Module 6: The Cybersecurity Cube

Objectives

- The Cybersecurity Cube

  Describe the three dimensions of the McCumber Cube (Cybersecurity Cube).
- CIA TRIAD

  Describe the principles of confidentiality, integrity, and availability.
- States of Data

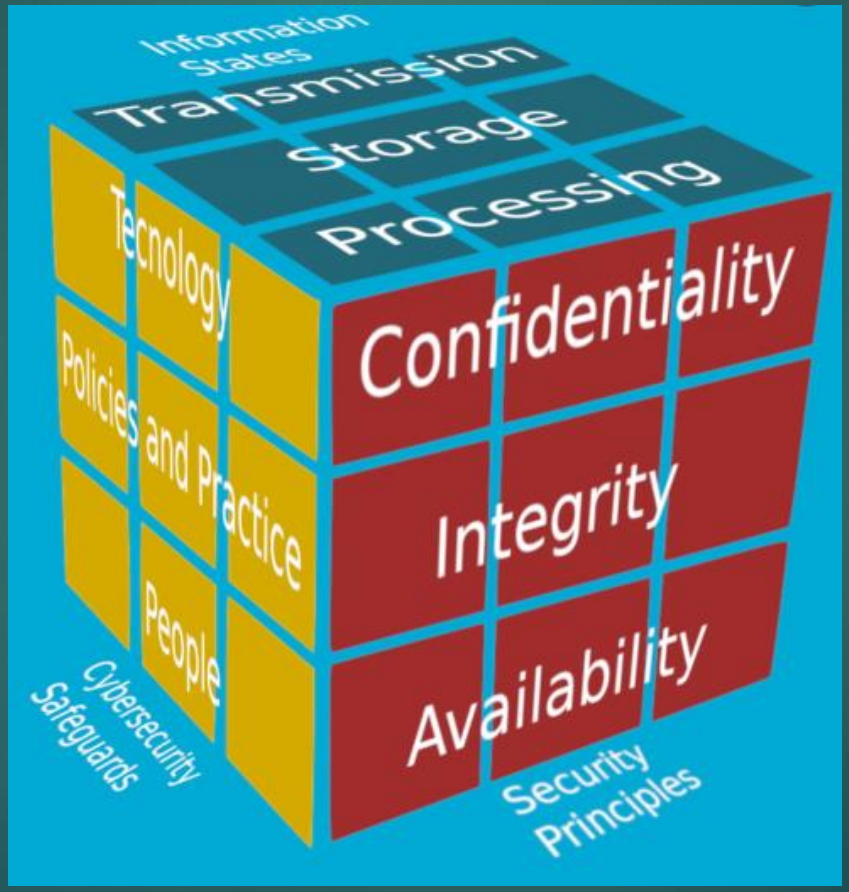
  Differentiate the three states of data.
- Cybersecurity Countermeasures

  Compare the types of cybersecurity countermeasures.
- IT Security Management Framework

  Describe the ISO Cybersecurity Model

The Three Dimensions of the Cybersecurity Cube

The Three Dimensions

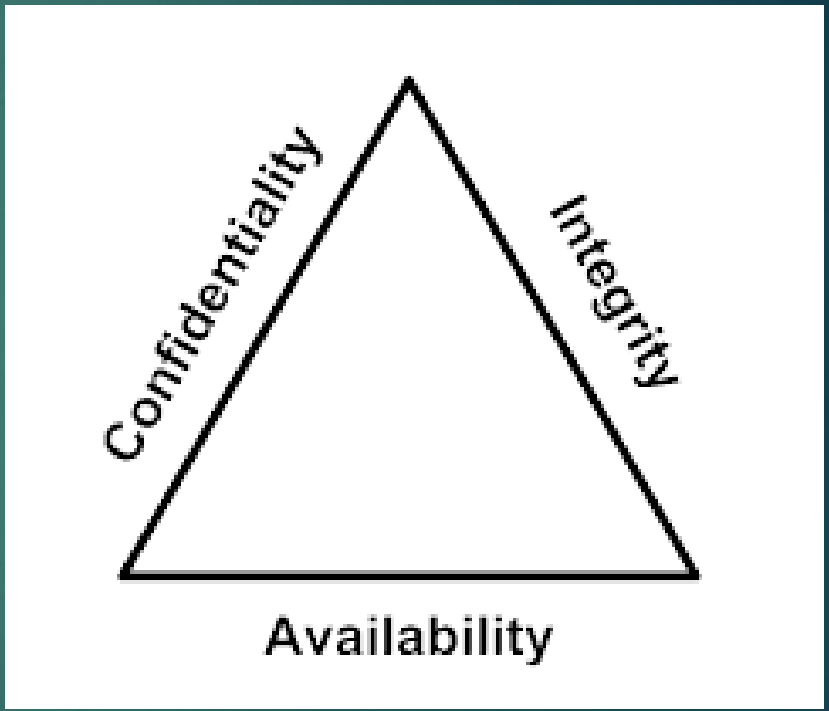


The Three Dimensions of the Cybersecurity Cube

The Three Dimensions

The Principles of Security:

- The first dimension of the cybersecurity cube identifies the goals to protect the cyber world. The goals identified in the first dimension are the foundational principles of the cybersecurity world.
- These three principles are confidentiality, integrity and availability.
- The principles provide focus and enable cybersecurity specialists to prioritize actions in protecting the cyber world.
- Use the acronym CIA to remember these three principles.



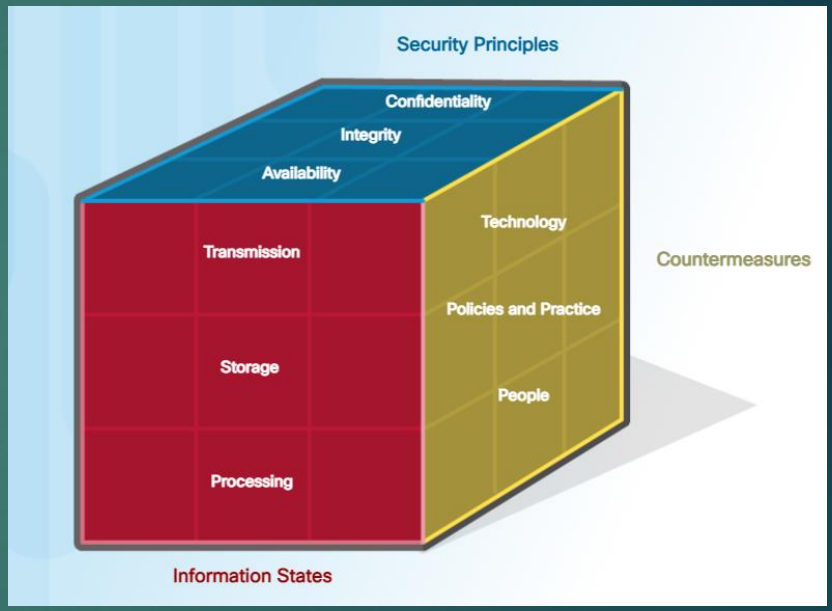
The Three Dimensions of the Cybersecurity Cube

The Three Dimensions

The States of Data

- The cyber world is a world of data; therefore, cybersecurity specialists focus on protecting data. The second dimension of the cybersecurity cube focuses on the problems of protecting all of the states of data in the cyber world. Data has three possible states:

1) Data at rest or in storage 2) Data in transit 3) Data in process

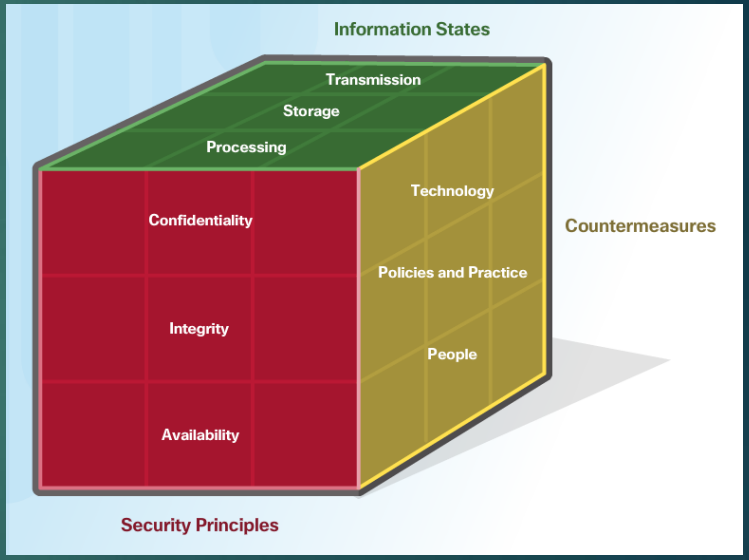


The Three Dimensions of the Cybersecurity Cube

The Three Dimensions (Cont.)

Cybersecurity Safeguards

- The third dimension of the cybersecurity sorcery cube defines the types of powers used to protect the cyber world. The sorcery cube identifies the three types of powers:
- **Technologies -** devices, and products available to protect information systems and fend off cyber criminals.
- **Policies and Practices -** procedures, and guidelines that enable the citizens of the cyber world to stay safe and follow good practices.
- **People -** Aware and knowledgeable about their world and the dangers that threaten their world.



CIA TRIAD

Confidentiality

The Principle of Confidentiality

- Confidentiality prevents the disclosure of information to unauthorized people, resources and processes. Another term for confidentiality is privacy.
- Organizations need to train employees about best practices in safeguarding sensitive information to protect themselves and the organization from attacks.
- Methods used to ensure confidentiality include data encryption, authentication, and access control.

Protecting Data Privacy

- Organizations collect a large amount of data and much of this data is not sensitive because it is publicly available, like names and telephone numbers.
- Other data collected, though, is sensitive. Sensitive information is data protected from unauthorized access to safeguard an individual or an organization.

CIA TRIAD

Confidentiality (Cont.)

Controlling Access

Access control defines a number of protection schemes that prevent unauthorized access to a computer, network, database, or other data resources.

The concepts of AAA involve three security services: Authentication, Authorization and Accounting.

- ***Authentication*** verifies the identity of a user to prevent unauthorized access. Users prove their identity with a username or I.D.
- ***Authorization*** services determine which resources users can access, along with the operations that users can perform. Authorization can also control when a user has access to a specific resource.
- ***Accounting*** keeps track of what users do, including what they access, the amount of time they access resources, and any changes made.

CIA TRIAD

Confidentiality (Cont.)

Confidentiality and privacy seem interchangeable, but from a legal standpoint, they mean different things.

- Most privacy data is confidential, but not all confidential data is private. Access to confidential information occurs after confirming proper authorization. Financial institutions, hospitals, medical professionals, law firms, and businesses handle confidential information.
- Confidential information has a non-public status. Maintaining confidentiality is more of an ethical duty.
- Privacy is the appropriate use of data. When organizations collect information provided by customers or employees, they should only use that data for its intended purpose.

- The Personal Information Protection and Electronic Documents Act (Canada)
- Computer Processed Personal Information Protection Act (China)
- Act on the Protection of Personal Information (Japan)
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Russia)
- Article 8 European Convention on Human Rights (United Kingdom)

CIA TRIAD

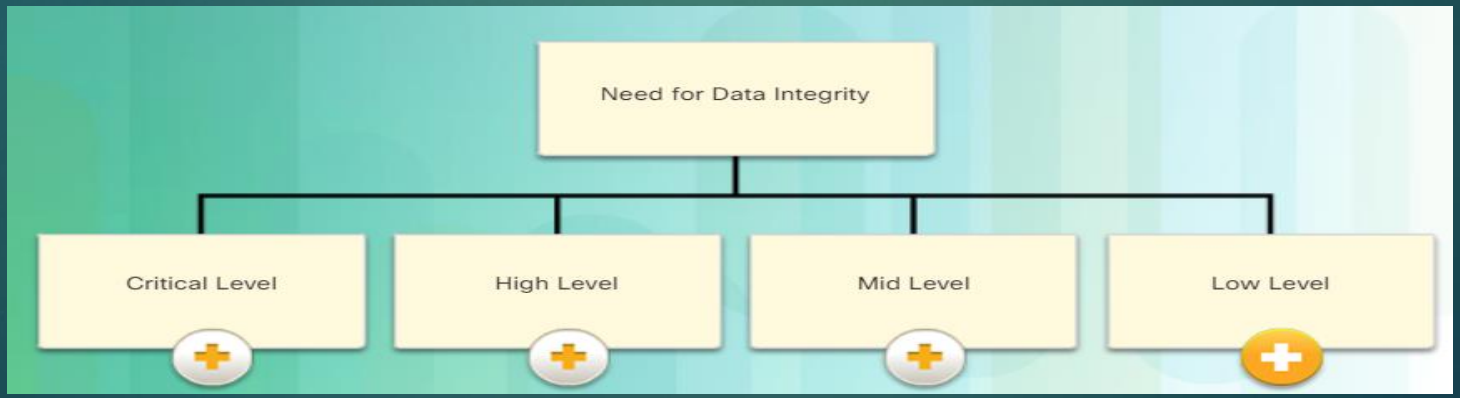
Integrity

Principle of Data Integrity

- Integrity is the accuracy, consistency, and trustworthiness of data during its entire life cycle.
- Another term for integrity is quality.
- Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls.

Need for Data Integrity

- The need for data integrity varies based on how an organization uses data.
- Protecting data integrity is a constant challenge for most organizations. Loss of data integrity can render entire data resources unreliable or unusable.

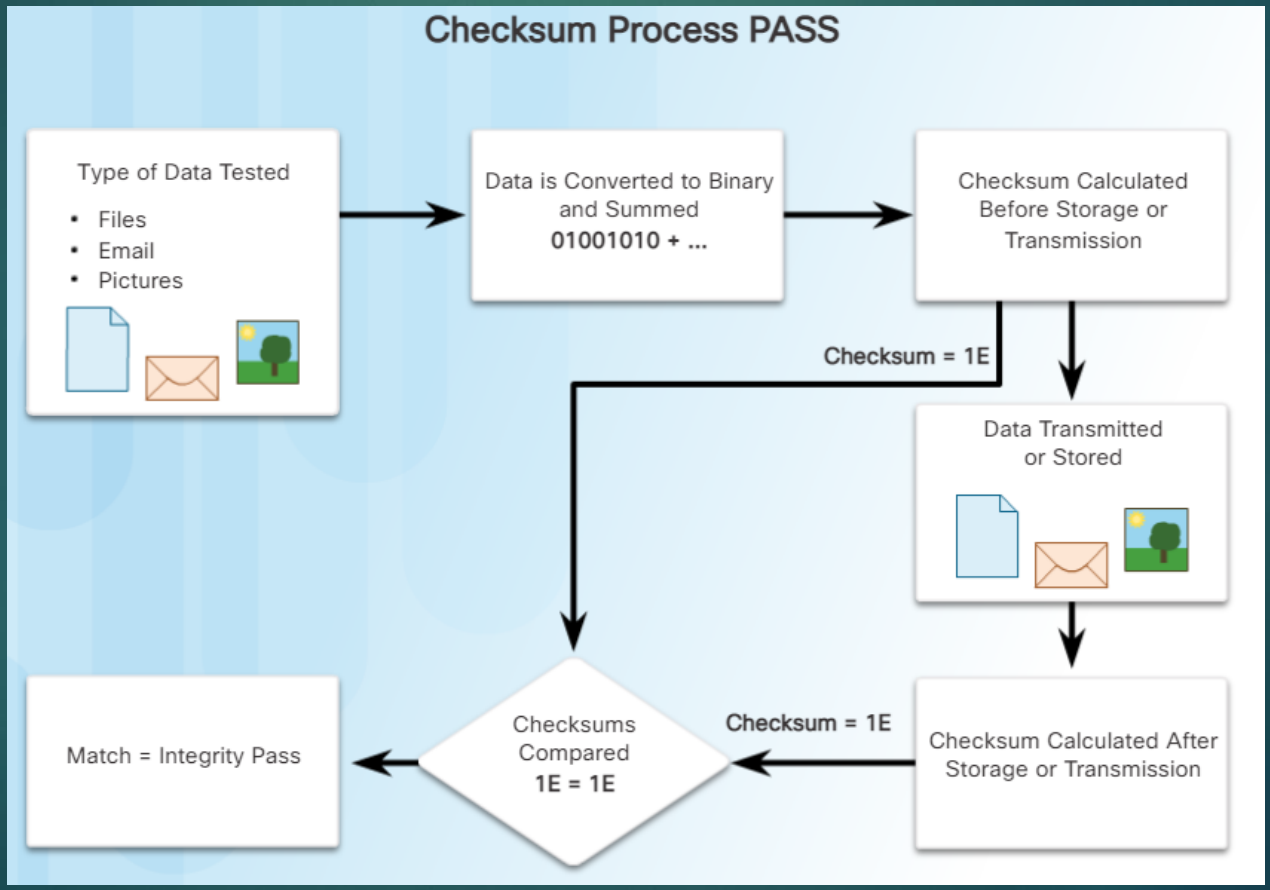


CIA TRIAD

Integrity

Integrity Checks

- An integrity check is a way to measure the consistency of a collection of data (a file, a picture, or a record). The integrity check performs a process called a hash function to take a snapshot of data at an instant in time.



CIA TRIAD

Availability

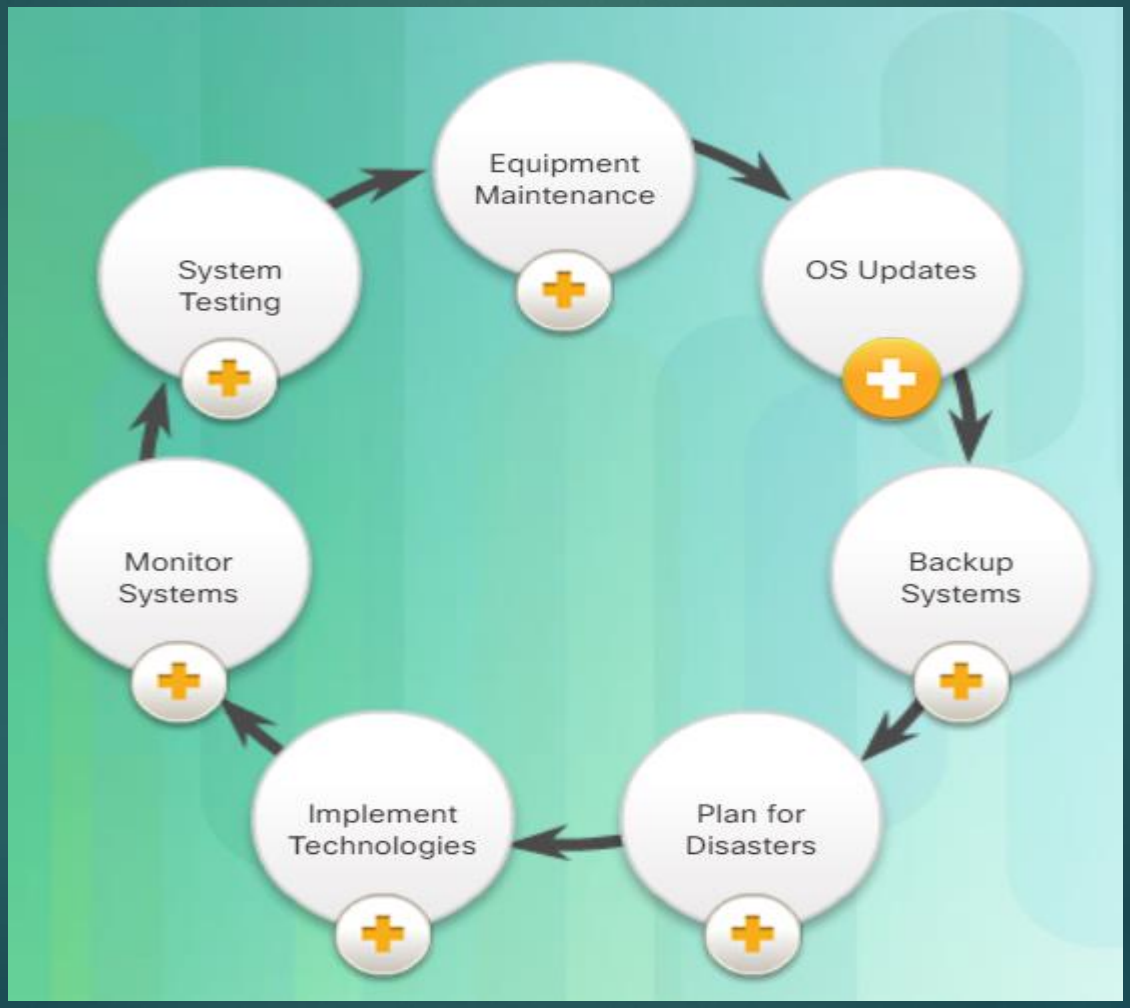
Data availability is the principle used to describe the need to maintain availability of information systems and services at all times. Cyberattacks and system failures can prevent access to information systems and services.

- High availability systems typically include three design principles: eliminate single points of failure, provide for reliable crossover, and detect failures as they occur.

CIA TRIAD

Availability

Organizations can ensure availability by implementing the following:



Activity– Principles of Cybersecurity

Cybersecurity Safeguards	Confidentiality	Integrity	Availability
Hashing Files and Data Structures			
Redundancy			
Encryption			
Eliminate Single Points of Failure			
Identification and Authentication			
Password & ID Badges			
Data Backups			
Biometrics			

States of Data

Data at Rest

- Stored data refers to data at rest. Data at rest means that a type of storage device retains the data when no user or process is using it.
- A storage device can be local (on a computing device) or centralized (on the network). A number of options exist for storing data.
  - Direct-attached storage (DAS) is storage connected to a computer. A hard drive or USB flash drive is an example of direct-attached storage.
  - Redundant array of independent disks (RAID) uses multiple hard drives in an array, which is a method of combining multiple disks so that the operating system sees them as a single disk. RAID provides improved performance and fault tolerance.

States of Data

Data at Rest (Cont.)

- A network attached storage (NAS) device is a storage device 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 administrators can increase the capacity as needed.
- A storage area network (SAN) architecture is a network-based storage system. SAN systems connect to the network using high-speed interfaces allowing improved performance and the ability to connect multiple servers to a centralized disk storage repository.
- Cloud storage is a remote storage option that uses space on a data center provider and is accessible from any computer with Internet access. Google Drive, iCloud, and Dropbox are all examples of cloud storage providers.

States of Data

Data In Transit

Data transmission involves sending information from one device to another. There are numerous methods to transmit information between devices including:

- **Sneaker net** – uses removable media to physically move data from one computer to another
- **Wired networks** – uses cables to transmit data
- **Wireless networks** – uses the airwaves to transmit data

The protection of transmitted data is one of the most challenging jobs of a cybersecurity professional. The greatest challenges are:

- **Protecting data confidentiality** – cyber criminals can capture, save and steal data in-transit.
- **Protecting data integrity** – cyber criminals can intercept and alter data in-transit.
- **Protecting data availability** - cyber criminals can use rogue or unauthorized devices to interrupt data availability.

States of Data

Data In Process

The third state of data is data in process. This 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, such as manual data entry, scanning forms, file uploads, and data collected from sensors.
- Each of these methods pose potential threats to data integrity.
- Data modification refers to any changes to the original data such as users manually modifying data, programs processing and changing data, and equipment failing resulting in data modification.
- Processes like encoding/decoding, compression/decompression and encryption/decryption are all examples of data modification. Malicious code also results in data corruption.

Activity – Identify the State of Data for a Given Technology

Description	Data at Rest	Data in Transit	Data in Process
SAN and NAS			
VPN or SSL			
USB Flash Drive			
Wireless WEP			
Data Backup			
Modification of a Database Record			
Direct-Attached Storage			
Data Entry by a Clerk			

Cybersecurity Countermeasures

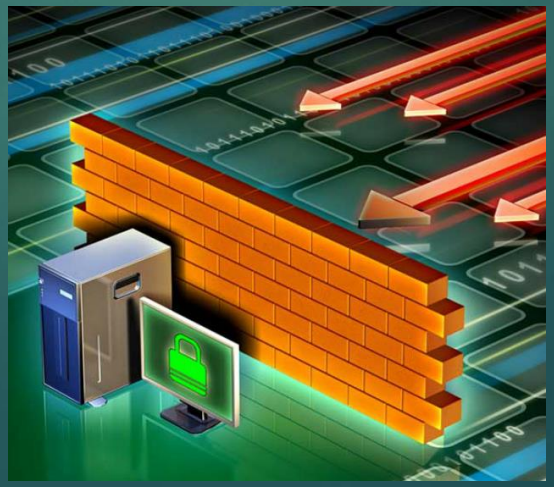
Technologies

Software-based Technology Safeguards

- Software safeguards include programs and services that protect operating systems, databases, and other services operating on workstations, portable devices, and servers. There are several software-based technologies used to safeguard an organization's assets.

Hardware-based Technology Safeguards

- Hardware based technologies are appliances that are installed within the network faculties. They can include: Firewall appliances, Intrusion Detection Systems (IDS),Intrusion Prevention Systems (IPS) and Content filtering systems.



Cybersecurity Countermeasures

Technologies

Network-based Technology Safeguards

Technological countermeasures can also include network-based technologies.

- **Virtual Private Network (VPN)** is a secure virtual network that uses the public network (i.e., the Internet). The security of a VPN lies in the encryption of packet content between the endpoints that define the VPN.
- **Network access control (NAC)** requires a set of checks before allowing a device to connect to a network. Some common checks include up-to-data antivirus software or operating system updates installed.
- **Wireless access point security** includes the implementation of authentication and encryption.

Cybersecurity Countermeasures

Technologies

Cloud-based Technology Safeguards

- The three main cloud computing services include:
  - **Software as a Service (SaaS)** allows users to gain access to application software and databases. Cloud providers manage the infrastructure. Users store data on the cloud provider's servers.
  - **Infrastructure as a Service (IaaS)** provides virtualized computing resources over the Internet. The provider hosts the hardware, software, servers, and storage components.
  - **Platform as a Service (PaaS)** provides access to the development tools and services used to deliver the applications.
- Cloud service providers use virtual security appliances that run inside a virtual environment with a pre-packaged, hardened operating system running on virtualized hardware.

Cybersecurity Countermeasures

Implementing Cybersecurity Education and Training

A security awareness program is extremely important for an organization. An employee may not be purposefully malicious but just unaware of what the proper procedures are.

There are several ways to implement a formal training program:

- Make security awareness training a part of the employee's onboarding process
- Tie security awareness to job requirements or performance evaluations
- Conduct in-person training sessions
- Complete online courses

Security awareness should be an ongoing process since new threats and techniques are always on the horizon.

Cybersecurity Policies and Procedures

- A security **policy** is a set of security objectives for a company that includes rules of behavior for users and administrators and specifies system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems within an organization.
- **Standards** help an IT staff maintain consistency in operating the network. Standards provide the technologies that specific users or programs need in addition to any program requirements or criteria that an organization must follow.
- **Guidelines** are a list of suggestions on how to do things more efficiently and securely. They are similar to standards, but are more flexible and are not usually mandatory. Guidelines define how standards are developed and guarantee adherence to general security policies.
- **Procedure** documents are longer and more detailed than standards and guidelines. Procedure documents include implementation details that usually contain step-by-step instructions and graphics.

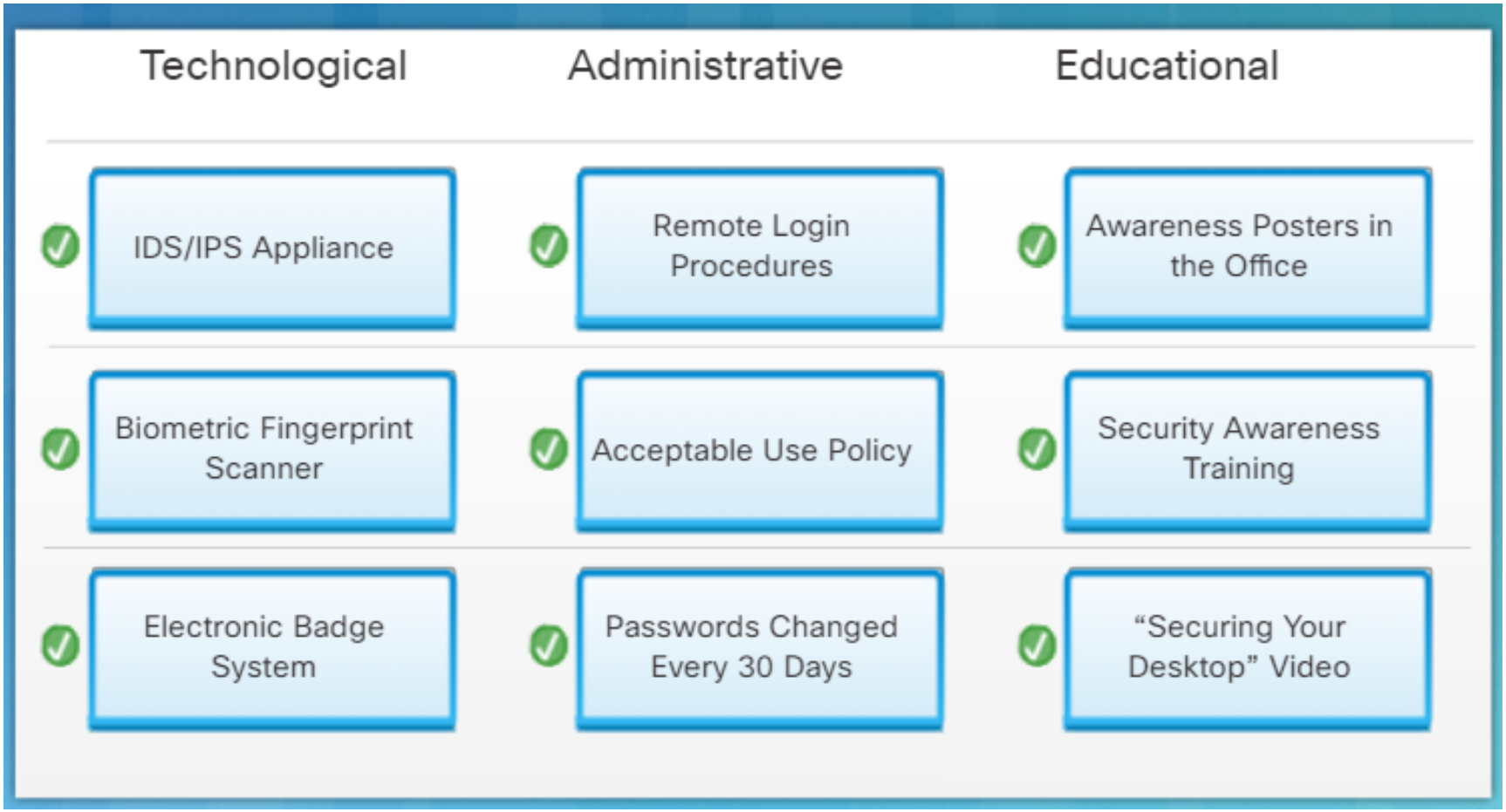
Identify the Countermeasure Category

Instructions

Match each safeguard to the column representing the correct CIA countermeasures category.

Biometric Fingerprint Scanner	Awareness Posters in the Office	IDS/IPS Appliance
Security Awareness Training	Passwords Changed Every 30 Days	Electronic Badge System
"Securing Your Desktop" Video	Remote Login Procedures	Acceptable Use Policy

Technological	Administrative	Educational


Technological
Administrative
Educational
IDS/IPS Appliance
Remote Login Procedures
Awareness Posters in the Office
Biometric Fingerprint Scanner
Acceptable Use Policy
Security Awareness Training
Electronic Badge System
Passwords Changed Every 30 Days
“Securing Your Desktop” Video

Security Management Framework

The ISO Model

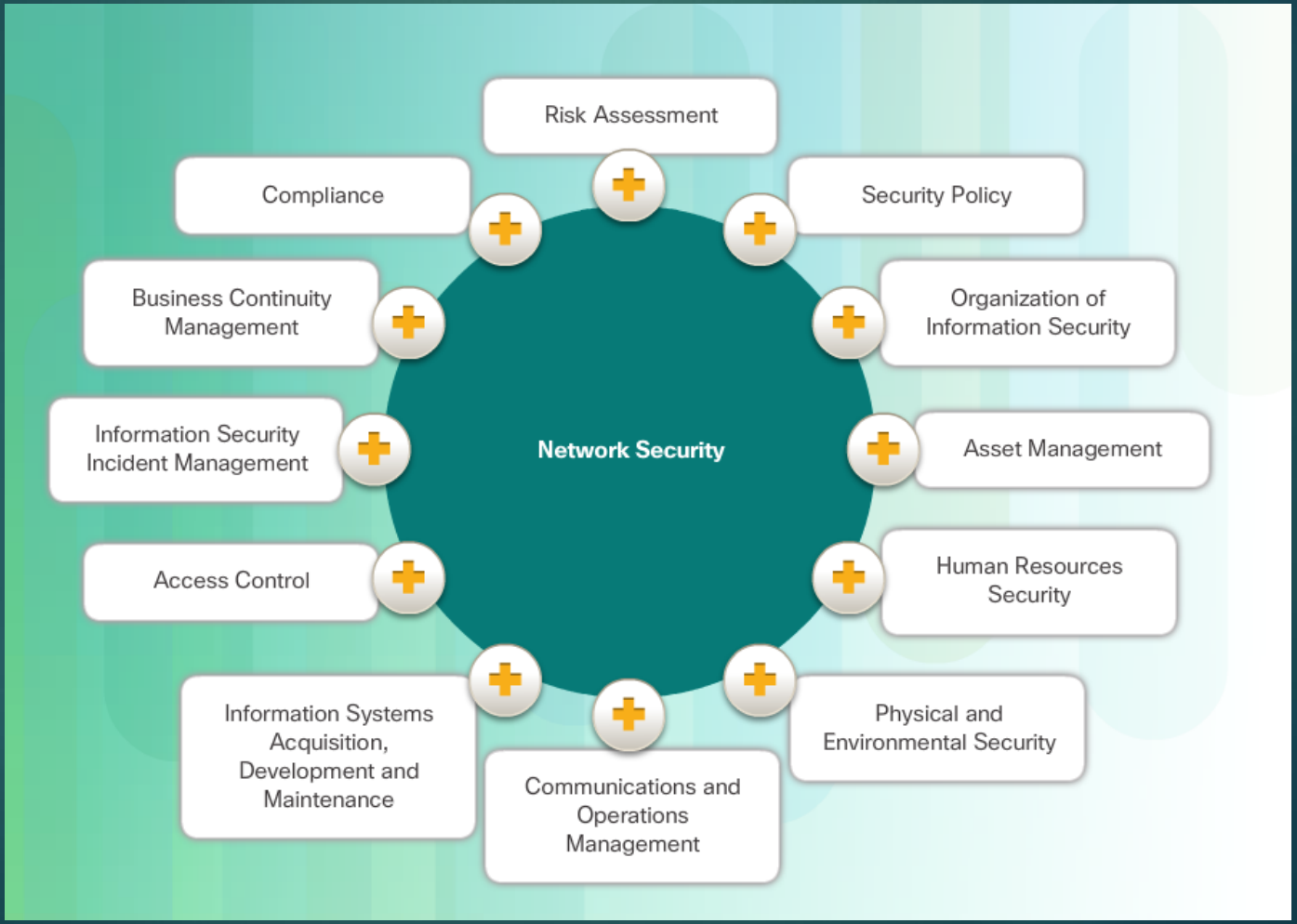
The **International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)** developed a comprehensive framework to guide information security management.

ISO/IEC 27000 is an information security standard published in 2005 and revised in 2013.

Security Management Framework

The ISO Model (Cont.)

The ISO 27000 standards describe the implementation of a comprehensive information security management system (ISMS).



Activity – Identify the ISO/IEC 27000 Domains and Controls

Instructions

Match the ISO/IEC Domain to the appropriate cybersecurity control.

Physical/Environmental Security

Business Continuity Management

Security Policy

Access Control

Asset Management

Risk Management

Check

Reset

ISO/IEC 27000 Domains	Cybersecurity Controls
	Evaluation of individual threats to the organization.
	Implementation of multi-factor authentication system.
	Definition of strong password requirements.
	Implementing tagging, inventory and tracking of mobile and laptop computers.
	Installation of lighting, fencing and security guards systems.
	Operation of data backup and restoration systems.

Activity – Identify the ISO/IEC 27000 Domains and Controls

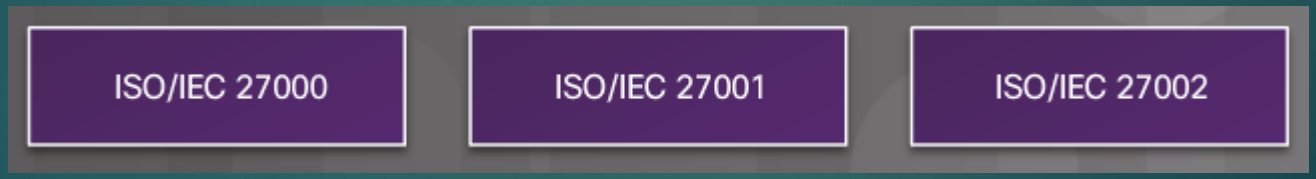
ISO/IEC 27000 Domains	Cybersecurity Controls
Risk Management	Evaluation of individual threats to the organization.
Access Control	Implementation of multi-factor authentication system.
Security Policy	Definition of strong password requirements.
Asset Management	Implementing tagging, inventory and tracking of mobile and laptop computers.
Physical/Environmental Security	Installation of lighting, fencing and security guards systems.
Business Continuity Management	Operation of data backup and restoration systems.

Security Management Framework

Using the ISO Cybersecurity Model (Cont.)

The ISO Cybersecurity Model and Safeguards

- The ISO 27001 control objectives relate directly to the organization's cybersecurity policies, procedures and guidelines which upper management determines.
- The ISO 27002 controls provide technical direction. For example, upper management establishes a policy specifying the protection of all data coming in to or out of the organization. Implementing the technology to meet the policy objectives would not involve upper management.
- It is the responsibility of IT professionals to properly implement and configure the equipment used to fulfill the policy directives set by upper management.



Summary

- This chapter discussed the three dimensions of the cybersecurity sorcery cube. The central responsibility of a cybersecurity specialist is to protect an organization's systems and data.
- The chapter explained how each of the three dimensions contributes to that effort.
- The chapter also discussed the ISO cybersecurity model. The model represents an international framework to standardize the management of information systems.
- This chapter explored the twelve domains. The model provides control objectives that guide the high-level design and implementation of a comprehensive information security management system (ISMS).
- The chapter also discussed how security professionals use controls to identify the technologies, devices, and products to protect the organization.
- If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.