Lesson 01

In this week student will obtain the knowledge to;

- Define Information Security, Cybersecurity & Network Security

- Understand three dimensional security approach

- Define states of Data

- Explain about IT Security Management Framework

Last modified by E1946350 Kahatapitiya KKPL on Sunday, 5 July 2020, 2:56 PM
This document was downloaded on Friday, 23 December 2022, 1:26 AM

Introduction

This lesson will;

- Define Information Security, Cybersecurity and Network Security
- Describe the three dimensions of the McCumber Cube
- Describe the principles of confidentiality, integrity, and availability
- Differentiate the three states of data.
- Describe the ISO Cybersecurity Model

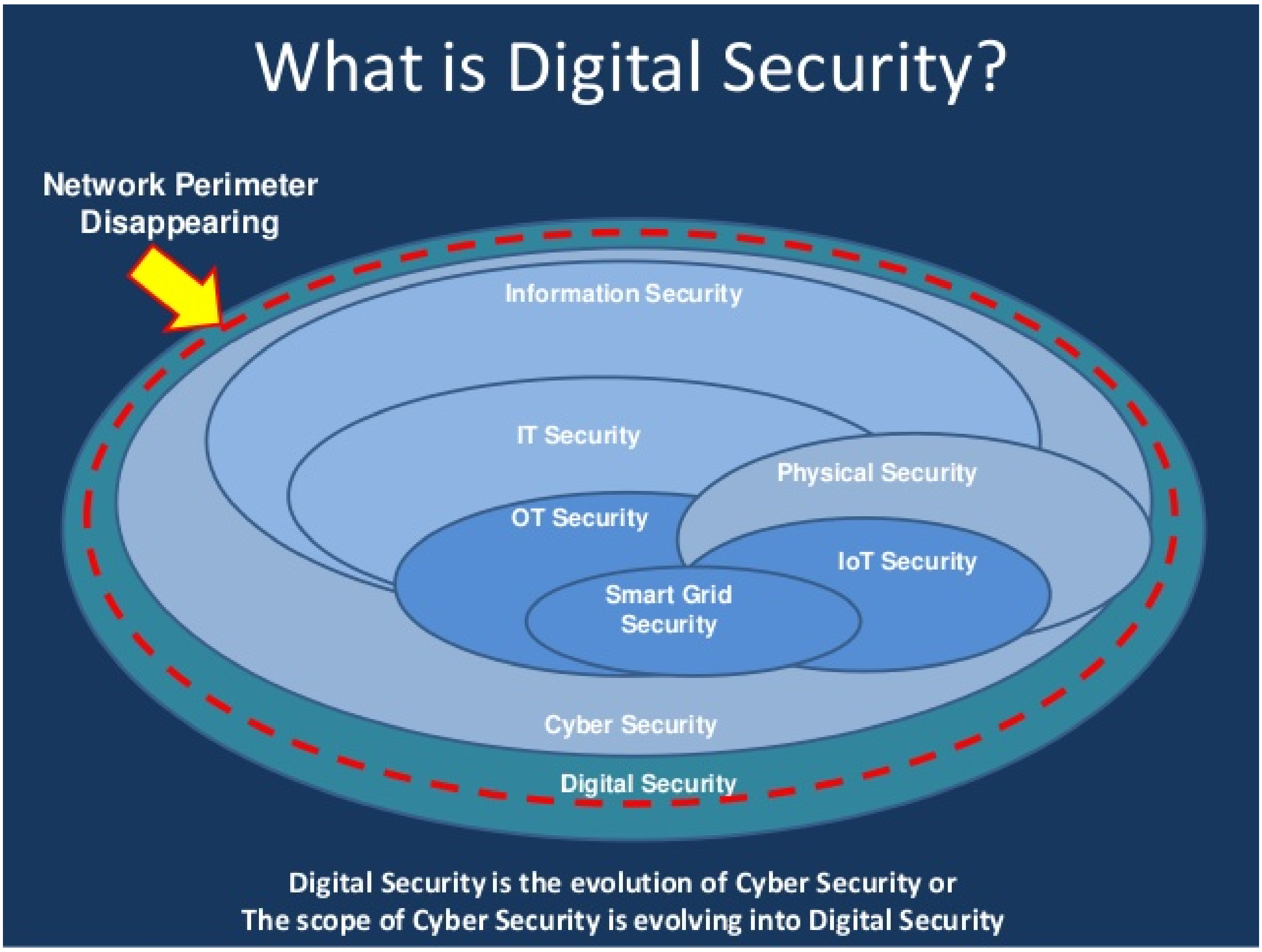
IMPORTANT: At the end of the lesson there will be one quiz which is using for grading.

Information Security, Cybersecurity & Network Security

Do you think Information Security, Cybersecurity & Network Security are describing the same thing? The answer is 'No'. These three areas are explaining different dimension of Security. However, they are interrelated in different levels.

According to the NISTIR 7298r2 document published by National Institute of Standards and Technology (NIST) - USA, Security has defined as a condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.

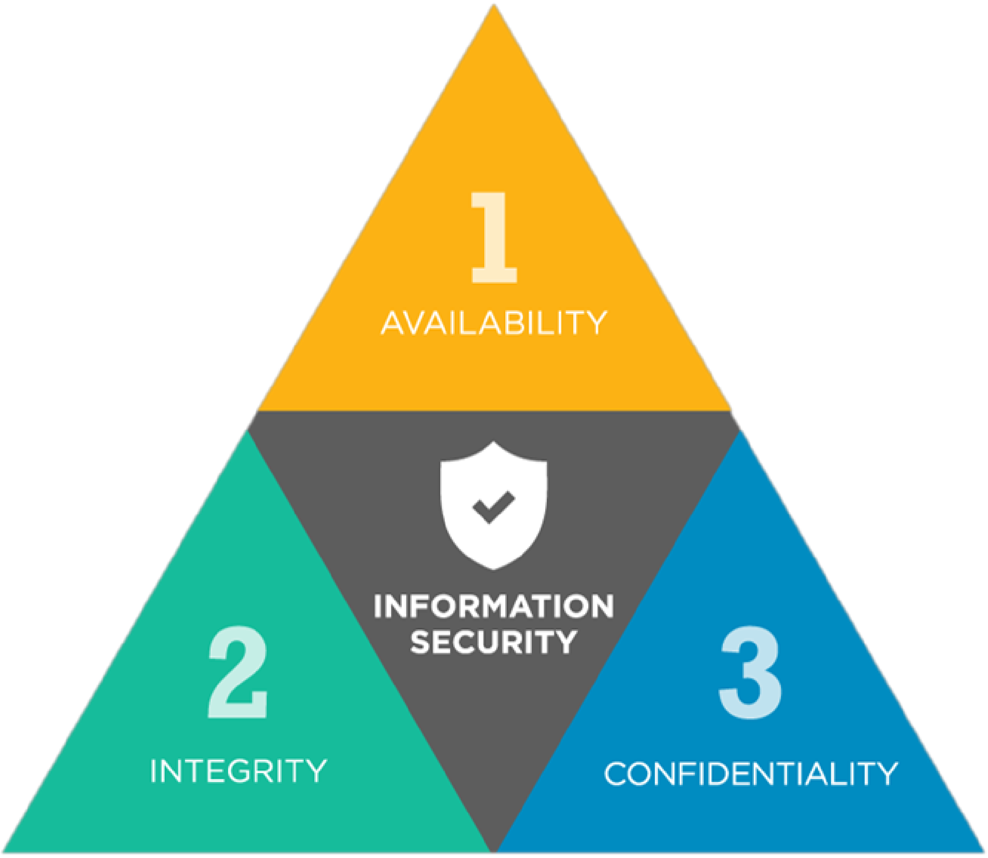
Furthermore, security can be divided in to many sub categories such as Information Security, Cybersecurity, Network Security, Computer Security, etc.


What is Digital Security?
Network Perimeter Disappearing
Information Security
IT Security
Physical Security
OT Security
IoT Security
Smart Grid Security
Cyber Security
Digital Security
Digital Security is the evolution of Cyber Security or
The scope of Cyber Security is evolving into Digital Security

What is Information Security?

The Information Security has defined in NISTIR 7298r2 document as;

"*The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.*"



Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity

Availability

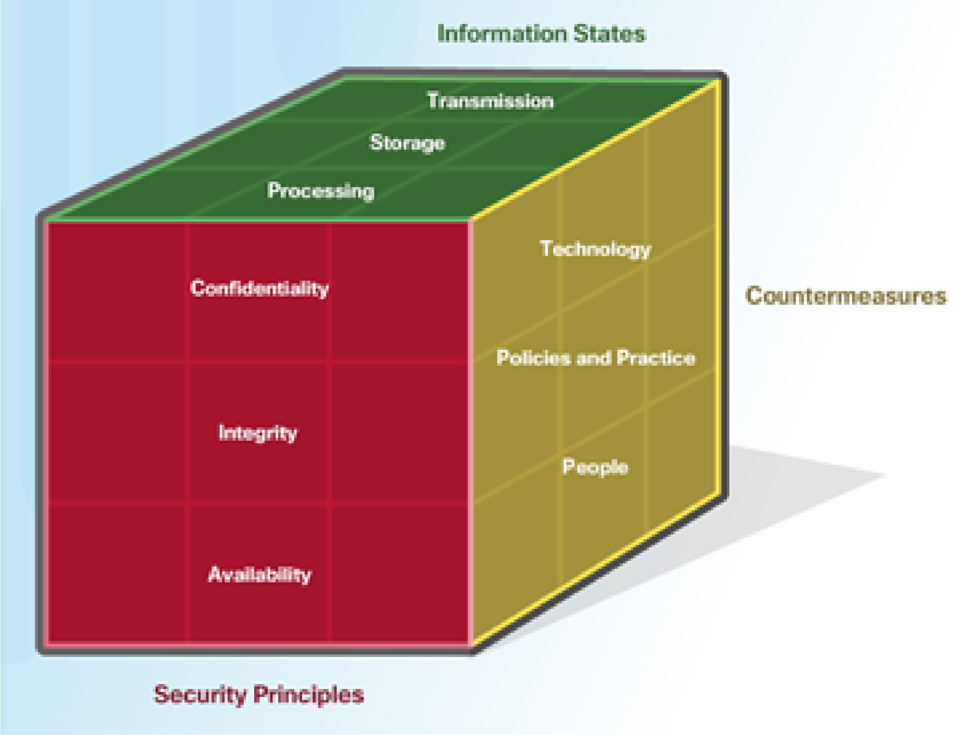
Ensuring timely and reliable access to and use of information.

What is Cybersecurity?

Cybersecurity is "The ability to protect or defend the use of cyberspace from cyber attacks."

Cyberspace is a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

To protect cyberspace, cybersecurity professionals use the Cybersecurity Sorcery Cube to identify, analyse and mitigate cyber attacks.



There are three dimensions explained in Cybersecurity Sorcery Cube.

Security Principles

The goals identified in the first dimension are the foundation principles of the cybersecurity world.

Information State

The cyber world is a world of data; therefore, cyber wizards focus on protecting data. The second dimension of the cybersecurity sorcery cube focuses on the problems of protecting all of the states of data in the cyber world.

Countermeasures

The third dimension of the cybersecurity sorcery cube defines the types of powers used to protect the cyber world.

What is Network Security?

Network Security will provide the assurance to the information when the communication happens.

In other words Network Security measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Therefore, may best practices are followed by organizations to protect their networks from network attacks.

Network Security Best Practices

- Develop a written security policy.
- Educate employees about the risks of social engineering, and develop strategies to validate identities over the phone, via email, or in person.
- Control physical access to systems.
- Use strong passwords and change them often.
- Encrypt and password-protect sensitive data.
- Implement security hardware and software.
- Perform backups and test the backed up files on a regular basis.
- Shut down unnecessary services and ports.
- Keep patches up-to-date by installing them weekly or daily to prevent buffer overflow and privilege escalation attacks.
- Perform security audits to test the network.

Principle of Confidentiality

Confidentiality prevents the disclosure of information to unauthorized people, resources and processes. Another term for confidentiality is privacy. Organizations restrict access to ensure that only authorized operators can use data or other network resources. For example, a programmer should not have access to the personal information of all employees.

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.

Organizations collect a large amount of data. 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. There are three types of sensitive information:

- **Personal information** is personally identifiable information (PII) that traces back to an individual.

- **Business information** is information that includes anything that poses a risk to the organization if discovered by the public or a competitor.

- **Classified information** is information belonging to a government body classified by its level of sensitivity.

Access controlling is one of a essential practice to implement confidentiality in information.The 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. These services provide the primary framework to control access.

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. Most organizations will require the customer or employee to sign a release form giving the organization permission to use the data.

Principle of Data Integrity

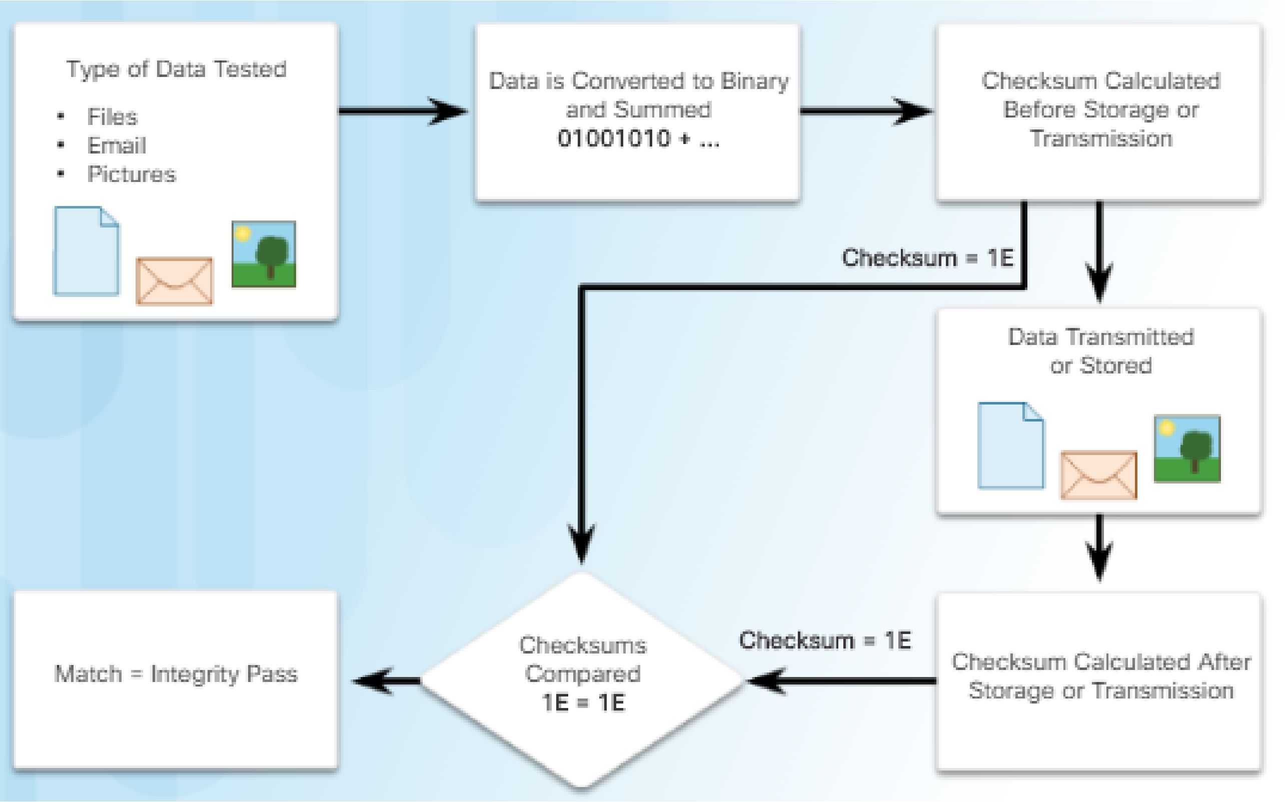
Integrity is the accuracy, consistency, and trustworthiness of data during its entire life cycle. Another term for integrity is quality. Data undergoes a number of operations such as capture, storage, retrieval, update, and transfer. Data must remain unaltered during all of these operations by unauthorized entities.

Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls. Data integrity systems can include one or more of the methods listed above.

Data integrity is a fundamental component of information security. The need for data integrity varies based on how an organization uses data. For example, Facebook does not verify the data that a user posts in a profile. A bank or financial organization assigns a higher importance to data integrity than Facebook does. Transactions and customer accounts must be accurate. In a healthcare organization, data integrity might be a matter of life or death. Prescription information must be accurate.

Protecting data integrity is a constant challenge for most organizations. Loss of data integrity can render entire data resources unreliable or unusable.

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. The integrity check uses the snapshot to ensure data remains unchanged.


Type of Data Tested
• Files
• Email
• Pictures
Data is Converted to Binary and Summed
01001010 + ...
Checksum Calculated Before Storage or Transmission
Checksum = 1E
Data Transmitted or Stored
Checksum Calculated After Storage or Transmission
Checksum = 1E
Checksums Compared
1E = 1E
Match = Integrity Pass

A checksum is one example of a hash function. A checksum verifies the integrity of files, or strings of characters, before and after they transfer from one device to another across a local network or the Internet. Checksums simply convert each piece of information to a value and sum the total. To test the data integrity, a receiving system just repeats the process. If the two sums are equal, the data is valid. If they are not equal, a change occurred somewhere along the line.

Common hash functions include MD5, SHA-1, SHA-256, and SHA-512. These hash functions use complex mathematical algorithms. The hashed value is simply there for comparison. For example, after downloading a file, the user can verify the integrity of the file by comparing the hash values from the source with the one generated by any hash calculator.

Organizations use version control to prevent accidental changes by authorized users. Two users cannot update the same object. Objects can be files, database records, or transactions. For example, the first user to open a document has the permission to change that document; the second person has a read-only version.

Accurate backups help to maintain data integrity if data becomes corrupted. An organization needs to verify its backup process to ensure the integrity of the backup before data loss occurs.

Authorization determines who has access to an organization’s resources based on their need to know. For example, file permissions and user access controls ensure that only certain users can modify data. An administrator can set permissions for a file to read-only. As a result, a user accessing that file cannot make any changes.

The Principle of Availability

Data availability is the principle used to describe the need to maintain availability of information systems and services at all times. Cyber-attacks and system failures can prevent access to information systems and services. For example, interrupting the availability of the website of a competitor by bringing it down may provide an advantage to its rival. These denial-of-service (DoS) attacks threaten system availability and prevent legitimate users from accessing and using information systems when needed.

Methods used to ensure availability include system redundancy, system backups, increased system resiliency, equipment maintenance, up-to-date operating systems and software, and plans in place to recover quickly from unforeseen disasters.

People use various information systems in their day-to-day lives. Computers and information systems control communications, transportation and the manufacturing of products. The continuous availability of information systems is imperative to modern life. The term high availability, describes systems designed to avoid downtime. High availability ensures a level of performance for a higher than normal period. High availability systems typically include three design principles;

- Eliminate single points of failure
- Provide for reliable crossover
- Detect failures as they occur

The goal is the ability to continue to operate under extreme conditions, such as during an attack. One of the most popular high availability practices is five nines. The five nines refer to 99.999%. This means that downtime is less than 5.26 minutes per year.

Organizations can ensure availability by implementing the following:

- Equipment maintenance
- OS and system updates
- Backup testing

- Disaster planning

- New technology implementations

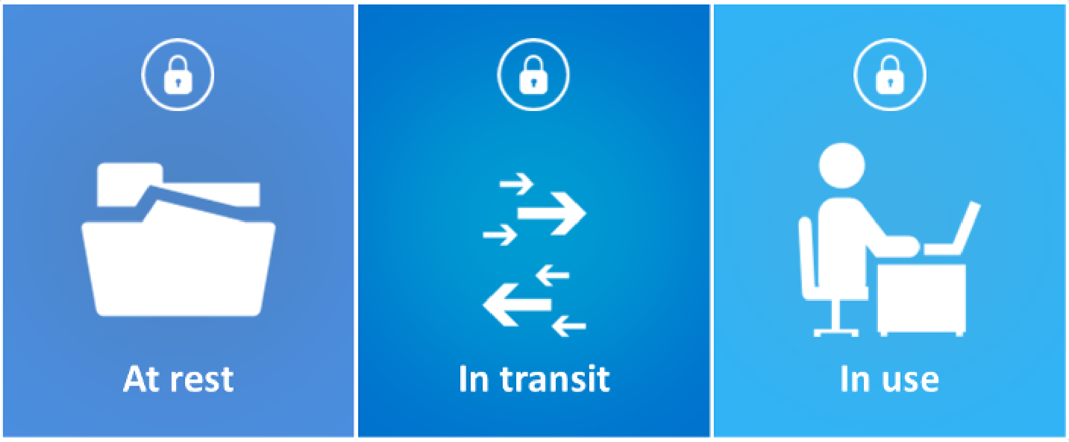
- Unusual activity monitoring

- Availability testing

States of Data

There are three states of data in Information & Communication.

1. Data at rest
2. Data in-transit
3. Data in process / Use



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. By default, systems are not set up to share 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.

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 salable, 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.

Organizations have a challenging task in trying to protect stored data. In order to improve data storage, organizations can automate and centralize data backups.

Direct-attached storage can be one of the most difficult types of data storage to manage and control. Direct-attached storage is vulnerable to malicious attacks on the local host. Stored data may also include backup data. Backups can be manual or automatic. Organizations should limit the types of data stored on direct-attached storage. In particular, an organization would not store critical data on direct-attached storage devices.

Network storage systems offer a more secure option. Network storage systems including RAID, SAN and NAS provide greater performance and redundancy. However, network storage systems are more complicated to configure and manage. They also handle more data, posing a greater risk to the organization if the device fails. The unique challenges of network storage systems include configuring, testing, and monitoring the system.

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 radio waves to transmit data

Organizations will never be able to eliminate the use of a sneaker net.

Wired networks include copper-wired and fiber optic media. Wired networks can serve a local geographical area (Local Area Network) or they can span great distances (Wide Area Networks).

Wireless networks are replacing wired networks. Wireless networks are becoming faster and able to handle more bandwidth. Wireless networks expand the number of guest users with mobile devices on small office home office (SOHO) and enterprise networks.

Both wired and wireless networks use packets or data units. The term packet refers to a unit of data that travels between an origin and a destination on the network. Standard protocols like Internet Protocol (IP) and Hypertext Transfer Protocol (HTTP) define the structure and formation of data packets. These standards are open source and are available to the public. Protecting the confidentiality, integrity, and availability of transmitted data is one of the most important responsibilities of a Security professional.

The protection of transmitted data is one of the most challenging jobs of a Security professional. With the growth in mobile and wireless devices, Security professionals are responsible for protecting massive amounts of data crossing their network on a daily basis. The Security professional must deal with several challenges in protecting this data:

- **Protecting data confidentiality** – cyber criminals can capture, save and steal data in-transit. Cyber professionals must take steps to counter these actions.

- **Protecting data integrity** – cyber criminals can intercept and alter data in-transit. Security professionals deploy data integrity systems that test the integrity and authenticity of transmitted data to counter these actions.

- **Protecting data availability** - cyber criminals can use rogue or unauthorized devices to interrupt data availability. A simple mobile device can pose as a local wireless access point and trick unsuspecting users into associating with the rogue device. The cybercriminal can hi-jack an authorized connection to a protected service or device. 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.

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. An example of data corruption during the input process includes data entry errors or disconnected, malfunctioning, or inoperable system sensors. Other examples can include mislabeling and incorrect or mismatched data formats.

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.

Data corruption also occurs during the data output process. Data output refers to outputting data to printers, electronic displays or directly to other devices. The accuracy of output data is critical because output provides information and influences decision-making. Examples of output data corruption include the incorrect use of data delimiters, incorrect communication configurations, and improperly configured printers.

Protecting against invalid data modification during processing can have an adverse impact. Software errors are the reason for many mishaps and disasters. For example, just two weeks before Christmas, some of Amazon’s third-party retailers experienced a change in the advertised price on their items to just one cent. The glitch lasted for one hour. The error resulted in thousands of shoppers getting the deal of a lifetime and the company losing revenue. In 2016, the Nest thermostat malfunctioned and left users with no heat. The Nest thermostat is a smart technology owned by Google. A software glitch left users, literally, out in the cold. A software update went wrong, forcing the device’s batteries to drain and leaving it unable to control temperature. As a result, customers were unable to heat their homes or get hot water on one of the coldest weekends of the year.

Protecting data during processing requires well-designed systems. Security professionals design policies and procedures that require testing, maintaining, and updating systems to keep them operating with the least amount of errors.

The ISO Cybersecurity Model

Security professionals need to secure information from end-to-end within the organization. This is a monumental task, and it is unreasonable to expect one individual to have all of the requisite knowledge. The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) developed a comprehensive framework to guide information security management. The ISO/IEC cybersecurity model is to cybersecurity professionals what the OSI networking model is to network engineers. Both provide a framework for understanding and approaching complex tasks.

ISO/IEC 27000 is an information security standard published in 2005 and revised in 2013. ISO publishes the ISO 27000 standards. Even though the standards are not mandatory, most countries use them as a de facto framework for implementing information security.

The ISO 27000 standards describe the implementation of a comprehensive information security management system (ISMS). An ISMS consists of all of the administrative, technical and operational controls to keep information safe within an organization. Twelve independent domains represent the components of the ISO 27000 standard. These twelve domains serve to organize, at a high level, the vast areas of information under the umbrella of information security.

The structure of the ISO cybersecurity model is different from the OSI model in that it uses domains rather than layers to describe the categories for security. The reason for this is that the ISO cybersecurity model is not a hierarchical relationship. It is a peer model in which each domain has a direct relationship with the other domains. The ISO 27000 cybersecurity model is very similar to the OSI model in that it is vital for cybersecurity specialists to understand both of these models to be successful.

The twelve domains serve as a common basis for developing organizational security standards and effective security management practices. They also help to facilitate communication between organizations.

The twelve domains consist of control objectives defined in the 27001 part of the standard. The control objectives define the high-level requirements to implement a comprehensive ISM. An organization’s management team uses the ISO 27001 control objectives to define and publish the organization’s security policies. Control objectives provide a checklist to use during security management audits. Many organizations need to pass an ISMS audit in order to earn a designation of ISO 27001 compliant.

Certification and compliance provide confidence for two organizations that need to trust each other’s confidential data and operations. Compliance and security audits prove that organizations are continuously improving their information security management system.

The ISO/IEC 27002 defines information security management system controls. Controls are more detailed than objectives. Control objectives tell the organization what to do. Controls define how to accomplish the objective.

Based on the control objective, to control access to networks by using the appropriate authentication mechanisms for users and equipment, the control would be:

Use strong passwords. A strong password consists of at least eight characters that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed. Passwords are case-sensitive, so a strong password contains letters in both uppercase and lowercase.

Cybersecurity professionals recognize the following:

- Controls are not mandatory, but they are widely accepted and adopted.

- Controls must maintain vendor-neutrality to avoid the appearance of endorsing a specific product or company.

- Controls are like guidelines. This means that there can be more than one way to comply with the objective.