Certified Information Systems Security Professional (CISSP) Certification Training Course

Domain 07: Security Operations

Learning Objectives

By the end of this lesson, you will be able to:

- Understand and comply with investigations
- Apply foundational security operations concepts
- Apply resource protection
- Operate detective and preventive measures
- Implement disaster recovery (DR) processes
- Test disaster recovery plans (DRP)
- Participate in business continuity (BC) planning and exercises
- Implement and manage physical security

Introduction to Security Operations

Importance of Security Operations: Case Study

Kevin, as a part of his preparation for the CISSP exam, read the Operational Security policy of Nutri Worldwide Inc.
There were clear guidelines on the operations and escalation matrix listed the steps that the operations personnel should follow when they do not have the authorization to perform a specific action.

The policy also clearly outlined the roles and responsibilities with the level and scope of the operations personnel authorization. It also defined the disciplinary actions to be taken in case of breaches.
Kevin understood that the policy played an important role in acting as a deterrent against deliberate misconfigurations.

Understand and Comply with Investigations

Introduction to Investigation

Investigation

- An investigation is a systematic, minute, and thorough attempt to learn the facts about something complex or hidden. It is often formal and official.
- Example: Investigation of a bank failure
- Digital investigations involve investigations of all crimes conducted using computer and related technologies where the evidence exists in an electronic or a digital form or in a storage or on a wire.
- Investigation of computer crimes is also known as computer forensics.

Introduction to Investigation

Operational investigation

Criminal investigation

Regulatory investigation

Civil investigation

Operational Investigation

Operational investigations examine issues related to the organization's computing infrastructure and have the primary goal of resolving operational issues.

Operational investigations have the loosest standards for collection of information.

Criminal Investigation

Criminal investigations, typically conducted by law enforcement personnel, investigate the alleged violation of criminal law.

Most criminal cases must have the evidence that proves the crime beyond a reasonable doubt.

Criminal investigations may result in charging suspects with a crime and the prosecution of those charges in a criminal court.

Civil Investigation

Civil investigations typically do not involve law enforcement but rather involve internal employees and outside consultants working on behalf of a legal team.

Most civil cases do not follow the beyond a reasonable doubt standard of proof. Instead, they use the weaker preponderance of the evidence standard.

They prepare the evidence necessary to present a case in a civil court resolving a dispute between two parties.

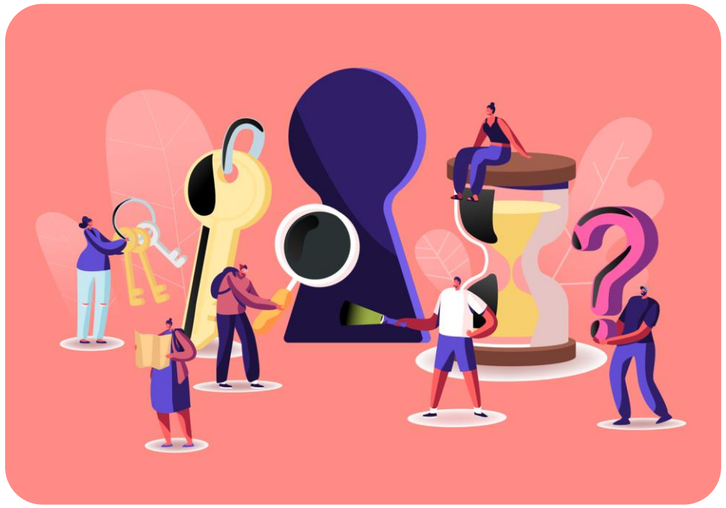
Regulatory Investigation

Government agencies may conduct regulatory investigations when they believe that an individual or a corporation has violated administrative law.

Regulatory investigations vary widely in scope and procedures and are almost always conducted by government agents.

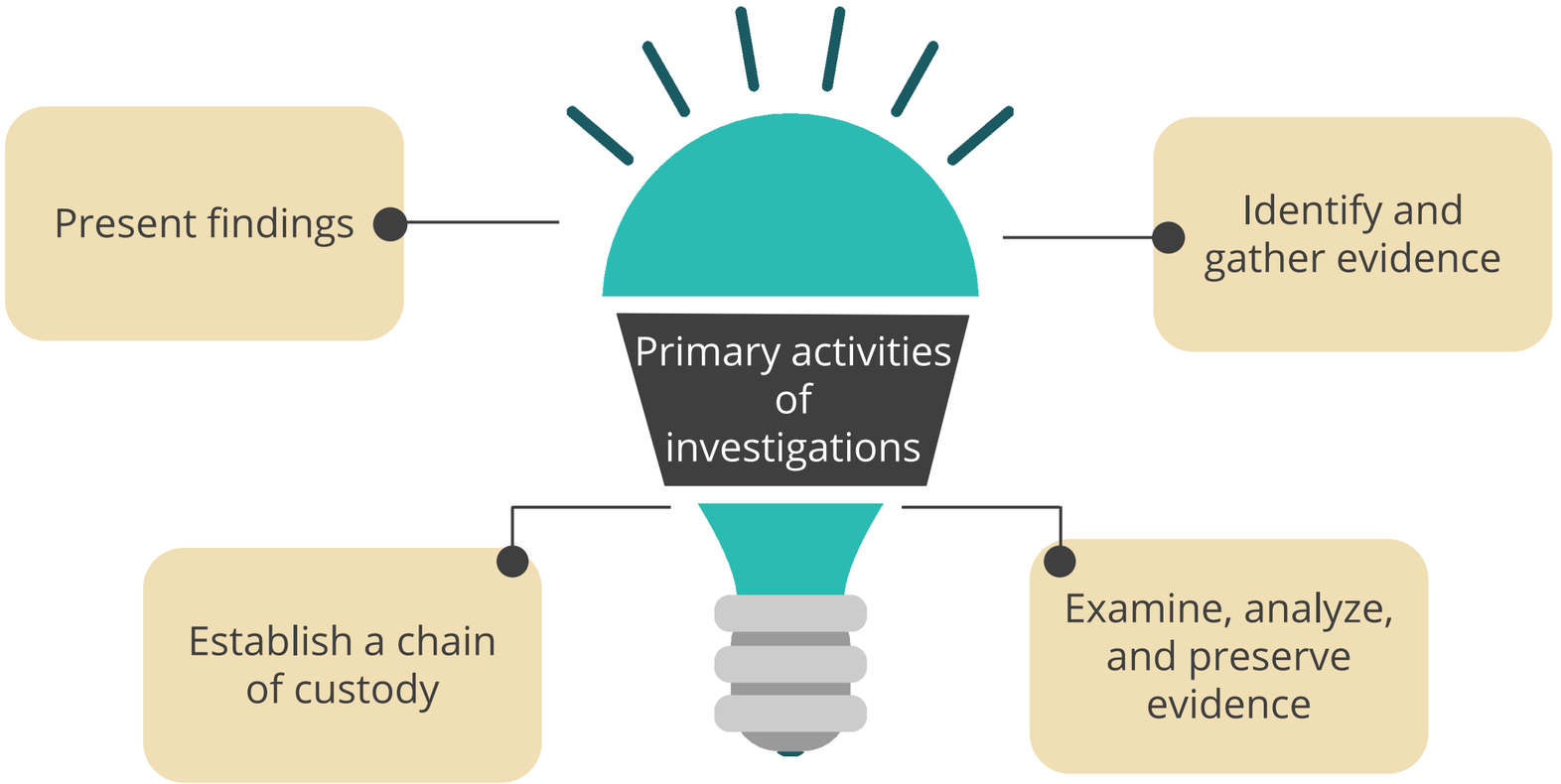
Investigation Challenges

1. Compressed time frame for the investigation
2. Intangible information
3. Difficulty in gathering the evidence
4. The investigation may interfere with the normal conduct of the business of an organization
5. Data associated with the criminal investigation may be located on a common computer that is used for the normal conduct of business
6. An expert or a specialist is required to retrieve data
7. Locations involved in the crime may be geographically separated by long distances in different jurisdictions



Investigation: Primary Activities

A crime scene is the environment where the potential evidence may exist. The security professional must understand the crime scene before starting to identify and collect the evidence.



Crime Scene

Best practices to handle evidence at a crime scene

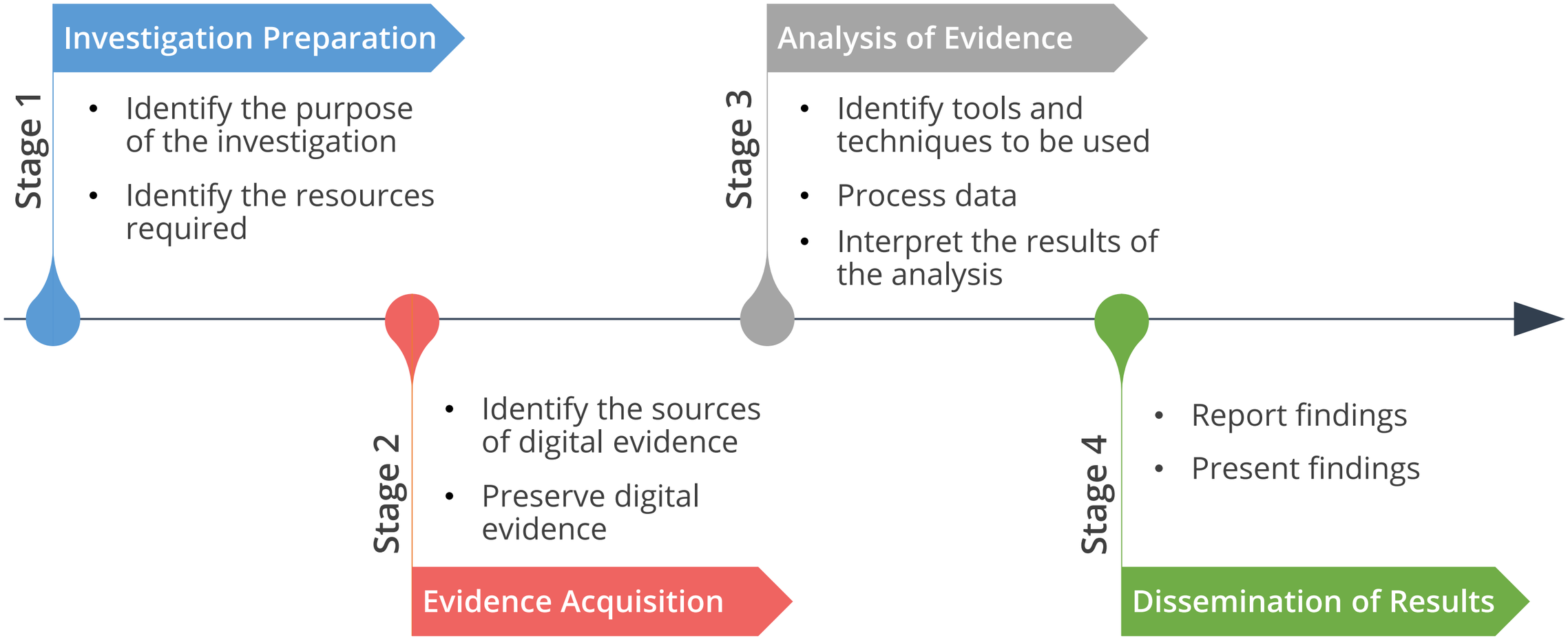
- Identifying the crime scene
- Protecting the environment
- Identifying evidence
- Identifying the potential sources of evidence
- Collecting evidence
- Reducing the degree of contamination

Digital Forensics

Digital forensics, sometimes known as digital forensic science, is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to cyber crimes.

The goal of digital forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing, and presenting facts and opinions about the digital information.

Forensic Process



Forensic Investigation Guidelines

Best practices according to Forensic Australian Computer Emergency Response Team

- Minimize handling or corruption of the original data
- Account for any changes and keep detailed logs of your actions
- Comply with the five rules of evidence
- Do not exceed knowledge and take the aid of experts and specialists if required
- Follow local security policies and obtain written permission
- Capture an accurate image of the system as possible
- Be prepared to testify
- Ensure actions are repeatable
- Work fast and proceed from volatile to persistent evidence
- Do not run any programs on the affected system

Information source: https://www.auscert.org.au/publications/2017-09-11-collecting-electronic-evidence-after-sy

Forensic Disk Controller or Write Blocker

Forensic Disk Controller

- A forensic disk controller or a hardware write-block device is a specialized type of computer hard disk controller made for the purpose of gaining read-only access to computer hard drives without the risk of damaging the drive's contents.
- The device is named forensic disk controller because its most common application is used in investigations where a computer hard drive may contain evidence.

Functions of a Forensic Disk Controller

- A hardware write-block (HWB) device will not transmit a command to a protected storage device that modifies the data on the storage device.
- An HWB device will return the data requested by a read operation.
- An HWB device will return without modification any access-significant information requested from the drive.
- Any error condition reported by the storage device to the HWB device will be reported to the host.

Forensics Investigative Assessment Types

Network Analysis

- Traffic analysis
- Log analysis
- Path tracing

Media Analysis

- Disk imaging
- Timeline analysis
- Registry analysis
- Shadow volume analysis

Software Analysis

- Reverse engineering
- Malicious code review
- Exploit review

Hardware or Embedded Device Review

- Dedicated appliance attack points
- Firmware and dedicated memory inspections
- Embedded operating systems, virtualized software, and hypervisor analysis

Evidence

- The available body of facts or information indicating whether a belief or proposition is true or valid.
- Evidence, broadly construed, is anything presented in support of an assertion.

Evidence

- Digital evidence or electronic evidence is any probative information stored or transmitted in the digital form that a party may use at a trial in court.

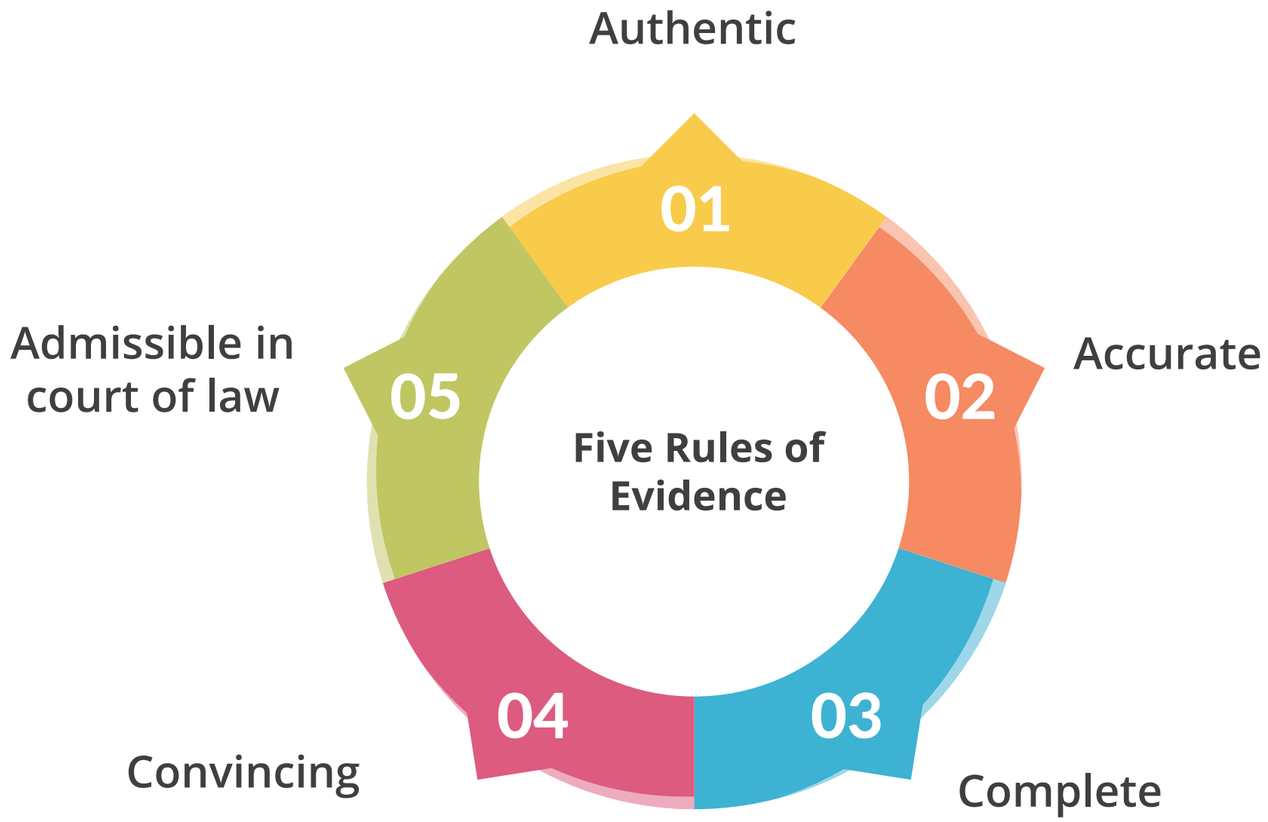
Digital Evidence

Evidence

- It is related to the crime.
- It can provide information describing the crime.
- It can provide information regarding the motives of the perpetrator.
- It can verify what has occurred.
- It can determine the time of occurrence of the crime.

Evidence is relevant when:

Evidence


Authentic
01
Accurate
02
Complete
03
Convincing
04
Admissible in court of law
05
Five Rules of Evidence

Admissible Evidence

There are three basic requirements for evidence to be introduced in a court of law. To be considered admissible evidence, it must meet all three of these requirements, as determined by the judge prior to being discussed in an open court:

Relevant:

The evidence must be relevant to determining a fact.

Material:

The fact that the evidence seeks to determine must be material, that is, related to the case.

Competent:

The evidence must be competent which means it must have been obtained legally. Evidence that results from an illegal search would be inadmissible, because it is not competent.

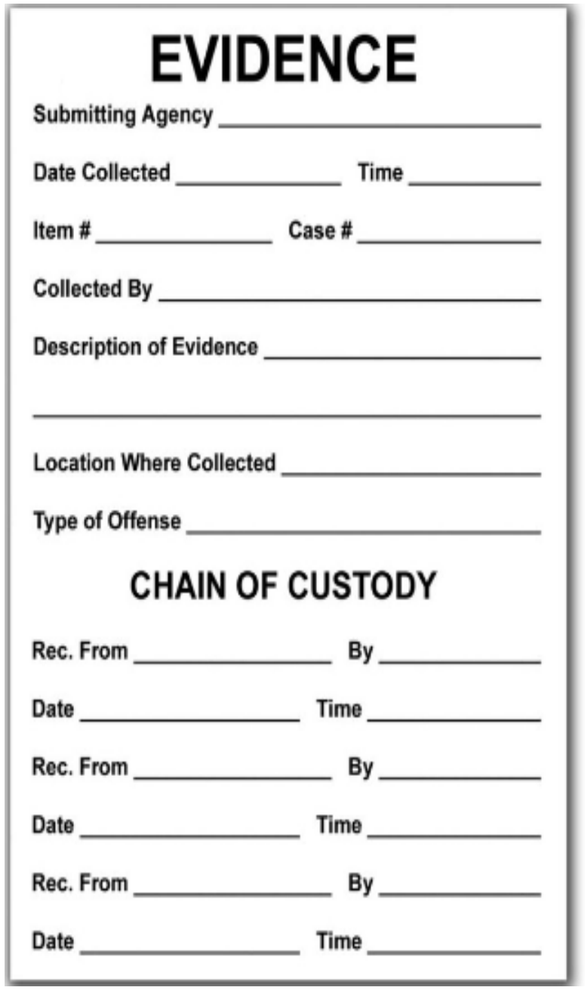
Evidence Life Cycle

The gathering, control, storage, and preservation of evidence are extremely critical in any legal investigation. The major components of an evidence life cycle are given below:

Chain of Custody

Chain of Custody (CoC)

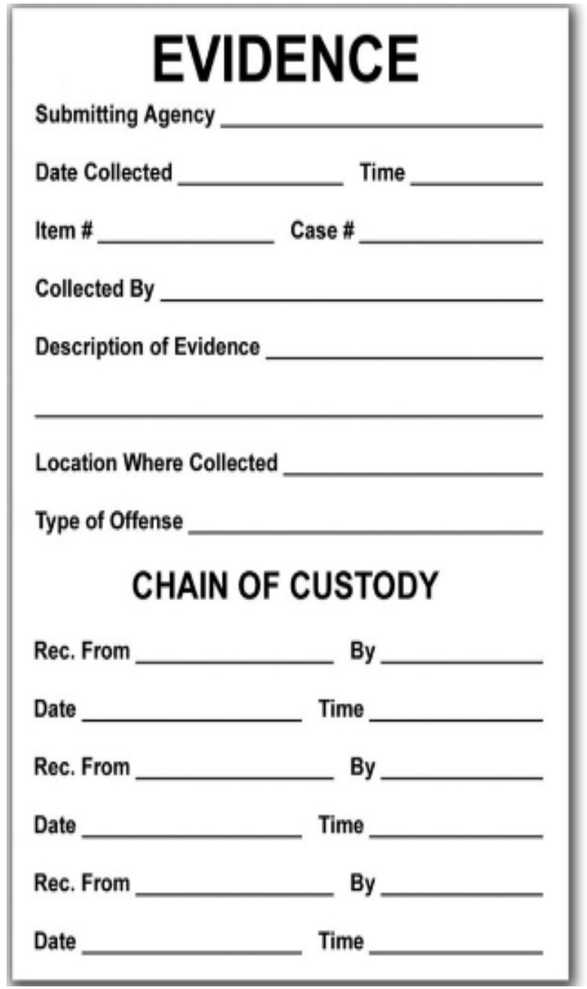
- In legal context, it refers to the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence.
- Chain of custody shows how the evidence was collected, analyzed, transported, and preserved to be presented in court.



Chain of Custody

Major components of the Chain of Custody

- Location of evidence when it was obtained
- Time at which evidence was obtained
- Identification of individual(s) who discovered evidence
- Identification of individual(s) who secured evidence
- Identification of individual(s) who controlled evidence and individual(s) who maintained possession of that evidence



EVIDENCE

Submitting Agency _____

Date Collected _____ Time _____

Item # _____ Case # _____

Collected By _____

Description of Evidence _____

_____

Location Where Collected _____

Type of Offense _____

CHAIN OF CUSTODY

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

Evidence Collection Guidelines

Scientific Working Group on Digital Evidence (SWGDE) Guidelines:

- When dealing with digital evidence, one must apply all of the general forensic and procedural principles.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access the original digital evidence, that person should be first trained for the purpose.

Evidence Collection Guidelines

Scientific Working Group on Digital Evidence (SWGDE) Guidelines:

- All activities related to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in his possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

E-Discovery

Electronic discovery, also called e-discovery, refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

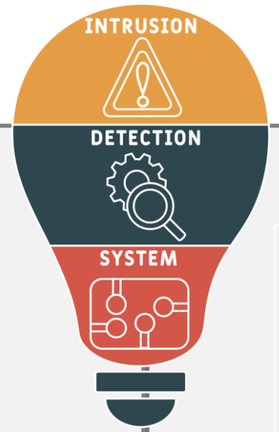
This discovery process applies to both paper records and electronic records.

Electronic discovery process facilitates the processing of electronic information for disclosure.

Conduct Logging and Monitoring Activities

Intrusion Detection System

An Intrusion Detection System (IDS) detects any unauthorized intrusion in a network, server, or system. The IDS tool is used to detect suspicious activity on the network and send an alarm to the network administrator.



IDS Types

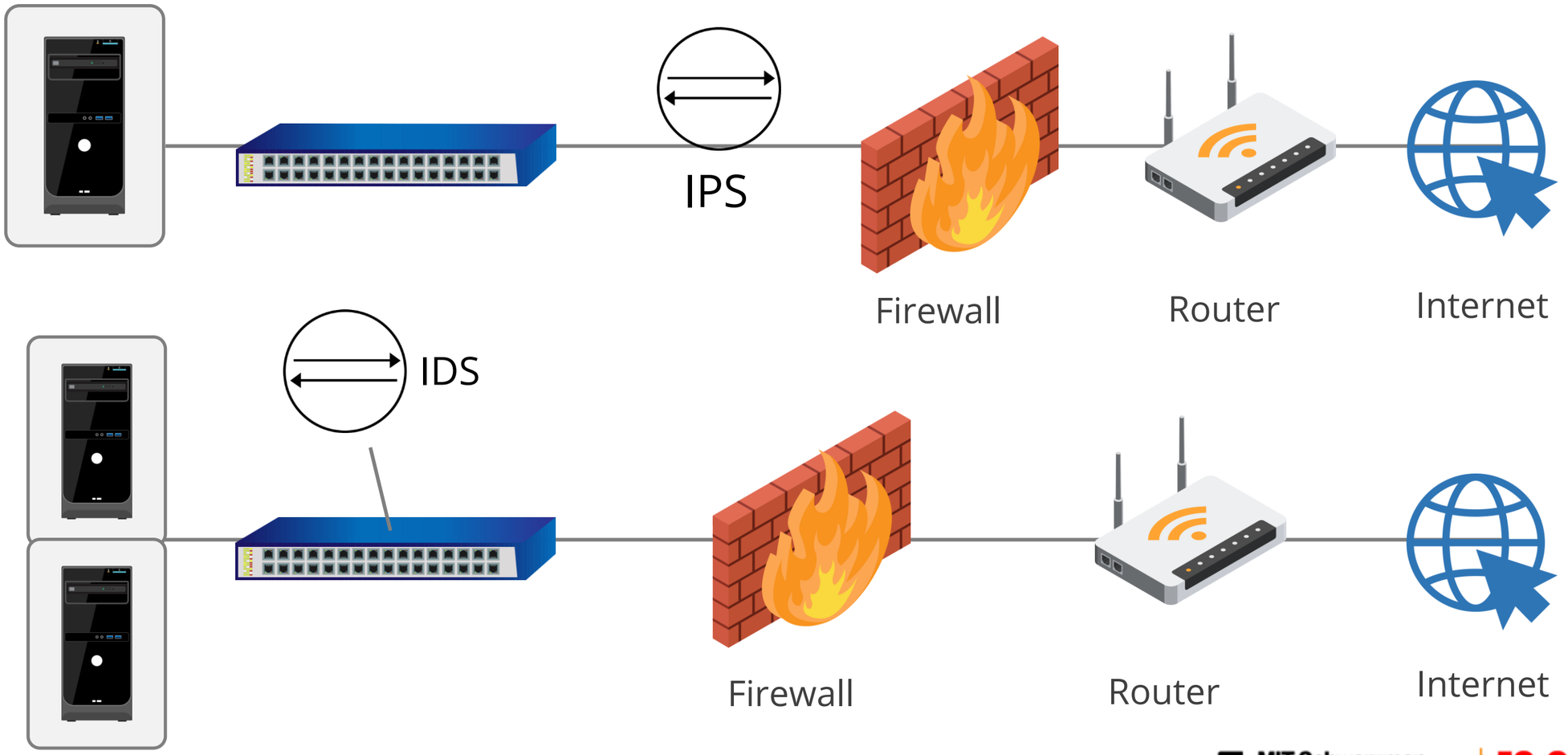
- Network-based IDS (NIDS): Dedicated appliances or a system having its Network Interface Card (NIC) in promiscuous mode and with the necessary software installed
- Host-based IDS (HIDS): Monitors for malicious or anomalous activity on a workstation or a server

HIDS and NIDS Types

- Signature-based
- Statistical anomaly-based: Traffic anomaly, protocol anomaly
- Rule-based: Model-based, stateful matching

Intrusion Prevention System

IPS is used to detect and prevent any malicious traffic or activity to gain access to the target.



Security Information and Event Management

- It is a term for software products and services combining security information management (SIM) and security event management (SEM).
- SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

Security Information and Event Management

FIGURE 2.13 The SIEM system

Security Information and Event Management

Components of SIEM:

Security event management (SEM):

The segment of security management that deals with real-time monitoring, correlation of events, notifications, and console views is commonly known as SEM.

Security information management (SIM):

The second area provides long-term storage, analysis, and reporting of log data.

SIEM Functionality

Security Information and Event Management

- Data aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
- Forensic analysis
- Automated response

Continuous Monitoring

A continuous monitoring system must meet the organization's security requirements. The security architect must design and implement a continuous monitoring program that protects the organization's critical information assets.

The security practitioner must be acquainted with Continuous Monitoring as a Service (CMaaS). There are many agencies that offer CMaaS such as, General Services Administration (GSA) and Federal Acquisition Service (FAS).

Egress Filtering

Egress filtering prevents any unauthorized or malicious traffic to leave the internal network. Information flowing from the internal network to the internet is monitored and controlled. TCP/IP packets that are being sent out of the internal network are examined through a router, firewall, or a similar edge device.

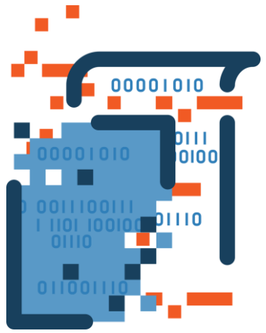
Egress filtering should comply with the standards and regulations

Example: Payment Card Industry Data Security Standard (PCI DSS) requires egress filtering from any server in the cardholder environment.

Data Loss or Leak Prevention (DLP)

Data Loss or Leak Prevention (DLP) helps an organization to prevent the loss of its sensitive data.

Data Loss or Leak Prevention (DLP)



The key objectives of DLP include:

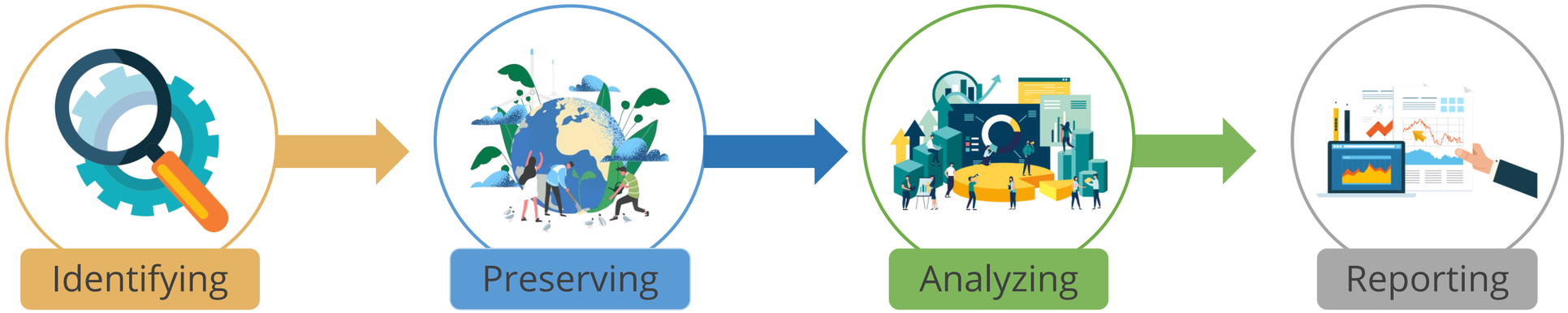
- Locating and cataloging critical information stored throughout the enterprise
- Monitoring and controlling the sensitive information flow across enterprise networks and end-user systems

Some of the benefits of DLP include:

- Protects sensitive data and intellectual property of an organization
- Meets compliance requirements
- Reduces security breaches

Digital Forensics Tools, Tactics, and Procedures

The diagram given below shows the forensic computing process.



Information source: https://www.auscert.org.au/publications/2017-09-11-collecting-electronic-evidence-after-sy
and
https://www.sans.org/reading-room/whitepapers/incident/computer-forensics-weve-incident-investigate-652

Artifacts

- Artifacts are forensic objects that may contain data or evidence relevant to the investigation.
- Artifacts can be a physical or a logical item such as a file in the laptop or the laptop itself.
- Investigators must identify and collect artifacts in their custody as evidence.

Examples include:

Threat Intelligence

Threat intelligence is the process of planning, collecting, processing, analyzing, and disseminating information that poses a threat to an organization and the application of this knowledge in mitigating the threat.

Threat intelligence collects information generated from a variety of internal and external sources in real-time for identifying threats.

Threat intelligence helps to process threat data to better understand the attackers, respond faster to incidents, and proactively get ahead of the attacker's next move.

Threat Intelligence

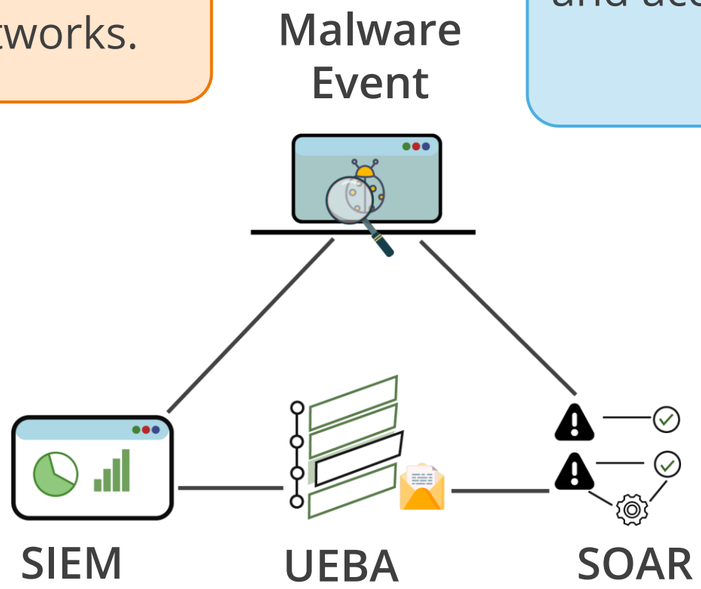
Cyber threat intelligence sources include:

- Open-source intelligence
- Social media intelligence
- Human Intelligence
- Technical intelligence
- Intelligence from the deep and dark web

User and Entity Behavior Analytics (UEBA)

User and Entity Behavior Analytics (UEBA) is a cyber threat detection technology that uses machine learning and deep learning technologies to model the behavior of users and devices on corporate networks.

UEBA can identify abnormal behavior, determine if it has security implications, and accordingly alert the security team.



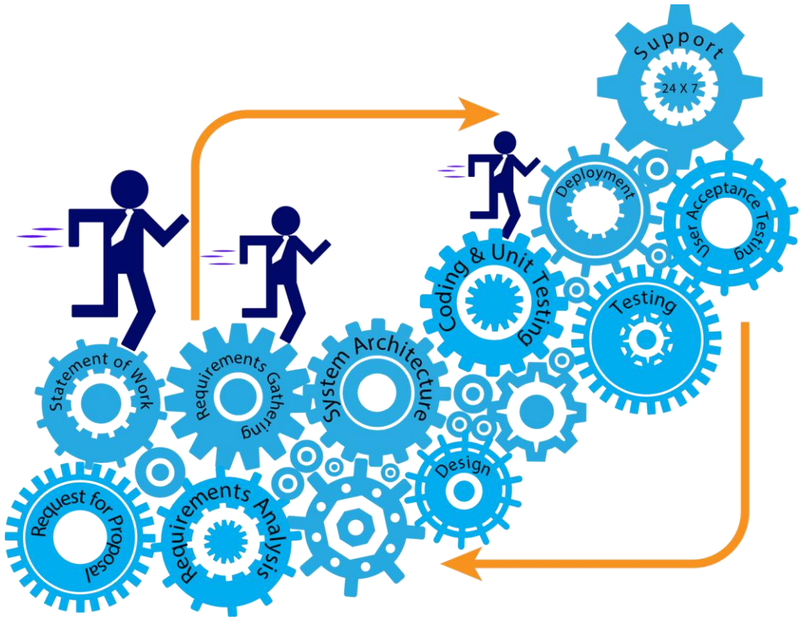
User and Entity Behavior Analytics (UEBA)

User	UEBA technology can monitor user behavior for any peculiar or suspicious behavior.
Entity	UEBA technology can monitor other entities besides users such as routers, servers, applications, or even IoT devices.
Behavior	It establishes baseline of **normal** behavioral profiles and patterns and then identifies anomalies that deviate from that baseline, which have security significance.
Analytics	The analytics tools based on **AI and machine learning** algorithms do not require signatures or human intervention and provide automated, accurate threat and anomaly detection.

Perform Configuration Management

Configuration Management

- Configuration management is a formalized higher-level process of managing changes in a complicated system.
- Change control falls under configuration management.



Configuration Management

Configuration management applies technical and administrative directions to:

Identify and document the functional and physical characteristics of each configuration item

Report the status of change processing and implementation

Manage changes

Configuration Management

An organized and consistent plan should cover the following items:

- Description of physical and media controls
- Electronic transfer of software
- Communication software and protocols
- Encryption methods and devices
- Security features and limitations of software
- Hardware requirements, settings, and protocols
- System responsibilities and authorities

Baselining

A baseline defines the common minimum requirements of a service, product, or infrastructure that has been formally reviewed and accepted as the basis for further activities.

Baseline controls can be applied to policies, standards, procedures, responsibilities, requirements, impact assessments, and software-level maintenance.

Provisioning

Provisioning is the process of setting up IT infrastructure.

Infrastructure as code is the approach of automating the provisioning of infrastructure through code instead of manual processes.

Configuration Automation

Configuration automation is the process of automating the deployment and configuration of applications, servers, middleware, databases, and other IT infrastructure for both on-premises and cloud data centre environments.

Benefits:

- Increases operational efficiency
- Enforces compliance policies and reduces risks
- Prevents data center outages caused by configuration drifts
- Establishes best practices to change life cycle management

Apply Foundational Security Operation Concepts

Controls for Protecting Assets: Administrative Controls

The administrative controls include:

Personnel security	Mandatory Vaccination	Personnel security	Separation of duties and responsibilities
Ensure quality levels of the personnel; employment screening or background checks refer to pre-employment screening	Detect evidence of fraud	Action taken when employees violate the published computer behavior standards	Divide the security-sensitive tasks in various parts and assign to several individuals

Controls for Protecting Assets: Administrative Controls

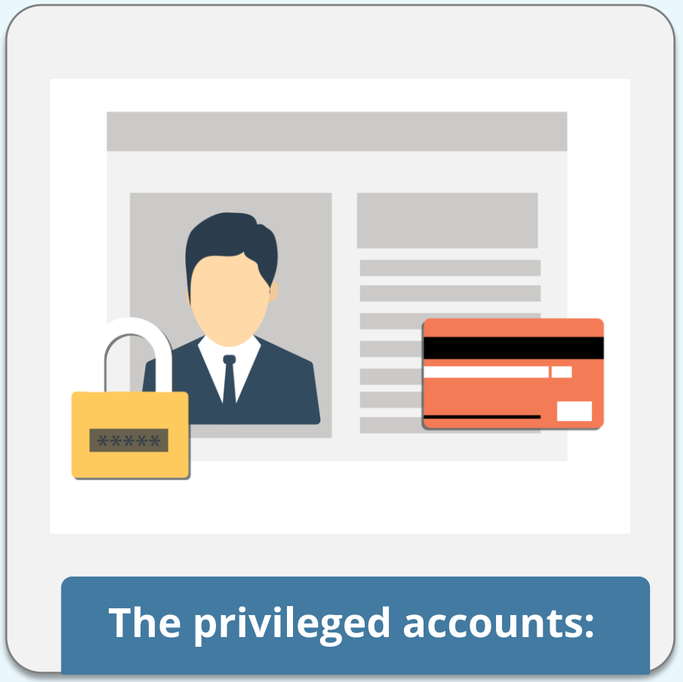
The administrative controls include:

Least privilege	Need to know	Change control	Record retention and documentation control
Restrict the set of privileges	Provide minimum information to perform an assigned task	Protect a system from unauthorized changes	Administer security controls on documentation and procedures

Need for Controlling Privileged Accounts

Accounts with greater privileges are distinct from less privileged user accounts.

- Have extensive powers on a given system
- If compromised, the attacker could damage the system
- Need regular monitoring as they can be misused
- Are controlled by security operations
- Require a defined procedure



Identity and Access Management

Identity management controls the life cycle process of every account in a system, from provisioning of the account to its eventual removal from the system.

Access management refers to the assignment of rights or privileges to accounts, which will allow them to perform their intended function.

Identity and access management (IAM) solutions focus on harmonizing the user provisions and access management across multiple systems with different native access control systems.

Types of User Accounts

The two types of user accounts are:

Privileged accounts

Possess extensive powers on a given system
The four types of accounts with different levels of privilege are root or built-in administrator accounts, service accounts, administrator accounts, and power user accounts

Ordinary user accounts

Assigned to most users with access limited by following the principles of least privilege and need-to-know

Monitoring Special Privileges

A security practitioner needs to validate and review the privileges granted to accounts.

- Only authorized users should be granted access for a required period of time.
- Access should only be granted based on user's clearances, thorough background checks, and the user's suitability for the role.
- Accounts should be validated and inactive accounts should be removed from the system based on the organization's policy.

Apply Resource Protection

Protecting Valuable Assets

Security operations should:

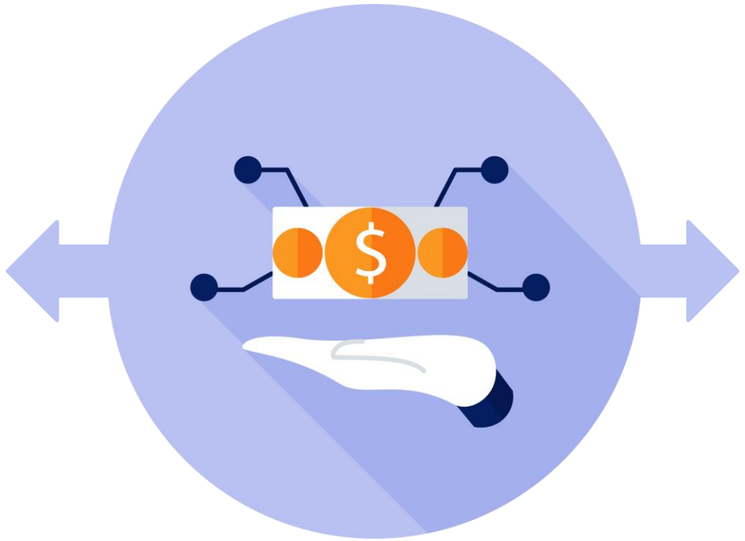
- Provide regular protection to human and material assets
- Maintain the security controls to protect sensitive or critical resources from being compromised

Assets can be:

- Tangible
- Intangible
- Both

Protecting Physical Assets

The security professional confirms the asset ownership, and security operations ensure the protection of physical assets.



The IT department plays the role of the owner as well as custodian of physical assets.

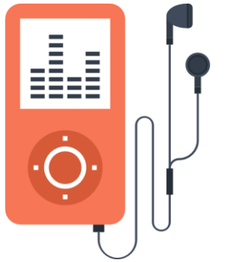
Protecting Physical Assets

The various types of physical assets are:

Facilities

Hardware

Software



Media

Protecting Information Assets

Information assets include all forms of information and types of intellectual properties. Information assets are hard to evaluate and delineate.

The important factors in protecting information assets are:

Information classification

Information labeling and handling

Access control

Accountability

Protecting Resources

Resource protection is the concept of protecting an organization's computing resources and assets from loss. Any software, hardware, or data owned and used by the organization are known as computing resources.

Protecting Resources

The resources that need protection are:

- Hardware resources: Routers, firewalls, switches, removable drives, file servers, workstations, disks, gateways, and printers
- Software resources: Program libraries, source code, vendor software, proprietary software, and operating system software
- Data resources: Backup data, user data files, password files, operating data directories, system logs, and audit trails

Controls for Protecting Assets: Hardware Controls

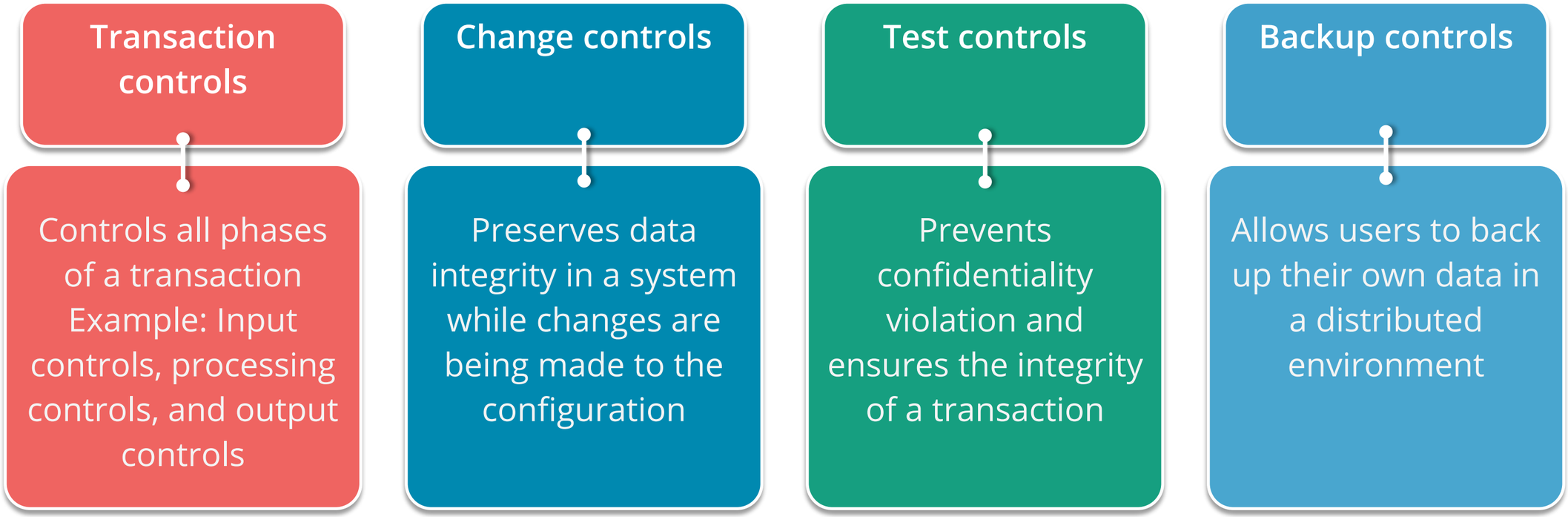
The hardware controls include:

Hardware maintenance:	Background investigations and escorting maintenance and service personnel as they have logical and physical access to the system
Account maintenance:	Changing the default passwords and disabling accounts
Diagnostic port controls:	Monitoring port usage by authorized personnel and block internal or external unauthorized access
Hardware physical controls:	Securing the server room, data center, and media storage with locks and alarms

Controls for Protecting Assets: Software Controls

Some of the elements of controls on software are antivirus management, software testing, powerful system utilities, and safe software storage.

The software controls include:



Controls for Protecting Assets: Media Controls

The media controls include:

Record retention

- Refers to the duration for which transactions and other types of records, such as legal documents, audit trails, and emails, should be retained
- This can be done according to management, legal, and audit or tax compliance requirements

Data remanence

Refers to the data left on the media after the data has been erased

Object reuse

- Refers to the reassignment to some subject of a storage medium, such as page frame, disk sector, and magnetic tape, that contains one or more objects
- To be securely reassigned so that no residual data is available to the new subject through standard system mechanisms

Conduct Incident Management

Incident Management

Event

Any observable occurrence in a system or a network

Incident

Any event that negatively affects the company and impacts its security posture

Incident response

A practice of detecting a problem, determining its cause, minimizing the damage it causes, resolving the problem, and documenting each step of the response for future references

Incident Response Goals

The goals of incident response are:

Reduce the potential impact to the organization

Provide management with sufficient information

Deter attacks through investigation and prosecution

Maintain or restore business continuity

Defend against future attacks

Incident Response Team

An incident response team is a group of people who prepare for and respond to emergencies.

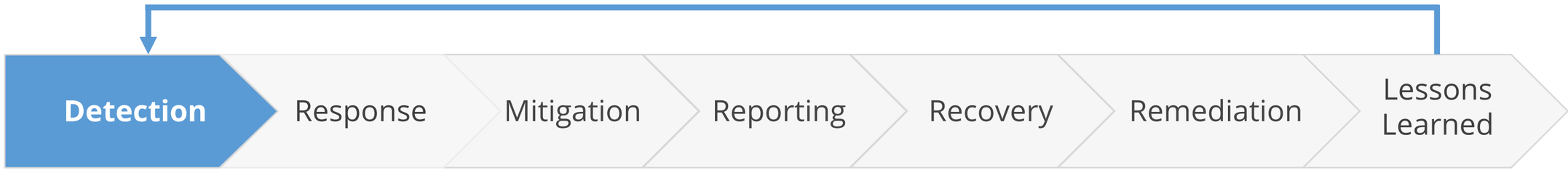
Basic checklist of an incident response team

- A list of outside agencies and resources to contact or report to
- An outlined list of roles and responsibilities
- A call tree to contact the defined roles and outside entities
- A detailed procedure to secure and preserve evidence
- A list of items that should be included in the report for the management and the courts
- A description of how different systems should be treated in a particular situation

Incident Management: Planning and Preparation

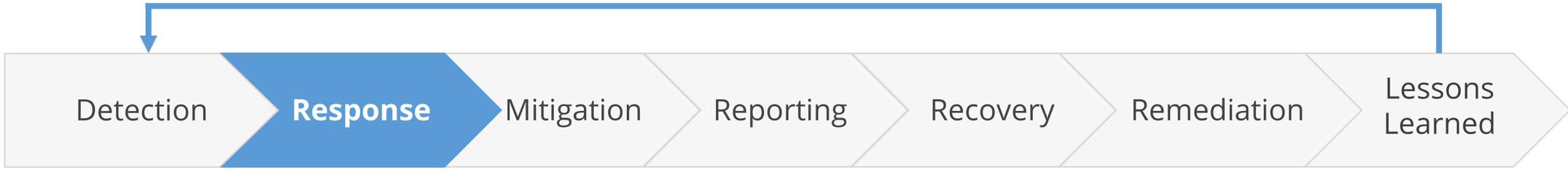
1. Incident response policy and procedures
2. Incident response handling methodologies
3. Communication plan for internal and external parties
4. Call tree and notification processes for solutions, products, and support teams
5. Regular skill development, improvement, and training for information security staff
6. Incident response plan tests and team drills
7. Collection of threat and vulnerability intelligence

Incident Response Life Cycle



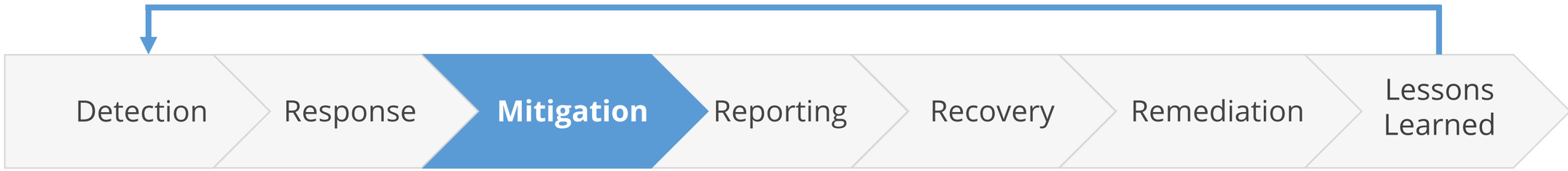
- Automated detection capabilities include network-based and host-based IDPSs, antivirus software, and log analyzers.
- Manual detection includes problems reported by end users.

Incident Response Life Cycle



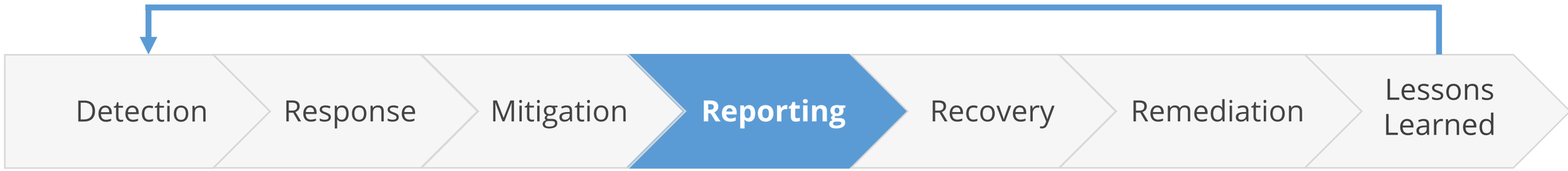
- The triage process will ensure that only valid alerts are promoted to **investigation or incident** status. False positives or incorrect alerts are identified and removed.
- Information is collected to investigate its severity and set priorities on how to deal with the incident.
- Incidents are categorized according to their severity level, level of potential risk, the source whether it is internal or external, its rate of growth, and the ability to contain the damage.
- More data is gathered to try and figure out the root cause of the incident.

Incident Response Life Cycle



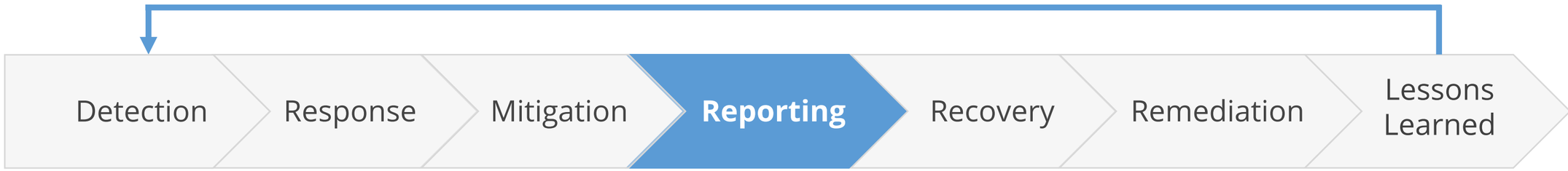
- The goal of mitigation is to prevent or minimize any further loss or damage from this incident so that you can begin to recover and remediate.
- Prioritizes the mitigation of most critical assets, followed by mitigation of less important assets.
- Isolation and containment can limit the exposure of your organization and prevent further damage.
- The response team needs to take its last forensic samples prior to commencing mitigation activities.

Incident Response Life Cycle



The incident response team should document and maintain the status of the incidents to help ensure that incidents are handled and resolved in a timely manner.

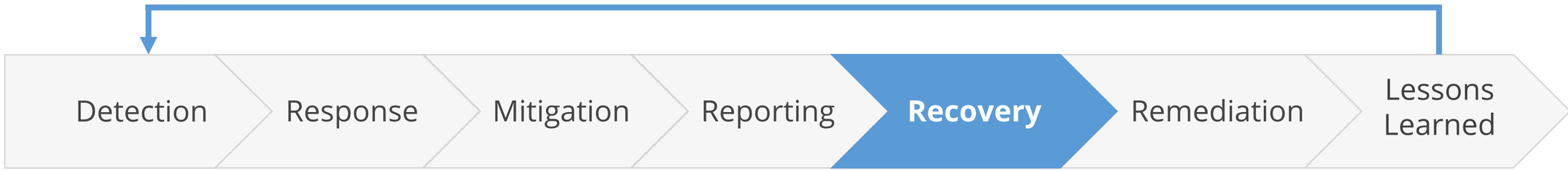
Incident Response Life Cycle



The document could contain the following information:

- The current status of the incident (new, in progress, forwarded for investigation, or resolved)
- Summary of the incident
- Related incidents
- Actions performed
- Chain of custody (if applicable)
- Impact assessment report
- List of evidence gathered
- Comments of incident handlers
- Next actions

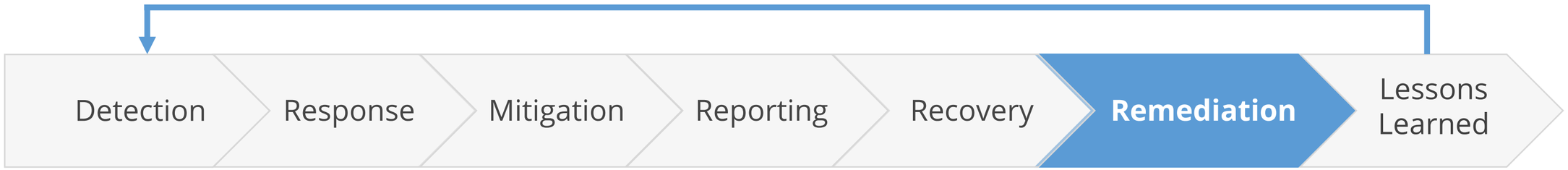
Incident Response Life Cycle



Recovery and repair phase is the process of restoring a system to its pre-incident condition. Recovery and repair activities include:

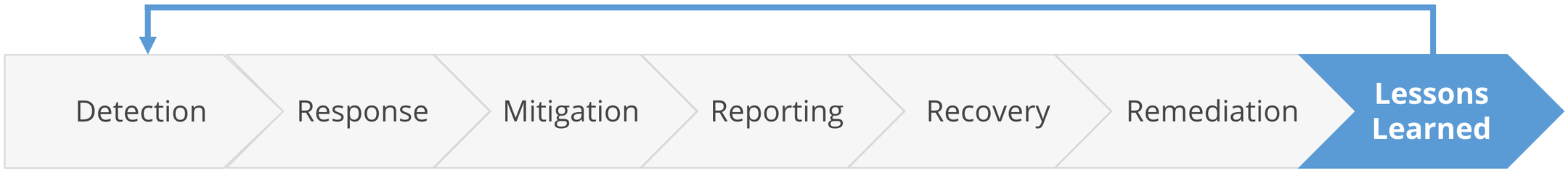
- Repairing or replacing hardware
- Reinstalling, reconfiguring operating system, or application software
- Removing unwanted programs and data
- Restoring damaged or missing data from the backup media

Incident Response Life Cycle



- Remediation is the post-incident repair of affected systems, communication and instruction to affected parties, and analysis that confirms the incident has been contained.
- Remediation involves measures to ensure that the particular attack will never again be successful against the organization.

Incident Response Life Cycle



- This final stage is often skipped as the business moves back into normal operations but it's critical to look back and heed the lessons learned.
- Holding a **lessons learned** meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, provides a chance to achieve closure with respect to an incident by reviewing what occurred, what was done to intervene, and how well intervention worked.
- A follow-up report for each incident provides a reference that can be used to assist in handling similar incidents in the future.

Operate and Maintain Detective and Preventive Measures

Firewalls

Network Firewall	These are purpose-built appliances for securing enterprise corporate networks.
Web Application Firewall (WAF)	WAF is designed to protect web applications and APIs from a variety of attacks, including automated (bots), injection and application-layer denial of service (DoS).
Next Generation Firewall (NGFW)	NGFW is a deep-packet inspection firewall that moves beyond port or protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.

Whitelisting and Blacklisting

Whitelisting

- Whitelisting **allows access** for only approved entities.
- The default is to **block access**.
- Whitelisting is **trust-centric.**

Blacklisting

- Blacklisting **blocks access** to suspicious or malicious entities.
- The default is to **allow access**.
- Blacklisting is **threat-centric.**

Third-Party Provided Security Services

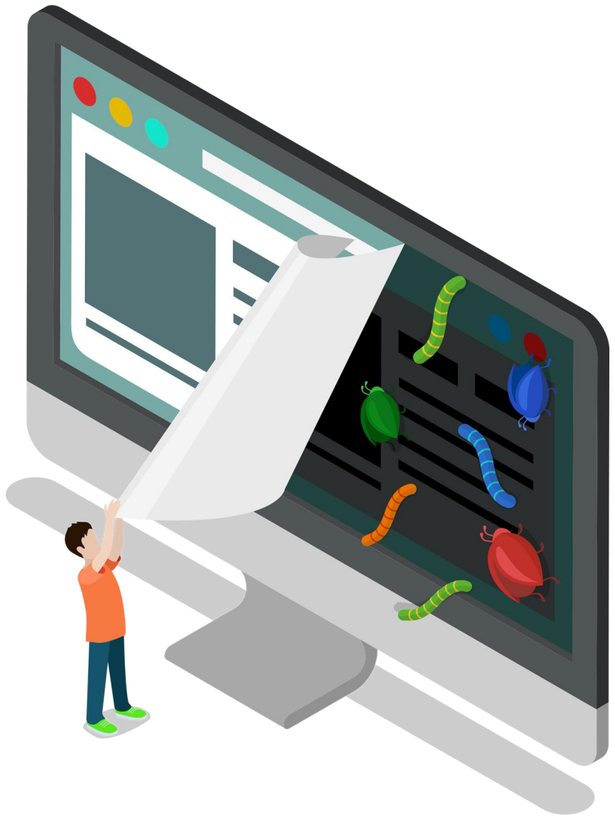
Security services provided by third-party are:

- Threat intelligence
- Vulnerability assessment and penetration testing
- Physical security
- Network management
- Audits and forensics

Sandboxing

Sandboxing is a technique used to safely evaluate the threat in an isolated test environment (sandbox).

- Sandboxing is used to test suspicious programs that may contain a virus or other malicious code in an isolated environment, without allowing the software to harm the host device.
- It provides effective protection against zero-day attacks and advanced threats.
- Suspicious email attachments are sent to a virtual sandbox that performs deep analysis for malicious activity.



Sandboxing

Virtualization

This approach uses a virtual machine (VM) based sandbox to contain and test suspicious programs in an isolated environment.

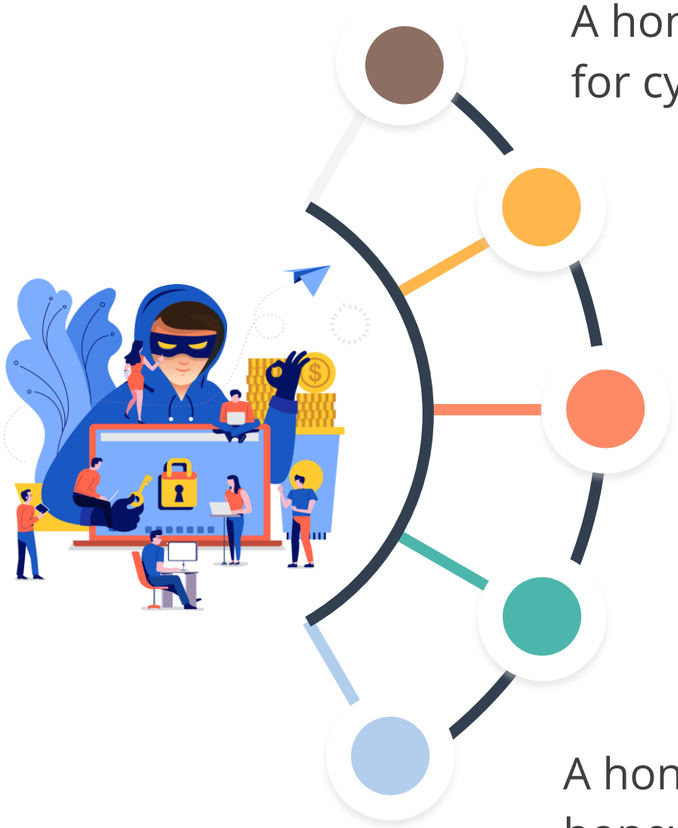
Hardware or Full System Emulation

The sandbox emulates the entire hardware, including CPU and memory, and I/O devices, providing deep visibility into program behavior and impact.

Operating Systems Emulation

The sandbox emulates the operating system but not the machine hardware which allows for greater visibility into what the malware is doing.

Honeypots and Honeynets



A honeypots is a decoy system intended to mimic likely targets for cyberattacks.

It is not hardened or locked down and has services enabled and open ports.

It is designed to confuse the attacker into thinking that it is a production server.

It does not contain anything sensitive or valuable data.

A honeynet is a decoy network that contains one or more honeypots.

Anti-Malware Systems

It is important to assess the risk of exposure to infection by malicious code or malware (viruses, worms, Trojan horses, and spyware), and respond to the risk by implementing anti-virus and anti spyware controls.

Anti-Malware Systems

Malware has the capacity to disrupt the operation of user workstations as well as servers, which could result in:

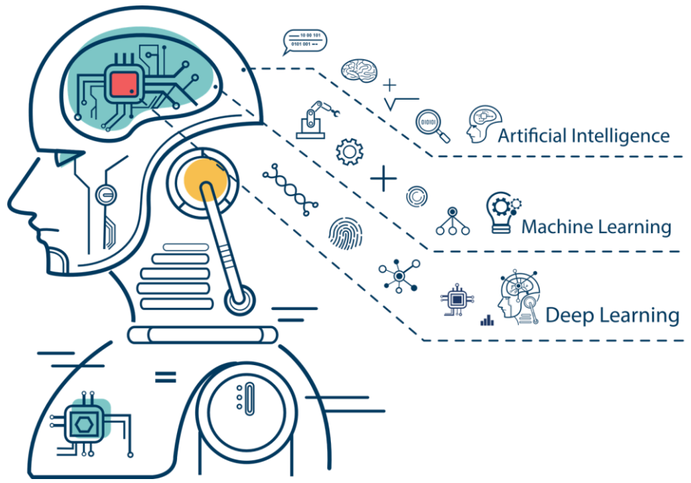
- Loss of business information
- Disclosure or compromise of business information
- Corruption of business information
- Disruption of business information processing
- Inability to access business information
- Loss of productivity

Protection against malware can be achieved by applying defense-in-depth and installing central anti-malware management.

Machine Learning and Artificial Intelligence (AI)

Artificial Intelligence

Engineering of computers to mimic human behavior



Machine Learning

Ability to learn without being explicitly programmed

Deep Learning

Learning based on deep neural network that can learn and make intelligent decisions on its own

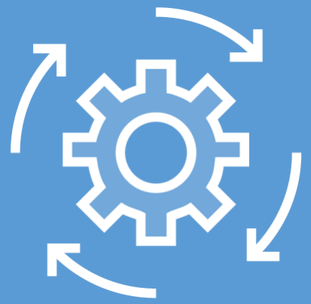
Machine Learning and Artificial Intelligence (AI)

Artificial Intelligence:

Engineering of computers to mimic human behavior

Machine Learning:

Ability to learn without being explicitly programmed



Deep Learning:

Learning based on deep neural network that can learn and make intelligent decisions on its own

ML and AI for Cybersecurity

Automate Tasks	Use machine learning to automate repetitive security tasks for higher levels of accuracy and in a fraction of the time
Threat Hunting	Search of recurrent patterns, anomalous behavior, and other outliers
Application Security	Automate code reviews with AI to help eliminate false negatives and false positives
Incident Investigation	Automatically investigate indicators of compromise and gain critical insights, to accelerate threat response times
Incident Response	Orchestrate and automate hundreds of time-consuming, repetitive and complicated response actions that previously required significant human intervention

Real World Scenario

Google tackles Gmail spam with Machine Learning:
Since its launch in 2004, Gmail has employed machine learning techniques such as neural networks to filter emails in its spam filters. Unlike rule-based spam filters, machine-learning models can adapt to varying conditions and hunt for patterns in unwanted emails that people may not catch. The machine learning model used by Google reportedly can detect and filter out spam, phishing emails, and malware with about 99.9 percent accuracy.

In 2019, Google integrated TensorFlow in Gmail to try and block the last 0.1% of spam emails from getting through. TensorFlow is an open-source machine learning (ML) framework developed at Google in 2015.

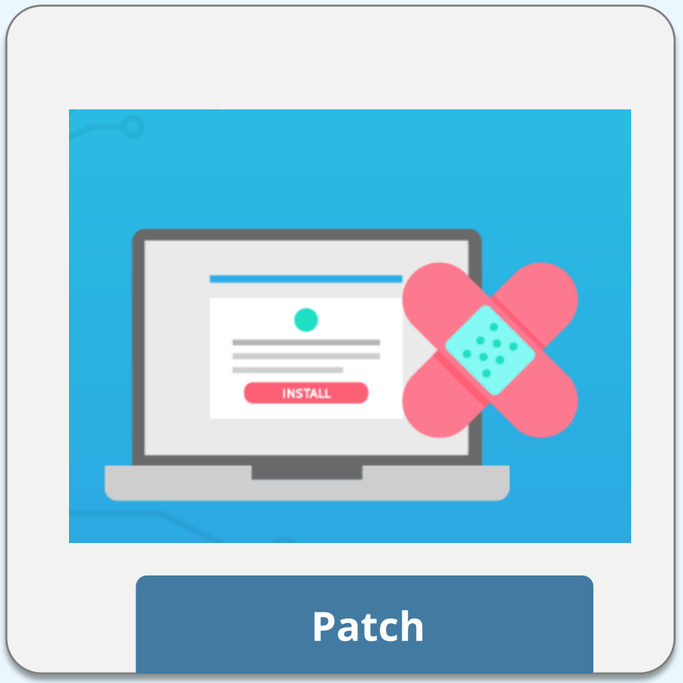
TensorFlow's advantage is that it allows Gmail's team to refine its existing machine learning algorithms so they're even more accurate at detecting spam. With TensorFlow, Google can also better personalize its spam protection for each user. The same email could be considered spam to one person but important information to another.

Gmail has announced that with TensorFlow it is now able to detect 100 million more spam emails every day.

Implement and Support Patch and Vulnerability Management

Patch Management

- A patch is a piece of software designed to fix problems and update a computer program.
- This includes fixing security vulnerabilities and bugs and improving usability and performance.



Patch Management

Patch management is the process of applying proper patches to a system at a specified time using a strategy and plan.

Patch management:

Types of Patches

Hotfixes

Small updates with a specific purpose that alter the behavior of installed applications in a limited manner

Service packs

Tested and cumulative set of all hotfixes, security updates, and critical updates

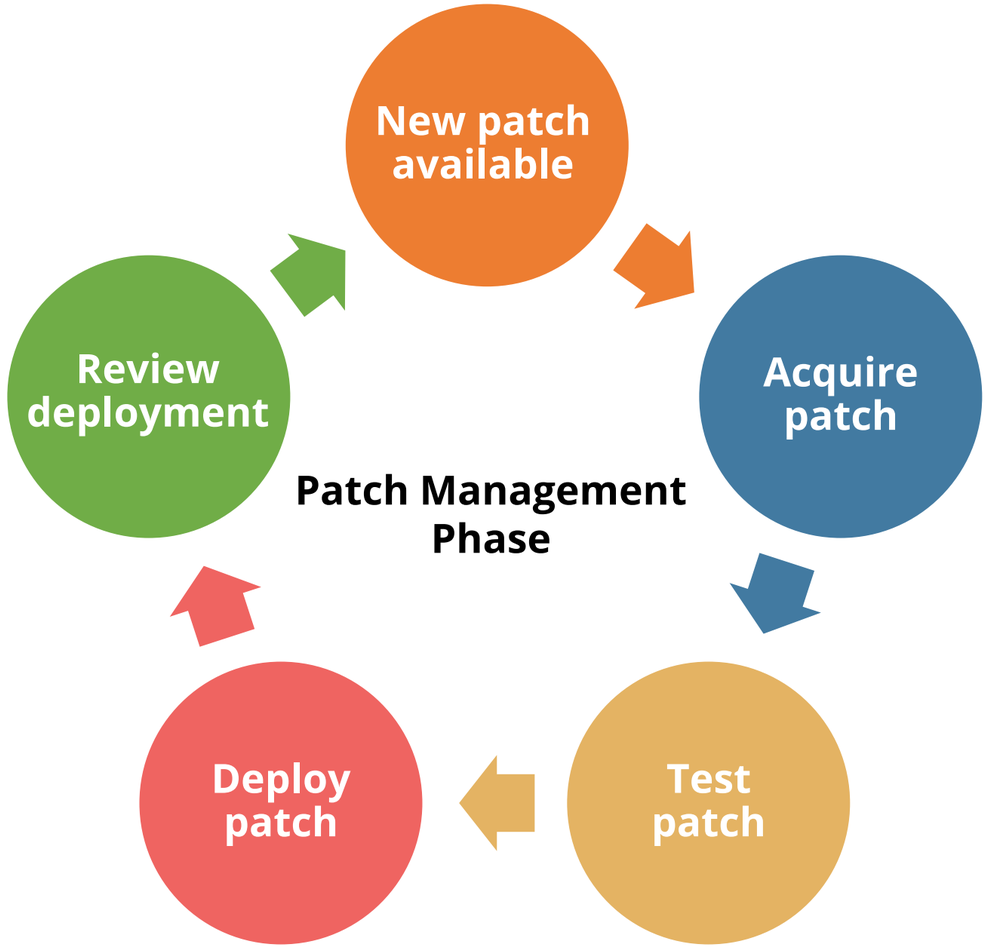
Updates

Address a noncritical, non-security-related bug and are a fix for a specific problem

Patch Management Activities and Cycle

Patch management involves:

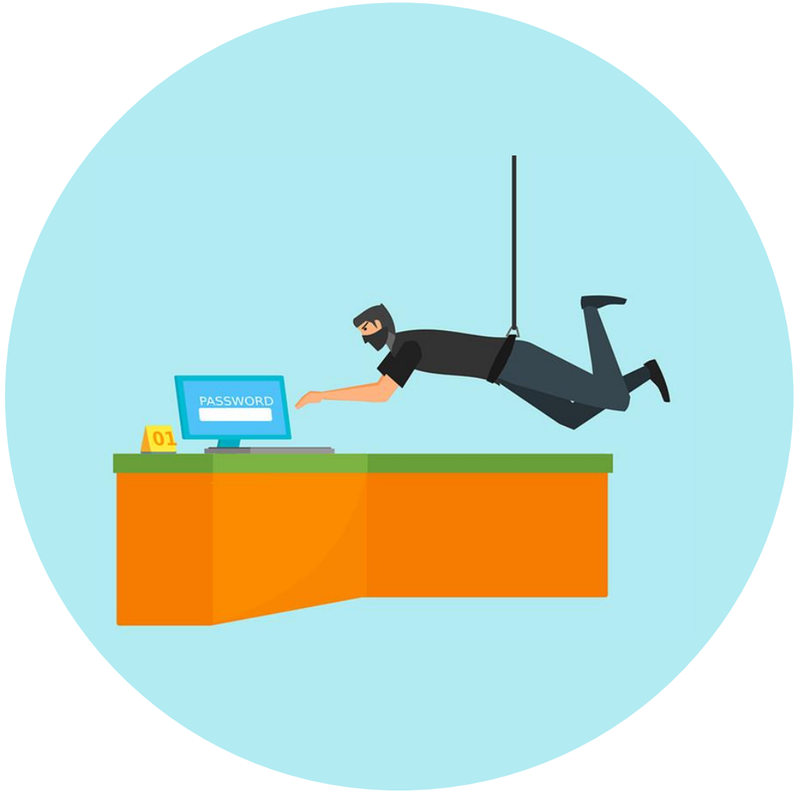
- Scheduling and prioritizing patches
- Testing the patches
- Changing management
- Installing and deploying patches
- Auditing and assessment
- Compliance



Vulnerability Management

With increasing attacks on the systems and networks, identifying their vulnerabilities provides enough knowledge to defend against these attacks.

- Flaws, system misconfigurations, and policy failures give rise to vulnerabilities
- Examples: Buffer overflow, unpatched system
- Vulnerabilities can be fixed with new code, by changing hardware, with security patches, and by reconfiguring systems



Real-World Scenario

Equifax data breach

Equifax Inc., an American multinational consumer credit reporting agency, suffered a data breach between May and July 2017 that affected at least 147 million individuals. The leaked data included sensitive PII such as first and last names, Social Security numbers, birth dates, addresses, and driver's license numbers.

An investigation revealed that Equifax had failed to implement basic security measures as it failed to implement a policy to ensure that security vulnerabilities were patched, failed to segment its database servers to block access to other parts of the network once one database was breached, and failed to install robust intrusion detection protections for its legacy databases.

Real-World Scenario

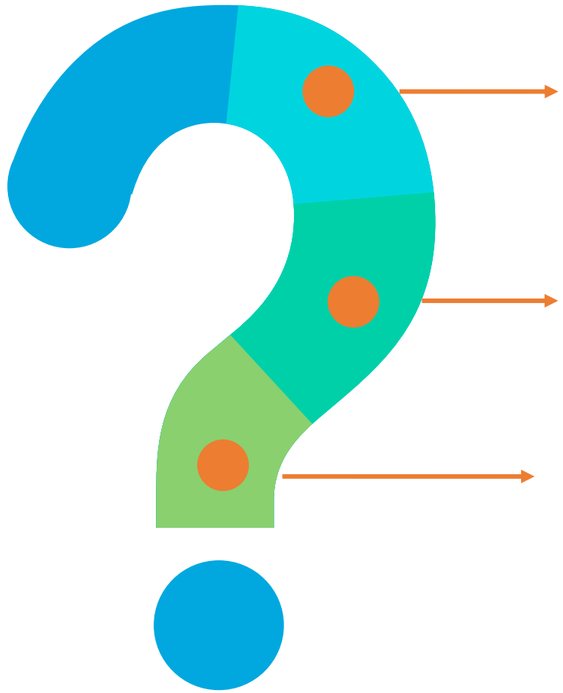
Following the huge data breach, Equifax's CIO, CSO, and CEO resigned.

Equifax Inc. agreed to pay at least $575 million, and potentially up to $700 million, as part of a global settlement.

In addition to the monetary relief to its consumers, Equifax was required to implement a comprehensive information security program.

Real-World Scenario

How did the Equifax breach happen?



On March 9, 2017, Equifax was made aware of a critical vulnerability in the Apache Struts Web Framework, but the company had failed to apply the patch even after 2 months.

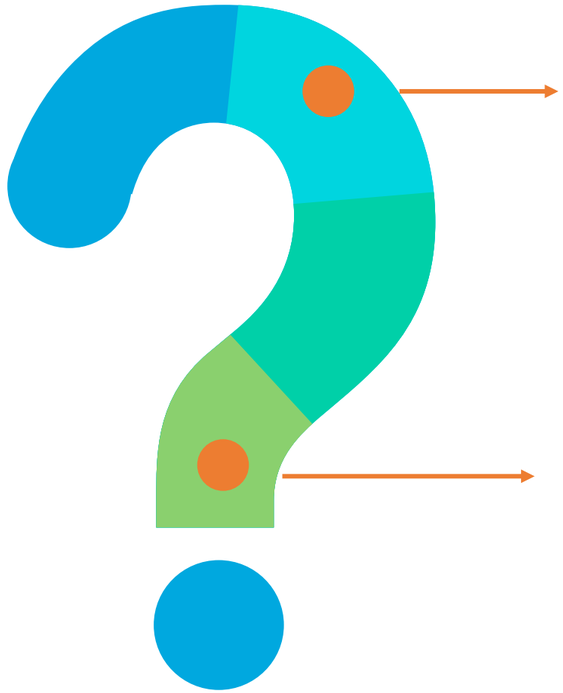
The company was initially hacked via an unpatched server housing Equifax's online dispute portal.

After gaining the ability to issue system-level commands on the online dispute portal, the attackers were able to access additional databases as these systems were not isolated or segmented from each other.

* The Apache Struts Web Framework is a commonly-used, open-source software suite for developing web applications.

Real-World Scenario

How did the Equifax breach happen?



The attackers gained access to a database that contained unencrypted credentials which allowed them to access other databases containing PII. They were able to steal data over an encrypted connection and were undetected for months as Equifax had failed to renew the digital certificate of their network detection tool.

Equifax discovered the breach on July 29, 2017, but they didn't alert the public until September.

Understand and Participate in Change Management Processes

Change Management

Changes to the system are tracked and approved through change control procedures. It includes identifying, controlling, and auditing all changes made to the system.

Change control:

- Ensures the implementation of change in an orderly manner through formalized testing
- Ensures creation of awareness regarding the impending change among the users
- Analyzes the effect of the change on the system after implementation
- Reduces the negative impact of the change on the computing services and resources

Information Security Management

The procedures for change control process implementation and support are:

1. Request for a change to be introduced	Request is sent to the responsible individual or group who administers and approves changes
2. Change approval	After proper analysis and justification for change, it is approved
3. Change intended cataloging	Change control log is updated and documented

Information Security Management

The procedures for change control process implementation and support are:

4. Change testing	Change is formally tested
5. Change scheduling and implementation	Change is scheduled and implemented
6.Report to the appropriate parties about the change	Change is summarized and reported to the management

Change Types

According to ITIL, changes can be broadly divided into three types:

Standard change

A pre-authorized, low-risk, and low-impact change that is well understood, fully documented, and can be implemented without needing additional authorization

Normal change

- A change that must follow the entire change process
- It should be scheduled, assessed, and authorized following a standard process
- It includes both minor (low to medium impact) and major (high impact) changes

Emergency change

A high-impact and urgent change that must be implemented as soon as possible without strictly following the standard process

Implement Recovery Strategies

Backup Methods

Backup methods ensure data integrity and network availability by protecting and restoring deleted, corrupted, or lost information. The different methods are:

	Full backup	Differential backup	Incremental backup
Methodology	• It is the starting point for all other types of backups. • It contains all the data in the folders and files that are selected to be backed up. • A single full backup can provide the ability to completely restore all backed-up files.	• It contains all files that have changed since the last full backup, the latest full backup, and the latest differential backup is needed for a complete restoration.	• It stores all files that have changed since the last full, differential, or incremental backup. • When restoring from an incremental backup, the most recent full backup as well as every incremental backup made since the last full backup are needed.
Backup speed	Slow	Medium	Fast
Restoration speed	Fast	Medium	Slow
Storage space required	High	Medium	Low

Develop a Recovery Strategy

The way in which a subject will access an object is guided by an access control model. A model must be chosen to fulfill the directives of the security policy.

According to NIST 800-34, recovery strategy is the fourth phase to achieve a comprehensive business continuity plan (BCP) or disaster recovery plan (DRP).

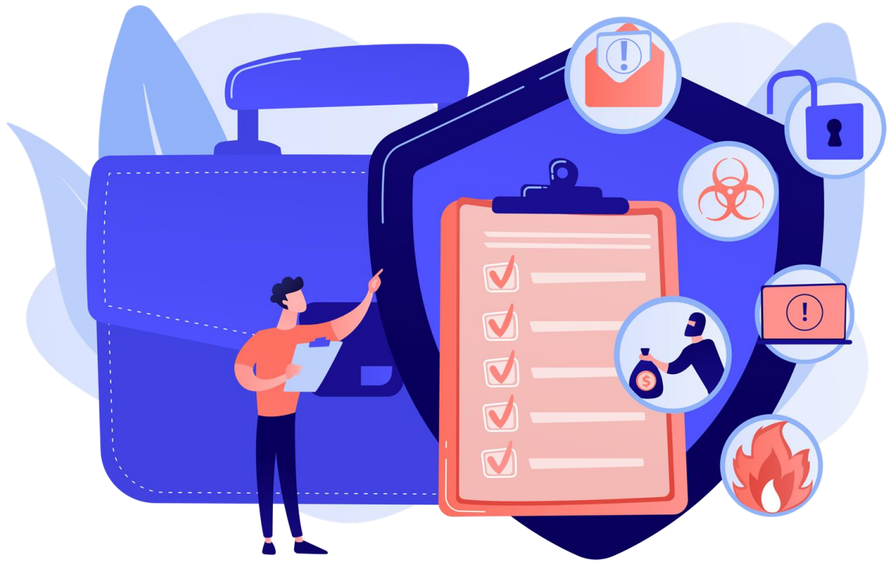
Recovery strategies are predefined actions approved by management and executed in emergencies, leading to the development of a DRP.

A key element of a recovery strategy is the recovery time of critical business systems. The recovery strategies are formulated based on the maximum tolerable downtime (MTD).

Develop a Recovery Strategy

The focus of the recovery process should be on:

- Responding to the disaster
- Recovering critical functions
- Recovering noncritical functions
- Salvaging and repairing hardware and software
- Returning to the primary site for operations



Types of Recoveries: Business Recovery

Identification of critical systems, data, equipment, materials, office space, and key business support personnel

In the event of a disaster, major corporate applications and the related components would be restored first

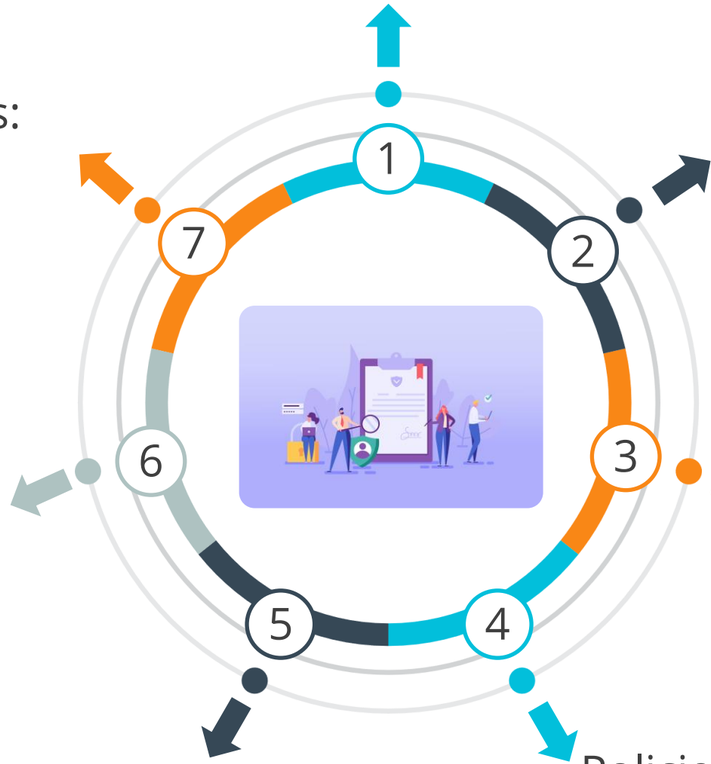
Types of Recoveries: Facility and Supply Recovery

Focuses on the main facility, remote sites, and needed equipment such as networks, servers, telecommunication, HVAC systems, technical documents, required supplies, and the transportation of equipment and staff

Types of Recoveries: User Recovery

Documentation of procedures for employees to follow during emergency situations. It includes:

1. Responsibilities of the team: Who does what?
2. Manual processing techniques: Most tasks must be done manually
3. Procedures for notification: How are employees notified?
4. Policies for disaster: Safety first should be the company's first policy
5. Staff information: Includes contact information and vital records storage
6. Employee accessibility and transportation: Pick-up and drop facilities for the employees
7. Personnel requirements: Computers, desks, and phones for users



Types of Recoveries: Operational Recovery

Operational recovery includes:

- Mainframes, systems, servers, LANs, peripherals, switches, routers, and other data communication equipment's needed for recovery
- Determining alternative recovery locations based on MTD and acceptable costs

Types of Recoveries: Operational Recovery

Businesses have the following options for a secure facility:

- Mirror or redundant site
- Hot site
- Warm site
- Cold site

Additional location options include reciprocal or mutual aid agreements, mobile sites, multiple processing centers, service bureaus, self service, surviving sites, internal arrangements, and work from home.

Recovery Partner Strategies

The recovery partner strategies are:

Reciprocal agreements

- Mutual or bidirectional arrangements between two organizations where one organization can move its operations to other organization in case of disaster
- Also known as mutual aid agreements (MAAs)

Multiple processing centers

- Processing centers spread across different geographical locations
- Handle the business' operational requirements during recovery

Service bureaus

- Recovery contracts with an offsite service bureau helps to have the site ready and available for the organization during emergencies
- Offer expertise in processes, technology, and business-domains to customers

Backup Sites

Backup sites are locations where the business can be recovered in the event of a disaster at the primary site. The different backup sites available are:

Mirror site

- Mirror or redundant site is a duplicate production of a system capable of seamlessly conducting IT operations without loss of services to the system's end user.
- A redundant site is configured like the primary site and is the most expensive recovery option.
- Example: Regulatory bodies have made it mandatory for commercial banks to have redundant sites.

Backup Sites

Backup sites are locations where the business can be recovered in the event of a disaster at the primary site. The different backup sites available are:

Hot site

- Hot site is where an organization relocates its data center following a major disruption or disaster.
- It consists of servers, raised floors, power, utilities, fully configured computers, hardware, and critical applications' data mirrored in real time.
- It helps resume critical operations within a very short period.
- Hot sites can be internal (owned) or external (outsourced).

Backup Sites

Backup sites are locations where the business can be recovered in the event of a disaster at the primary site. The different backup sites available are:

Warm site

- Warm site has hardware and connectivity but lacks the real-time data.
- It relies on backup data to rebuild a system after a disruption.
- It consists of raised floors, power, utilities, computer peripherals, and fully configured computers.
- It is less expensive, more flexible, and requires fewer resources for maintenance.
- It requires more time and resources to activate the site.

Backup Sites

Backup sites are locations where the business can be recovered in the event of a disaster at the primary site. The different backup sites available are:

Cold site

- A cold site does not have data backups and immediately available hardware.
- Configuring cold sites and restoration of critical IT services take more time. It has a raised floor, power, utilities, and physical security.
- It has no resources or geographic constraints.

Backup Sites

Backup sites are locations where the business can be recovered in the event of a disaster at the primary site. The different backup sites available are:

Mobile site

- Mobile sites are also called data centers on wheels.
- It has towable trailers that contain computer equipment as well as HVAC, fire suppression equipment, and physical security.
- It keeps the facility intact despite the data center being damaged.

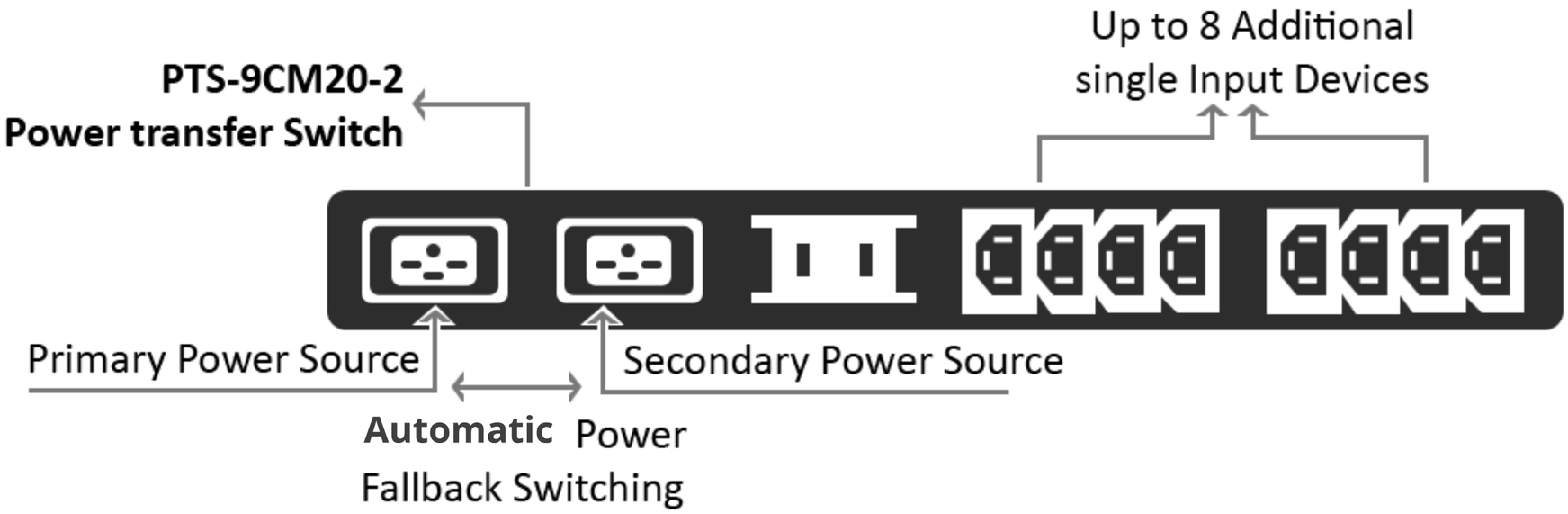
Importance of Maintaining Resilient Systems

The mechanisms used for controlling the behavior of a system when it fails are:

- Fail-safe mechanisms that focus on failing with minimum harm to personnel
- Fail-secure mechanisms that focus on failing in a controlled manner to block access while the systems are in an inconsistent state

Redundancy and Fault Tolerance

Fault tolerance is provided by redundant items within a system. The usage of the spare components will determine if it is a cold, warm, or hot spare. In the event of component failure, the fault tolerant system can continue to operate through:

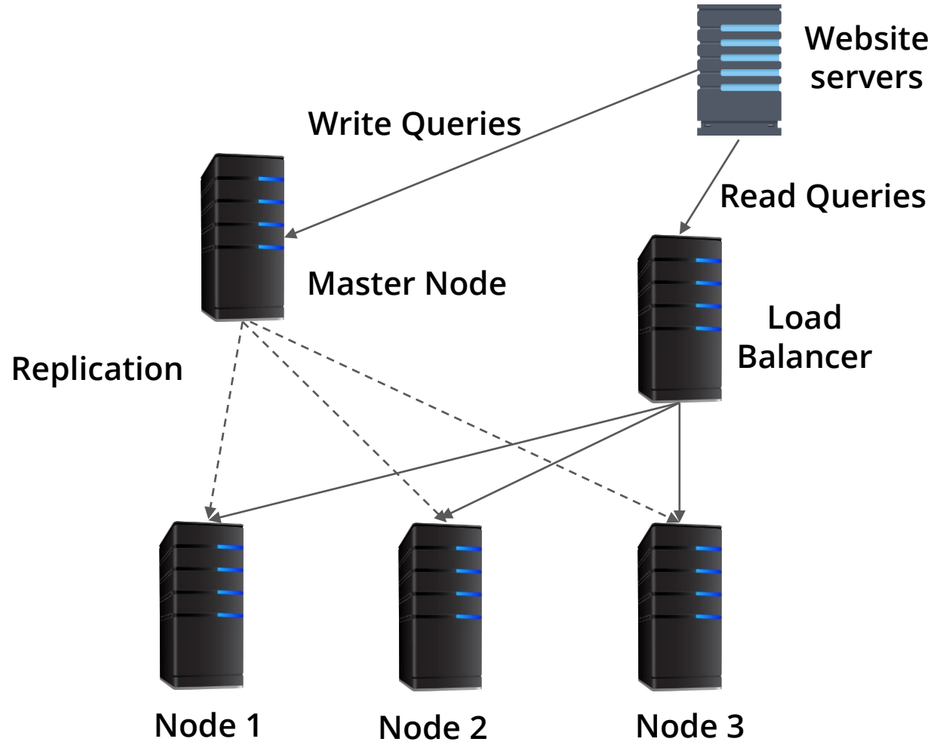


Redundant power supplies: Redundant or dual power supplies are common in systems where failures cannot be tolerated.

Example: Core network switches

Redundancy and Fault Tolerance

Fault tolerance is provided by redundant items within a system. The usage of the spare components will determine if it is a cold, warm, or hot spare. In the event of component failure, the fault tolerant system can continue to operate through:



Replication: Data changes are transmitted to a counterpart storage system which is an adjunct to clustering and makes current data available to all cluster nodes.

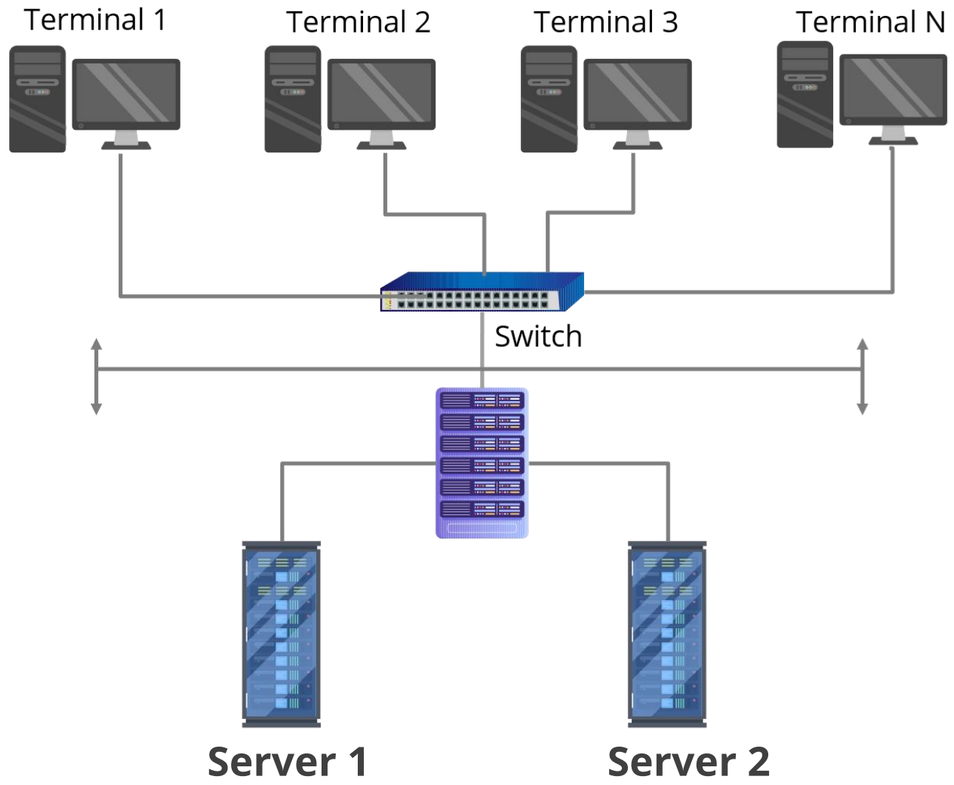
Redundancy and Fault Tolerance Methods

The following are the redundancy and fault tolerance methods:

Cluster

- Cluster refers to a group of two or more servers that function as a single logical server.
- Clusters generally operate in one of the following modes:

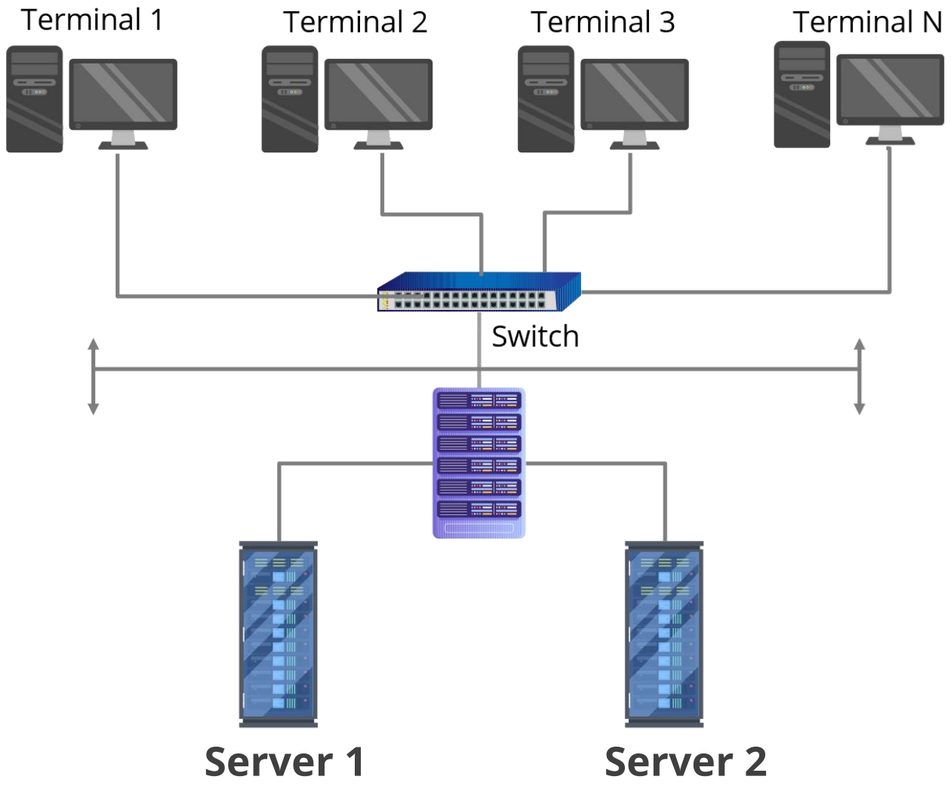
1. **Active-active mode**
   - Both servers actively operate and service incoming requests.



Redundancy and Fault Tolerance Methods

Active-passive mode

- One (or more) server actively services requests and one (or more) server remains in a standby state to be able to switch immediately to active mode when the active server fails.
- A failover is an event in a server cluster running in active-passive mode.
- Geographical cluster or geo-cluster systems is a cluster that can be located anywhere.



Redundancy and Fault Tolerance Methods

The types of **Redundant Arrays of Inexpensive Disks** or **Redundant Arrays of Independent Disks (RAIDs)** are:

RAID 0: Striping

- Data striping is done over many drives
- Redundancy or parity is not provided
- All volumes become unusable if one volume fails

RAID 1: Mirroring

- The data is written simultaneously on two drives
- If one drive fails, the other one has the data

RAID 3: Byte-level parity

- Parity data is held on one drive while data is striped over all drives
- A drive can be reconstructed from the parity drive if it fails

Redundancy and Fault Tolerance Methods

RAID 4: Striped set

- It has dedicated parity or block level.
- It stripes data at the block level.

RAID 5: Interleave parity

- It ensures that there is no single point of failure.
- It writes data along with parity on all drives.

RAID 6: Second or double-parity data

- It has more fault tolerance than level 5 with a second set of parity data written on all drives.

RAID 10: Striping and mirroring

- It supports multiple disk failures by simultaneously mirroring and striping data across several drives.

Best Practices for Backup and Recovery

In software and data recovery, data recovery is the prime focus. To create a level of fault tolerance and redundancy, the following concepts are used.

Database Shadowing

Database information is simultaneously written or duplicated to another server

Electronic Vaulting

Copies the backup data in a batch process to an offsite location

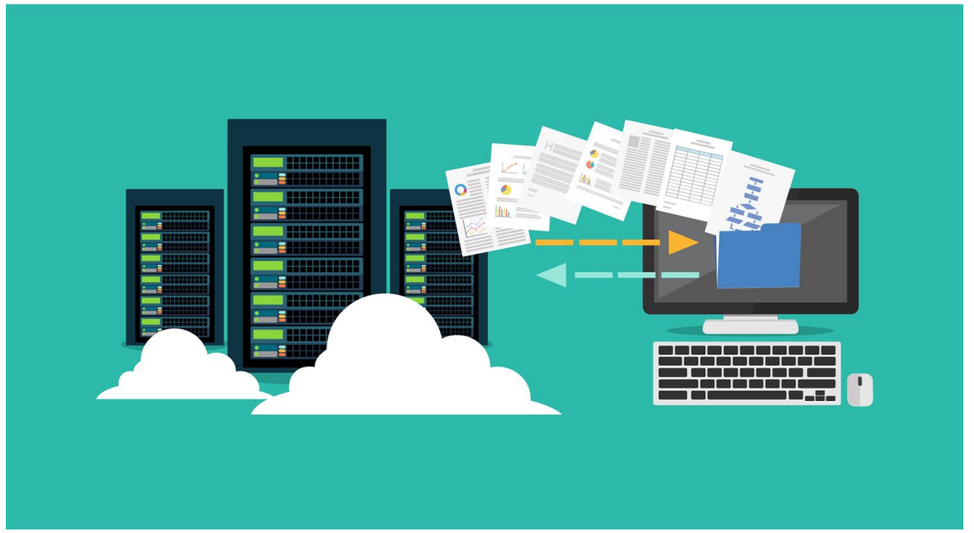
Remote Journaling

Allows full synchronization of sites by transferring live data to offsite locations

Best Practices for Backup and Recovery

Backups and offsite storage

- Frequency of backups, as required by the business for optimum recovery, needs to be ensured
- As a security measure, the backup tapes are stored at an offsite location



Implement Disaster Recovery (DR) Processes

Implement Disaster Recovery Processes

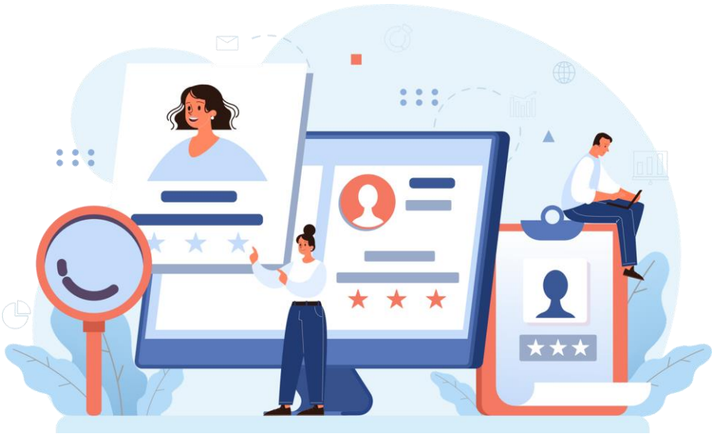
The general process of disaster recovery includes:

Response

- The BCDR plan must provide for both major and minor disasters.
- Personnel health and safety must be top-most priority.
- BCDR plan should also define, in terms of business interruption, what constitutes a disaster. Thus, authorizing the activation of the disaster recovery plan.
- It must address individual and organization-wide natural disasters, fire, and physical damage.

Personnel

BCDR plan should include a prioritized contact list of people who should be notified if a disaster occurs.



Appoint a disaster recovery team who will be responsible for taking action when a disaster does strike.

Personnel

BCDR team includes:

- Incident response team
- Emergency action team
- Information security team
- Human Resources (HR) team
- Damage assessment team
- Administrative support team
- Legal affairs team
- Public relations and communication team

Communications

- After BCP and DRP have been written, they must be communicated to the entire staff of the organization.
- This information should be tailored to individuals and groups to ensure.
- The conveyed information should be relevant, clear, and easily understandable for the target audience.
- **Crisis communication plan** provides procedures for disseminating internal and external communications.

Assessment

- **Assessment** is the process of determining the nature, source, and impact of a disaster.
- This assessment is carried out by the disaster response team with input from subject matter experts.
- Disaster assessments will facilitate the recovery process by estimating the extent of damage, what can be replaced, restored, or salvaged.
- It may also help estimate the time required for repair, replacement, and recovery.

Restoration

Restoration means bringing a **business facility and environment** back to its original capabilities.

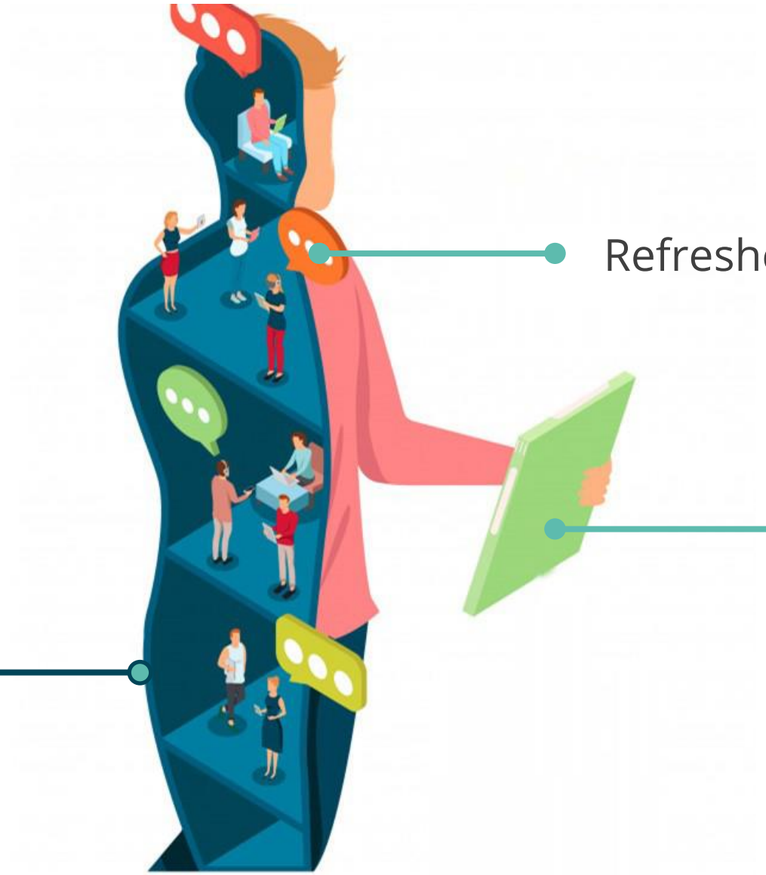
Recovery means bringing **business operations and processes** back to the normal working condition.

Restoration

- The ultimate goal of BCDR is to resume full normal operations.
- If the primary site is completely destroyed or severely damaged, then an alternate recovery site will function as the primary site.
- Ensure that the recovery site is safe for people before restoration process begins.
- The **order of restoration** of critical business functions is determined during the **BIA**.
- The disaster is considered to be officially over when all the business operations and processes return to normal at the primary site.

Training and Awareness

The effective execution of these plans will depend on the employees knowing what they have to do and under which circumstances.



Refresher trainings at regular intervals

Formal training at the time of hiring

Training includes professional seminars, special in-house educational programs, the use of consultants, and vendors tailored to the needs of individual groups

Training and Awareness

- Awareness is less formal than training and is generally targeted at all employees in the organization.
- Awareness includes frequent distribution of information (newsletter, email, posters, flyers).

Training

Training programs should be designed and developed by the organizations for all the BCP or DR activities

Trainings ensure employees:

Know the course of action in the event of an emergency

Are provided basic first aid and CPR training

Are interested in business continuity activities through periodic awareness programs

Training

The various training carried out are:

Starting Emergency Power

- Specific training for operating emergency power supplies
- Regular testing of operation of the emergency power supplies

Call Tree Training or Testing

- Answering the call and taking necessary steps
- Ensuring the calling tree process is successful

Lessons Learned

Lessons learned and gaps identified in the plan when either recovering at the disaster recovery site or restoring the primary site should be recorded.

Their recommendations should be implemented to continuously improve the effectiveness of the disaster recovery plan.

Test Disaster Recovery Plans (DRP)

Importance of Testing

Testing is important because it:

- Helps to keep the plans updated
- Identifies the shortcomings of the plans
- Tests the readiness of the organization to face disasters
- Refines the existing controls
- Satisfies the requirements of regulatory bodies

Types of Tests

Review is the initial, and most basic, DRP test.

A review:

- Ensures the complete coverage of the plan
- Is performed by the team that had developed the plan
- Helps discover any flaws in DRP
- Ensures that there are no obvious shortcomings and omissions in the plan

Types of Tests

Checklist testing is also known as consistency testing. A checklist test:

- Is a list of important and necessary components required in the process of recovery
- Ensures necessary components are and will be available in the event of a disaster
- Is an easy and cost-effective method of testing the plan

Types of Tests

Structured walkthrough or tabletop is usually performed prior to in-depth testing. A structured walkthrough is used to:

- Review the overall approach of targeted recovery of systems and services
- Help the group discuss and perform the proposed recovery procedures in a structured manner
- Identify gaps, omissions, technical missteps, or erroneous assumptions in the process

Types of Tests

Simulation test is also known as walkthrough drill.
A simulation test:

- Helps team members carry out a recovery process
- Simulates a disaster, and the teams need to respond as directed by the DRP

Types of Tests

Parallel processing is used in a business where critical processes involve transactional data. The parallel processing test:

- Involves the usage of alternate computing sites to recover crucial processing components and restore data from the latest backup
- Does not interrupt the regular production systems

Types of Tests

Partial and complete business interruption test has the highest fidelity of all DRP tests. Partial and complete business interruption test:

- Should be exercised with extreme caution as it can actually cause a disaster
- Makes the organization use the alternate computing facilities and stops normal business processing at the primary location
- Can only be conducted in organizations with fully redundant and load-balanced operations

Discussion

Discussion

Full-interruption tests present the highest risk to the business if not managed properly.

What could be done before performing a full-interruption test to mitigate this risk?

Participate in Business Continuity (BC) Planning and Exercises

Disaster Recovery: Planning Design and Development

According to NIST 800-34, planning design and development is the fifth phase to achieve a comprehensive BCP or DRP.

For the recovery of critical business systems, a detailed plan is:

- Prepared and documented by the BCP team
- Inclusive of long-term and short-term goals, such as recovery plans, employee training, plan maintenance, and testing procedures

Steps for Plan Design and Development

Step 1: Define the scope of the plan

Step 2: Identify potential disasters

Step 3: Define the BCP strategy

Step 4: Calculate funding

- Identify critical sites, systems, and business processes
- Set priorities for restoration

Steps for Plan Design and Development

Step 1: Define the scope of the plan

Step 2: Identify potential disasters

Step 3: Define the BCP strategy

Step 4: Calculate funding

- Identify the potential disasters which may impact the site
- Identify the resources needed to recover
- Identify actions that might eliminate risks in advance

Steps for Plan Design and Development

Step 1: Define the scope of the plan

Step 2: Identify potential disasters

Step 3: Define the BCP strategy

Step 4: Calculate funding

- Select the recovery strategies
- Identify important personnel, systems, and equipment that are required for recovery
- Define the roles and responsibilities of the team members
- Document the continuity strategy, which includes guidance on declaring a disaster

Steps for Plan Design and Development

Step 1: Define the scope of the plan

Step 2: Identify potential disasters

Step 3: Define the BCP strategy

Step 4: Calculate funding

- Identify the long-term and short-term goals to calculate the funding needs

Disaster Recovery Phases: Maintenance

According to NIST 800-34, BCP (or DRP) maintenance is the seventh phase to achieve a comprehensive BCP (or DRP).

The BCP (or DRP) must be updated once it is completed, tested, trained, and implemented. The plan must incorporate all business and IT system changes as they become obsolete quickly.

Disaster Recovery Phases: Maintenance

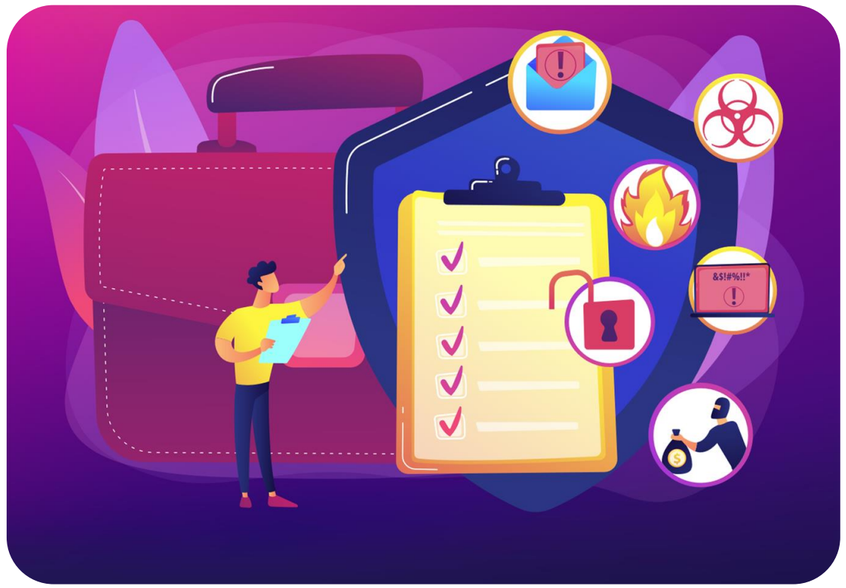
Change management ensures:

- Security is not adversely affected when new systems are introduced, modified, and updated
- All planned changes are documented and tracked
- Substantial changes are formally approved and documented

Disaster Recovery Phases: Maintenance

The strategies to maintain the plan and ensure it is valid are:

- Make BC planning a part of every business decision
- Insert BCP maintenance responsibilities into job descriptions
- Include maintenance in personnel evaluations
- Perform internal audits that include disaster recovery and BCP procedures
- Test the plan annually

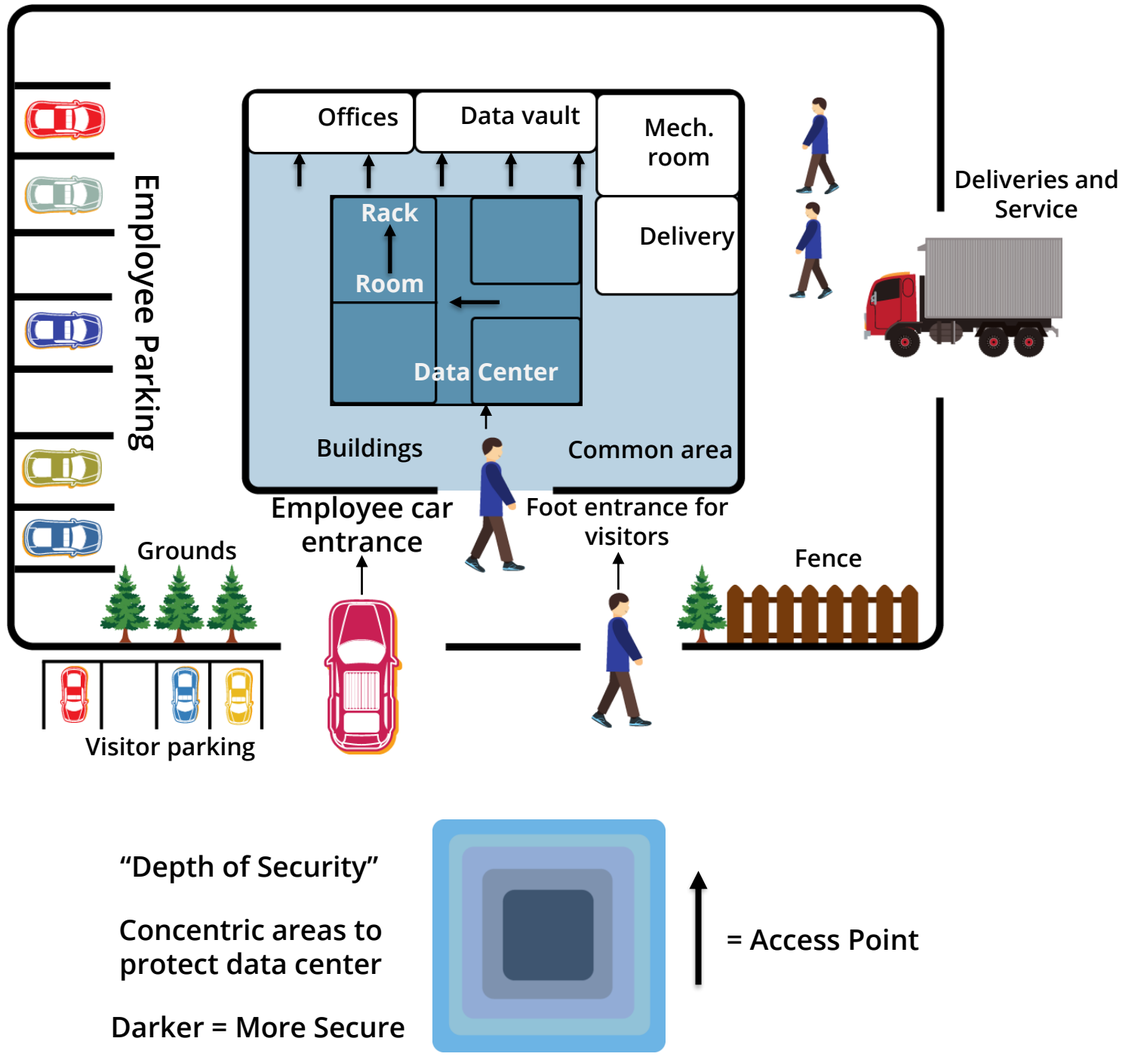


Implement and Manage Physical Security

Perimeter Security Controls

Perimeter defenses help prevent, detect, and correct unauthorized physical access and control access into the facility.

- It employs the **defense-in-depth** concept.
- With layered architecture for barriers, the center or the most protected area has the highest level of security.
- Security systems are designed utilizing multiple barriers called rings of protection.
- The layered design can reduce the likelihood of a successful attack.

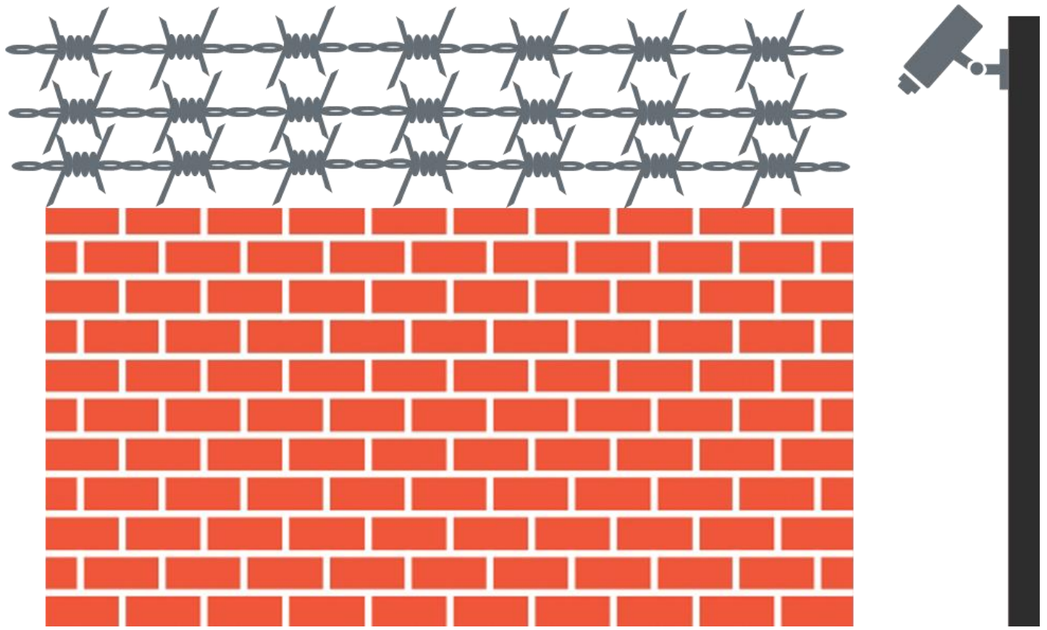


Barriers

Barriers define how an area should be designed in order to obstruct or deny access.

Objectives of barriers include:

- Keep intruders out
- Cause delays in intrusion



Fences

Fences are perimeter identifiers that are designed and installed to keep intruders out.

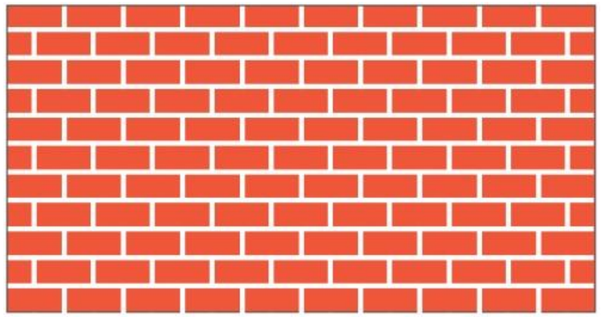
The various types of fences include:

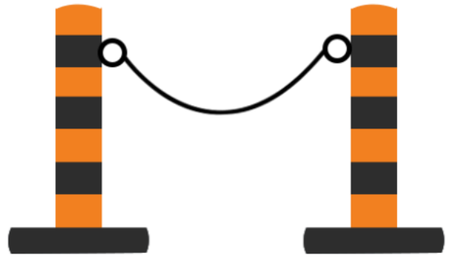
- Chain link
- Barbed wire
- Barbed tape
- Concertina wire

Height	Effectiveness
3 -4 ft.	Deters casual trespassers
6 – 8 ft.	Too difficult to climb easily
8 ft. plus 3 Strands of barbed or razor wire	Deters determined trespassers

Walls and Bollards

- Walls are man-made barriers but are usually more expensive to install than fences.
- Common types of walls are:
  - Cinder block
  - Masonry
  - Brick
  - Stone
- Bollards are small concrete pillars outside a building.
  - Example: Traffic bollard



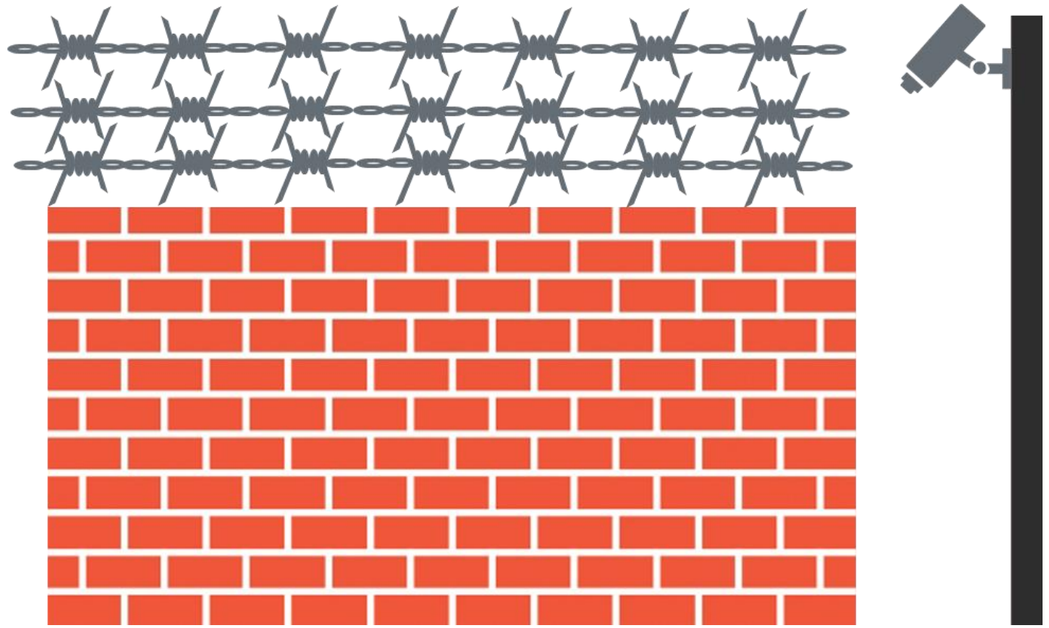


Perimeter Intrusion Detection

Perimeter sensors alert security when any intruders attempt to gain access across the open space or attempt to breach the fence line.

Open-terrain sensors include:

- Infrared
- Microwave systems
- Time-domain reflectometry (TDR) systems
- Video content analysis and motion path analysis



Business Scenario

Hilda Jacobs, general manager, was assigned the task of designing perimeter security for a new office in India. Kevin travelled to India on a short trip to understand the surroundings of the new office.

The location had already been fixed, but Kevin found that the surrounding area had recently seen a spike in the crime rate and thus had a high potential of unauthorized intrusions. The site had many concrete and steel structures in the open compound. Kevin submitted his report to Hilda.

Question: Which perimeter intrusion detection system should Hilda choose based on Kevin's report?

Business Scenario

Hilda Jacobs, general manager, was assigned the task of designing perimeter security for a new office in India. Kevin travelled to India on a short trip to understand the surroundings of the new office.

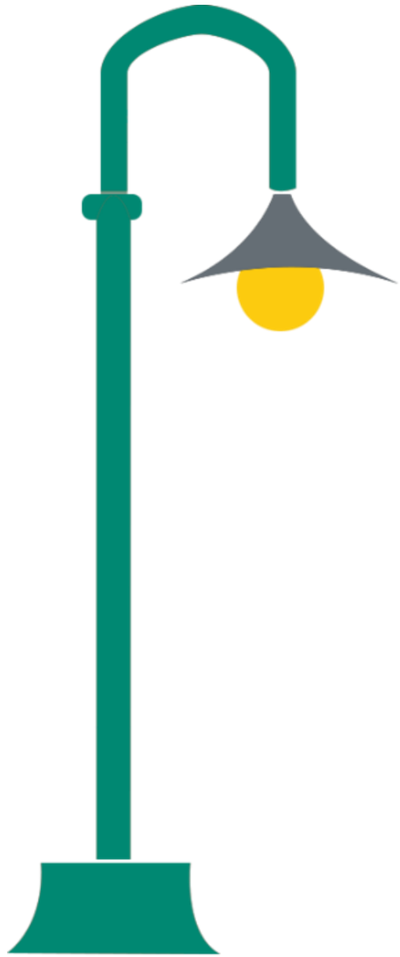
The location had already been fixed, but Kevin found that the surrounding area had recently seen a spike in the crime rate and thus had a high potential of unauthorized intrusions. The site had many concrete and steel structures in the open compound. Kevin submitted his report to Hilda.

Question: Which perimeter intrusion detection system should Hilda choose based on Kevin's report?
Answer: Microwave sensors can be used since they can pass through concrete and steel structures.

Importance of Lighting

Lighting plays a vital role in the security function. It:

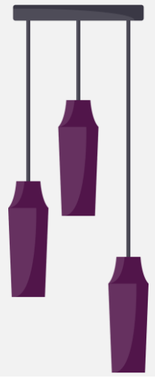
- Provides security personnel the ability to visually assess their surroundings at night
- Helps notice and identify individuals at night
- Increases the effectiveness of guard forces and CCTV
- Reduces the need for security personnel
- Provides real and psychological deterrents against intruders
- Provides illumination where natural light is insufficient
- Is inexpensive to maintain



Types of Lighting Systems

Lighting Systems

Continuous Light



Standby light

Emergency light

Movable light

Types of Lights

Fluorescent lights

Types of Lights

Mercury vapor lights

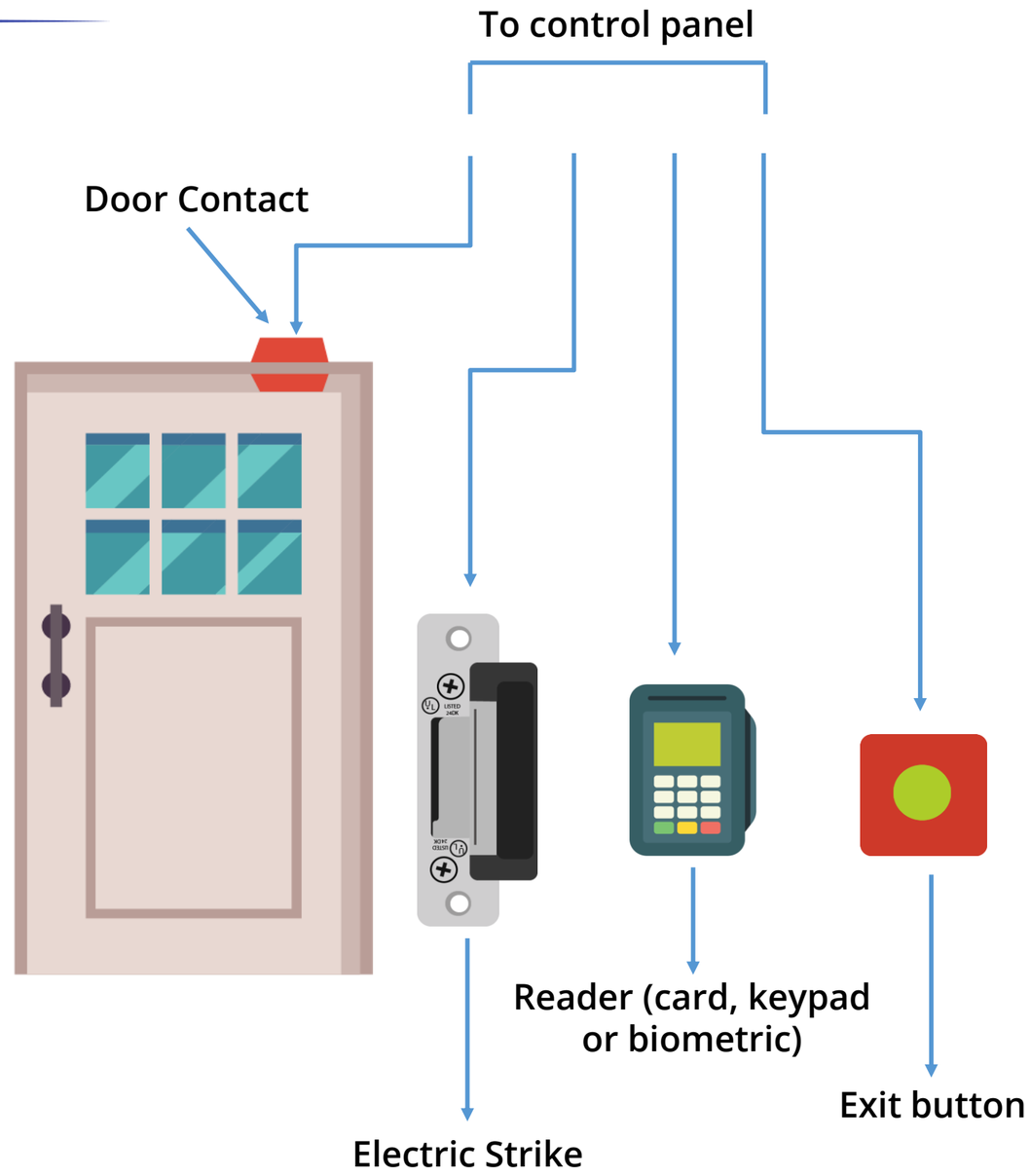
Infrared illuminators

Quartz lamps

Sodium vapor lights

Access Control

- The primary function of an access control system (ACS) is to allow only authorized personnel inside a controlled area.
- The goal of an access control program is to limit the opportunity for a crime to be committed.
- The basic components of an ACS include:
  - Card readers
  - Electric locks
  - Alarms
  - Computer systems



Types of Access Control Systems

Access cards	The different types of access cards are magnetic stripe, proximity card, and smart card.
Biometrics	The types of biometrics include fingerprint, facial image, hand geometry, voice recognition, iris patterns, retina scanning, signature dynamics, and keystroke dynamics.
Closed circuit television	It is a collection of cameras, recorders, switches, keyboards, and monitors that allow one to view and record security events.
CCTV color cameras	CCTV color cameras offer additional information, such as the color of a vehicle or a subject's clothing.

Types of Access Control Systems

Digital video recorder (DVR) and monitor displays → It is used to download camera footage to a hard drive for storage of historical information.

Guards → Security guards or officers patrol and inspect a property to protect it against fire, theft, vandalism, terrorism, and illegal activity.

Guard dogs → Guard dogs are a form of physical control that can serve as detective, preventive, and deterrent controls.

Securing a Building

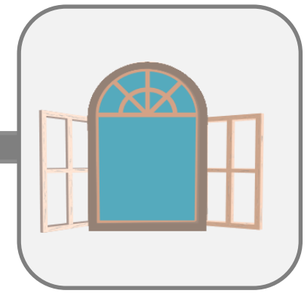
These are the various means to secure a building:

Doors: Solid core, hollow core, and glass

Locks: Rim, mortise, and cipher

Piggybacking: Mantrap and turnstile

Windows: Bulletproof and laminated



Interior intrusion detection systems: Infrared and ultrasound

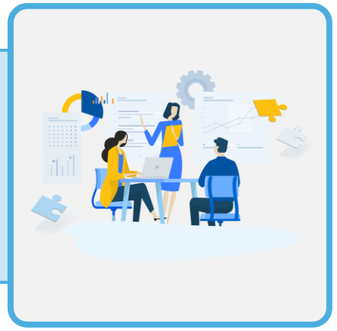
Escort and visitor controls

Address Personnel Safety and Security Concerns

Travel

Information about technical controls along with personnel training will ensure the safety of employees when they travel

Employees must understand the dos and don'ts about using IT systems when they go abroad



Encrypt the devices, use strong passwords, and follow other due care processes

Security Training and Awareness

The purpose of **security training and awareness** is to equip the learner with the knowledge, skill, and competence to recognize security threats and maintain safety practices.

Emergency Management

Emergency management is the organization and management of the resources and responsibilities needed to withstand, respond to, and recover from all types of emergencies and disasters.

Human safety should be the top priority.

Duress

Duress is defined as **any unlawful threat or coercion used to induce another to act [or not act] in a manner they otherwise would not [or would]**.

These situations can be life-threatening or deadly.

Employees should undergo training on how to handle a stressful situation and what to do when under duress.

Duress

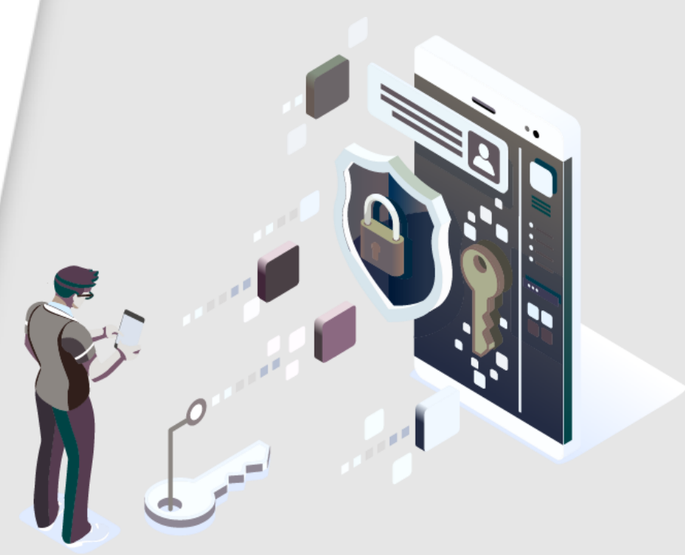
A duress code (covert signal) should be used by an individual that is under duress to convey their state.

Lone workers, security guards, or healthcare providers may also use duress or panic alarms if urgent assistance is needed.

While designing and implementing duress mitigation controls or training, it is always advisable to seek the assistance of law enforcement or other professionals.

Key Takeaways

- Intrusion detection and prevention, security information, event management, continuous monitoring, and egress monitoring can be used to log and monitor activities.
- The three important concepts of the security operations domain are threats, vulnerabilities, and assets.
- Incident response is the practice of detecting, determining, minimizing, and resolving a problem.
- The focus of the recovery process should be on responding to the disaster, recovering critical and noncritical functions, salvaging and repairing hardware and software, and returning to the primary site of operations.



This concludes **Security Operations.**

The next domain is **Software Development Security.**