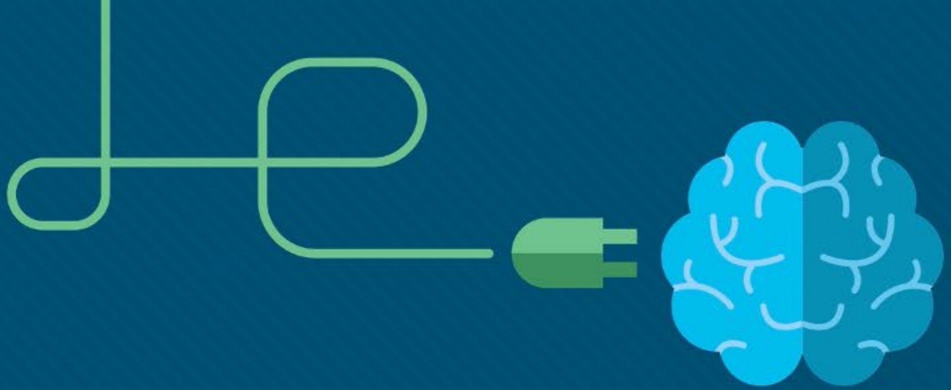


Module 10: Cybersecurity Principles, Practices, and Processes

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Cybersecurity Principles, Practices, and Processes

Module Objective: Use cybersecurity best practices to improve confidentiality, integrity, and availability.

Topic Title	Topic Objective
The Three Dimensions	Use hashes to verify the integrity of files
States of Data	Contrast the three states of data
Cybersecurity Countermeasures	Compare the types of cybersecurity countermeasures

10.1 The Three Dimensions

The Three Dimensions

The Cybersecurity Cube

The cybersecurity cube provides a useful way to think about protecting data and includes the three dimensions of information security.

1. Security Principles identify the goals to protect cyberspace.

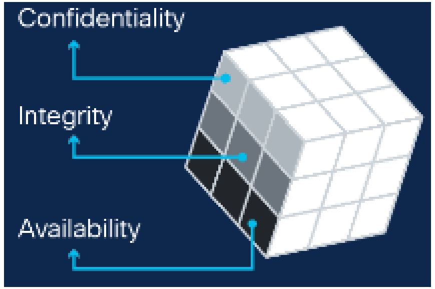
- Data **confidentiality**
- Data **integrity**
- Data **availability**

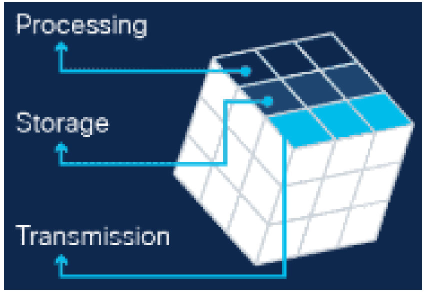
2. Data States represent the three possible data states.

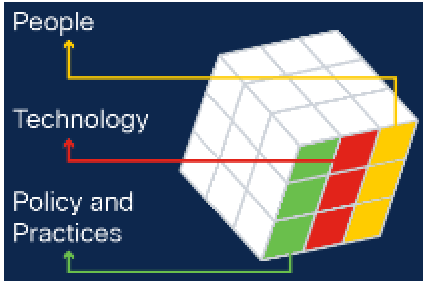
- Data **in transit**
- Data **at rest** or in storage
- Data **in process**

3. Safeguards define the pillars on which to base our cybersecurity defenses to protect data and infrastructure in the digital realm.

- **Technology**
- **Policy and practices**
- Improving education, training, and awareness in **people**







CIA Triad – The Principle of Confidentiality

- Tokenization is a substitution technique that can isolate data elements from exposure to other data systems.
  - Tokenization can be used to accomplish confidentiality without using encryption.
  - A random value with no mathematical relationship replaces original data.
  - Outside the system, a token has no value and is meaningless.
  - Tokenization can preserve the data format (its type and data length), which makes it useful for databases and card payment processing.

- Rights management covers both digital rights management (DRM) and information rights management (IRM).
  - DRM protects copyrighted material like music, films, or books.
  - IRM is used with email and other files that are relevant to the activities and communications of an organization.

Data Integrity

- Integrity is the accuracy, consistency, and trustworthiness of data across its entire lifecycle.
- Data undergoes several operations, such as capture, storage, retrieval, update, and transfer.
- Data must remain unaltered by unauthorized entities during all these operations.
- Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls.
- Data integrity is a fundamental component of information security.
- The levels of need for data integrity are:
  - Critical
  - High
  - Medium
  - Low

Ensuring Availability

There are many measures that organizations can implement to ensure the availability of their services and systems.

- **Equipment maintenance**: Regular equipment maintenance can dramatically improve system uptime. Maintenance includes component replacement, cleaning and alignment.
- **Operating systems and software updates and patches:** Modern operating systems, applications, and software are continuously updated to correct errors and eliminate vulnerabilities.
- **Backup testing:** Backup of organization data, configuration data, and personal data helps ensures availability. Backup systems and backed up data should also be tested to ensure they work properly, and that data can be recovered in the event of data loss.

Ensuring Availability (Cont.)

- **Disaster planning**: Planning for disasters is a critical part of increasing system availability. The cybersecurity team should practice response protocols, test backup systems, and be familiar with procedures for restoring critical systems.

- **New technology implementations:** High availability requires continuous evaluation and testing of new technologies to counter new threats and attacks. Cybercriminals use the latest tools and tricks, so cyber professionals are also required to keep up, using new technologies, products and devices.

- **Activity monitoring**: Continuous system monitoring increases system availability. Monitoring event logs, system alerts, and access logs provide the cybersecurity professional with real-time system information.

- **Availability testing:** All systems should be tested to find vulnerabilities. Testing can include port scans, vulnerability scans, and penetration tests.

The Three Dimensions

Lab - The Cybersecurity Sorcery Cube Scatter Quizlet

In this lab, you will identify the three dimensions of the Cybersecurity Sorcery Cube and the elements of each dimension.

Packet Tracer - File and Data Integrity Checks

In this Packet Tracer activity, you will meet the following objectives:

- Part 1: Recover Files after a Cyber Attack
- Part 2: Using Hashing to Verify File Integrity
- Part 3: Using HMAC to Verify File Integrity

Packet Tracer - Explore File and Data Encryption

In this Packet Tracer activity, you will meet the following objectives:

- Part 1: Discover the FTP Account Credentials for Mary
- Part 2: Upload Confidential Data using FTP
- Part 3: Discover the FTP Account Credentials for Bob
- Part 4: Download Confidential Data using FTP
- Part 5: Decrypt the Contents of a Sensitive File

10.2 States of Data

States of Data

Data at Rest

- Data that is not in transit or in-process is considered data at rest.
- If you have data that you need to store and will want to access later, some storage options exist:

Direct-attached storage (DAS)	It is connected to a computer. By default, systems are not set up to share direct-attached storage with other computers on their network.
Redundant array of independent disks (RAID)	It uses multiple hard drives in an array, combining multiple disks so that the operating system sees them as a single disk. RAID provides improved performance and fault tolerance.
Network attached storage (NAS) device	It is connected to a network that allows storage and retrieval of data from a centralized location by authorized network users. NAS devices are flexible and scalable, meaning that their capacity can be increased as needed.
Storage area Network (SAN)	It is a network-based storage system. SAN systems connect to the network using high-speed interfaces, which allows for improved performance and the ability to connect multiple servers to a centralized disk storage repository.
Cloud Storage	A remote storage that uses space on a data center provider and is accessible from any computer with Internet access, usually upon subscription.

States of Data

Challenges of Protecting Stored Data

- To improve data storage protection, organizations can automate and centralize data backups.

Direct-attached storage

- It can be one of the most difficult types of data storage to manage and control.
- It is vulnerable to malicious attacks on the local host.

Data at rest

- It also includes backup data (when it is not being written or in transit).
- To boost security and decrease data loss, organizations should limit the types of data stored on direct-attached storage devices.

Network storage systems

- It offers a more secure option.
- It includes RAID, SAN, and NAS providing greater performance and redundancy.

Methods of Transmitting Data

- Data in transit is the data which is being transmitted, not at rest nor in use.
- Data transmission involves sending information from one device to another.
- There are numerous ways to transmit data between devices:
  - **A sneaker net:** It uses removable media to physically move data from one computer to another.
  - **Wired networks:** It includes copper and fiber optic media and can serve a LAN or span great distances in wide area networks (WAN).
  - **Wireless networks:** It uses radio waves to transmit data. It increases the number of guest users with mobile devices on small office home office (SOHO) and enterprise networks.

Methods of Transmitting Data (Cont.)

- Both wired and wireless networks transmit packets.
- Packet refers to a unit of data that travels between a source and a destination on the network.
- Standard protocols such as the IP and HTTP define the structure and format of data packets.
- These standards are open source and fully available to the public.
- Protecting the confidentiality, integrity, and availability of transmitted data is one of the most important responsibilities of a cybersecurity professional.

Challenges of Data in Transit

- With the growth in mobile and wireless devices, and the increasing amounts of data collected and stored by organizations, cybersecurity professionals have become responsible for protecting massive amounts of data crossing their network daily.

- In order to protect this data, there are several challenges to overcome:

Protecting the confidentiality of data in transit	Cybersecurity professionals must take steps to safeguard data in transit, such as implementing VPNs, using SSL and IPsec, and various other methods of encrypting data for transmission.
Protecting the integrity of data in transit	Cybersecurity professionals deploy data integrity systems that test the integrity and authenticity of transmitted data to counter these actions. These systems include, for example, hashing and data redundancy.
Protecting the availability of data in transit	Network security professionals can implement mutual authentication systems to counter these actions. Mutual authentication systems require the user to authenticate to the server and requests the server to authenticate to the user.

States of Data

Data in Process

- Data in process refers to data during initial input, modification, computation, or output.

Input	Protection of data integrity starts with the initial input of data. Organizations use several methods to collect data, each posing a potential threat to data integrity: data entry, scanning forms, file uploads, and data collected from sensors. Corruption during the input process may include mislabeling and incorrect or mismatched data formats, data entry errors, or disconnected and/or malfunctioning or inoperable system sensors.
Modification	Data modification is any change made to original data, such as users manually modifying data, and programs processing and changing data. These changes are intentional, but changes to data can be unintentional or malicious. When data is modified in a way that stops it from being readable or usable, this is often referred to as data corruption.
Output	Data output refers to outputting data to output devices, such as printers, electronic displays and speakers. The accuracy of output data is critical because output provides information and influences decision-making.

Data in Process (Cont.)

- Protecting data in process requires well-designed systems. Otherwise, the results for organizations can be severe and costly to their finances or even their reputation.

- It is the role of cybersecurity professionals to design comprehensive policies and procedures regarding testing, maintenance, and updates to keep systems operating with the least number of errors.

States of Data

Lab - Data Security Challenges

In this lab, you will consider the challenges to secure:

- Data at Rest
- Data in Transit
- Data in Process

10.3 Cybersecurity Countermeasures

Cybersecurity Countermeasures

Hardware-Based and Software-Based Technologies

- Both software and hardware are utilized to protect the data and systems of organizations.
- Software safeguards include programs and services that protect operating systems, databases and other services operating on workstations, portable devices and servers.
- Administrators can install software-based countermeasures or safeguards on individual hosts or servers:

Software firewalls	They control remote access to a system. Operating systems typically include a firewall, or a user can purchase or download software from a third party.
Network and port scanners	They discover and monitor open ports on a host or server.
Protocol analyzers	Devices that collect and examine network traffic. They identify problems of performance and misbehaving applications, detect misconfigurations, establish baseline and normal traffic patterns and debug communication problems.
Vulnerability scanners	Programs designed to assess weaknesses on computers or networks.
Host-based intrusion detection systems (IDS)	They examine activity on host systems only. An IDS generates log files and alarm messages when it detects unusual activity.

Hardware-Based and Software-Based Technologies (Cont.)

- There are several hardware-based technologies used to safeguard an organization’s assets:

Firewalls	They block unwanted traffic. They contain customizable rules that define the traffic allowed into and out of a network.
Proxy servers	They use a network addressing scheme to present one organization-wide IP address to the Internet. A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.
Hardware-based access control	Devices that utilize biometric technology, such as fingerprint or iris scanners, to confirm the identity of anyone trying to access servers, data, and systems.
Network switches	Switches are commonly used as a connection point, linking other devices together, for example in a local area network. Their features enable them to add to the security efficiency of the network.

Establishing a Culture of Cybersecurity Awareness

- Investing a lot of money in technology will not make a difference if the people within the organization are not trained in cybersecurity.

- A security awareness program and solid, comprehensive security policies are extremely important for any organization.

- An employee might not be purposefully malicious but just unaware of what the proper procedures are and still cause great harm.

- There are several ways to implement training to prevent this and to ensure all employees feel knowledgeable and confident to make cybersecurity best practices part of their day-to-day activities.

Establishing a Culture of Cybersecurity Awareness (Cont.)

Education and training:

- Make security awareness training a part of an organization's onboarding process.
- Tie security awareness to job requirements or performance evaluations.
- Conduct in-person training sessions using gamification and activities (for example, capture the flag scenarios).
- Complete online modules and courses - such as the eLearning @Apollo creates.

Security awareness programs

- An active security awareness program depends on:
  - The organization's environment and network.
  - The level of threat.
  - The nature and demands of the data the organization holds.
- People are the first line of defense in cybersecurity, and every organization is only as strong as its weakest link.
- Every member of an organization must be aware of its security policies and implement them in their day-to-day activities.

Policies

- A security policy sets out the security objectives, rules of behavior and system requirements to be adhered to.

- A comprehensive security policy accomplishes several tasks:
  - It demonstrates an organization's commitment to security.
  - It sets the rules for expected behavior.
  - It ensures consistency in system operations and software and hardware acquisition, use, and maintenance.
  - It defines the legal consequences of violations.
  - It gives security staff the backing of management.

- Security policies inform users, staff, and managers of the organization's requirements, which protect technology and information assets.

- A security policy also specifies the mechanisms needed to meet security requirements.

Cybersecurity Countermeasures

Policies (Cont.)

A security policy typically includes:

Identification and authentication policies	Specify authorized persons that can have access to network resources and outlines verification procedures for said users.
Password policies	Ensure passwords meet minimum requirements and are changed regularly.
Acceptable use policies	Identify network resources and usage that are acceptable to the organization. It may also identify ramifications for policy violations.
Remote access policies	Identify how remote users can access a network and what is remotely accessible.
Network maintenance policies	Specify network device operating systems and end-user application update procedures.
Incident handling policies	Describe how security incidents are to be handled.

- One of the most common security policy components is an acceptable use policy (AUP). This component defines what users can and cannot do on the various system components.

Standards

- Standards help IT staff maintain consistency in operating the network.
- Security policies inform users, staff, and managers of the organization’s technology and information asset protection requirements.
- One of the most important security principles is consistency.
- Each organization develops standards that support its unique operating environment.
- An example of a standard would be an organization’s password policy.
    - The standard could stipulate that passwords require a minimum number of uppercase and lowercase alphanumeric and special characters.
    - The password policy may specify that users must change their passwords every 30 days.
    - A password history may be kept for the 12 most recent passwords to prevent anyone from reusing the same passwords during a twelve-month period.

Guidelines

- Guidelines are a list of suggestions on how to do things more efficiently and securely.
- Guidelines define how standards are developed and guarantee adherence to general security policies.
- In addition to an organization’s defined best practices, guidelines are also available from:
    - National Institute of Standards and Technology (NIST) Computer Security Resource Center
    - National Security Agency (NSA) Security Configuration Guides
    - The Common Criteria standard

10.4 Cybersecurity Principles, Practices, and Processes Summary

What Did I Learn in this Module?

- Wired networks use cables to transmit data. They include copper and fiber optic media and can serve a local area network (LAN) or span great distances in wide area networks (WAN).
- The first dimension of the cybersecurity cube identifies the goals to protect cyberspace: data confidentiality, data integrity, and data availability.
- The second dimension represents the three possible data states: data in transit, data at rest or in storage, and data in process.
- The third dimension defines the pillars on which to base your cybersecurity defenses. They are technology, policy and practices, and improving education, training, and awareness in people.
- Tokenization is a substitution technique that can isolate data elements from exposure to other data systems.
- Rights management covers both digital rights management (DRM) and information rights management (IRM)
- Types of sensitive information are categorized as personal, business, and classified.
- Integrity is the accuracy, consistency, and trustworthiness of data across its entire lifecycle.
- Methods to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls.
- Availability ensures that information can be accessed whenever it is needed.

What Did I Learn in this Module? (Cont.)

- Information security requires data to be protected when it is at rest, in transit, and in process.
- Data is at rest when no user or process is accessing, requesting, or amending it.
- Data can be stored in DAS, RAID, NAS, SAN, or in the cloud.
- Data in transit is data which is being transmitted
- A sneaker net uses removable media to physically move data from one computer to another.
- Standard protocols such as IP and HTTP define the structure and formation of data packets.
- Data in process refers to data during initial input, modification, computation, or output.
- Protection of data integrity starts with the initial input of data.
- Organizations use several methods to collect data, each posing a potential threat to data integrity: data entry, scanning forms, file uploads, and data collected from sensors.
- Software-based countermeasures or safeguards can be installed on individual hosts or servers: software firewalls, network and port scanners, protocol analyzers, vulnerability scanners, and host-based IDS.
- An active security awareness program depends on the organization's environment and network, the level of threat, and the nature and demands of the data the organization holds.
- A comprehensive security policy demonstrates an organization’s commitment to security.
- Types of security policies include identification and authentication, passwords, acceptable use, remote access, network maintenance, and incident handling.