated**, whereas a longer RTO may enable the enterprise to rely on a less costly tape backup system.

Recovery time objective (RTO)

The **target time set for recovery** of product, service, or activity delivery after an incident. It is the maximum allowable downtime that can occur or the time in which systems, applications, or business functions must be recovered after an outage.

Business Continuity Resilience

Resilience of the infrastructure, assets, and procedures of an enterprise—referred to as information system resilience—**improves the organization's ability to withstand and recover from disruptive events**.

Elements of business resilience (common strategies):

Recovery

The provision for safe, rapid, offsite data recovery in the event of a disaster

Hardening

The fortification of all or part of an infrastructure to make it less susceptible to natural disaster, employee error, or malicious actions

Redundancy

The duplication of all or part of the infrastructure to supply hot, active backup service in the event of an unanticipated event

Offensive measures that go beyond traditional approaches to resilience:

Accessibility

If the primary work site is inaccessible, accessibility measures enable enterprise personnel, partners, and customers to access the infrastructure from other locations

Diversification

Diversification measures entail the physical distribution of resources (hard assets and people) and implementation of diverse communication pathways

Automation

The inclusion of self-managed hardware and software components in the infrastructure

SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Simone **Soderi**

simone.soderi@unipd.it

M3.5 - Cybersecurity Operations and Management

Thanks for your attention!