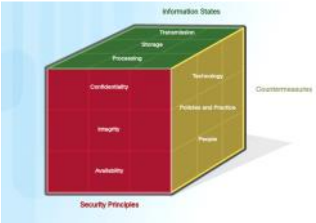
# The Cyber Security Cube

12 January 2024 18:35



John McCumber is one of the early cybersecurity experts, developing a commonly used framework called the McCumber Cube or the Cybersecurity Cube. This is used as tool when managing the protection of networks, domains and the Internet. The Cybersecurity Cube looks somewhat like a Rubik's Cube.
The first dimension of the Cybersecurity Cube includes the three principles of information security. Cybersecurity professionals refer to the three principles as the CIA Triad. The second dimension identifies the three states of information or data. The third dimension of the cube identifies the expertise required to provide protection. These are often called the three categories of cybersecurity safeguards.

## The Principles of Security

The first dimension of the cybersecurity cube identifies the goals to protect cyberspace. The goals identified in the first dimension are the foundational principles. These three principles are confidentiality, integrity and availability. The principles provide focus and enable the cybersecurity expert to prioritize actions when protecting any networked system.
Confidentiality prevents the disclosure of information to unauthorized people, resources, or processes. Integrity refers to the accuracy, consistency, and trustworthiness of data. Finally, availability ensures that information is accessible by authorized users when needed. Use the acronym CIA to remember these three principles.

Methods used to ensure confidentiality include data encryption, authentication, and access control.

## 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.

## 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. The integrity check uses the snapshot to ensure data remains unchanged.
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 (Figure 1). If they are not equal, a change occurred somewhere along the line (Figure 2).

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. Cyberattacks 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.

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 (Figure 1):

- 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. Figure 2 provides three approaches to five nines.

## Ensuring Availability

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

## The States of Data

Cyberspace is a domain containing a considerable amount of critically important data; therefore, cybersecurity experts focus on protecting data. The second dimension of the Cybersecurity Cube focuses on the problems of protecting all of the states of data in cyberspace. Data has three possible states:

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

The protection of cyberspace requires cybersecurity professionals to account for the safeguarding of data in all three states.

## Types of Data Storage

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 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.

## Challenges of Protecting Stored Data

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

## Methods of Transmitting Data

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 cybersecurity professional.

## Challenges of Protecting Data In-Transit

The protection of transmitted data is one of the most challenging jobs of a cybersecurity professional. With the growth in mobile and wireless devices, cybersecurity professionals are responsible for protecting massive amounts of data crossing their network on a daily basis. The cybersecurity 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. Cybersecurity 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 hijack 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.

## Forms of Data Processing and Computation

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.

## 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. Administrators install software-based countermeasures or safeguards on individual hosts or servers. There are several software-based technologies used to safeguard an organization's assets:

- Software firewalls 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 discover and monitor open ports on a host or server.
- Protocol analyzers, or signature analyzers, are devices that collect and examine network traffic. They identify performance problems, detect misconfigurations, identify misbehaving applications, establish baseline and normal traffic patterns, and debug communication problems.
- Vulnerability scanners are computer programs designed to assess weaknesses on computers or networks.
- Host-based intrusion detection systems (IDS) examine activity on host systems only. An IDS generates log files and alarm messages when it detects unusual activity. A system storing sensitive data or providing critical services is a candidate for host-based IDS.

## Hardware-based Technology Safeguards

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

- Firewall appliances block unwanted traffic. Firewalls contain rules that define the traffic allowed into and out of a network.
- Dedicated Intrusion Detection Systems (IDS) detect signs of attacks or unusual traffic on a network and send an alert.
- Intrusion Prevention Systems (IPS) detect signs of attacks or unusual traffic on a network, generate an alert and take corrective actions.
- Content filtering services control access and transmission of objectionable or offensive content.

## Network-based Technology Safeguards

There are several network-based technologies used to protect the organization's assets:

- **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.

## Cloud-based Technology Safeguards

Cloud-based technologies shift the technology component from the organization to the cloud provider. 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 have extended these options to include IT as a Service (ITaaS), which provides IT support for IaaS, PaaS, and SaaS service models. In the ITaaS model, an organization contracts with the Cloud provider for individual or bundled services.

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 Safeguards

The third dimension of the Cybersecurity Cube defines the skills and discipline a cybersecurity professional can call upon to protect cyberspace. Cybersecurity professionals must use a range of different skills and disciplines available to them when protecting the data in the cyberspace. They must do this while remaining on the 'right side' of the law.

The Cybersecurity Cube identifies the three types of skills and disciplines used to provide protection. The first skill includes the technologies, devices, and products available to protect information systems and fend off cyber criminals. Cybersecurity professionals have a reputation for mastering the technological tools at their disposal. However, McCumber reminds them that the technological tools are not enough to defeat cyber criminals. Cybersecurity professionals must also build a strong defense by establishing policies, procedures, and guidelines that enable the users of cyberspace to stay safe and follow good practices. Finally, users of cyberspace must strive to become more knowledgeable about the threats of the cyberspace and establish a culture of learning and awareness.

a security policy typically includes:

- **Identification and authentication policies -** Specifies authorized persons that can have access to network resources and outlines verification procedures.
- **Password policies -** Ensures passwords meet minimum requirements and are changed regularly.
- **Acceptable use policies -** Identifies network resources and usage that are acceptable to the organization. It may also identify ramifications for policy violations.
- **Remote access policies -** Identifies how remote users can access a network and what is remotely accessible.
- **Network maintenance policies -** Specifies network device operating systems and end user application update procedures.
- **Incident handling policies -** Describes how security incidents are 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. The AUP should be as explicit as possible to avoid misunderstanding. For example, an AUP lists specific websites, newsgroups, or bandwidth intensive applications that users cannot access using company computers or the company network.

## Standards

Standards help an IT staff maintain consistency in operating the network. Standards documents provide the technologies that specific users or programs need in addition to any program requirements or criteria that an organization must follow. This helps IT staff improve efficiency and simplicity in design, maintenance, and troubleshooting.

One of the most important security principles is consistency. For this reason, it is necessary for organizations to establish standards. Each organization develops standards to support its unique operating environment. For example, an organization establishes a password policy. The standard is that passwords require a minimum of eight upper and lowercase alphanumeric characters, including at least one special character. A user must change a password every 30 days, and a password history of 12 previous passwords ensures that the user creates unique passwords for one year.

There are three types of sensitive information:

- Personal information is personally identifiable information (PII) that traces back to an individual. Figure 2 lists this category of data.
- Business information is information that includes anything that poses a risk to the organization if discovered by the public or a competitor. Figure 3 lists this category of data.
- Classified information is information belonging to a government body classified by its level of sensitivity. Figure 4 lists this category of data.

## 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. These services provide the primary framework to control access.

The first "A" in AAA represents authentication. ***Authentication*** verifies the identity of a user to prevent unauthorized access. Users prove their identity with a username or ID. In addition, users need to verify their identity by providing one of the following as shown in Figure 1:

- Something they know (such as a password)
- Something they have (such as a token or card)
- Something they are (such a fingerprint)

For example, if you go to an ATM for cash, you need your bankcard (something you have) and you need to know the PIN. This is also an example of multifactor authentication. Multifactor authentication requires more than one type of authentication. The most popular form of authentication is the use of passwords.

***Authorization*** services determine which resources users can access, along with the operations that users can perform, as shown in Figure 2. Some systems accomplish this by using an access control list, or an ACL. An ACL determines whether a user has certain access privileges once the user authenticates. Just because you can log onto the corporate network does not mean that you have permission to use the high-speed color printer. Authorization can also control when a user has access to a specific resource. For example, employees may have access to a sales database during work hours, but the system locks them out after hours.

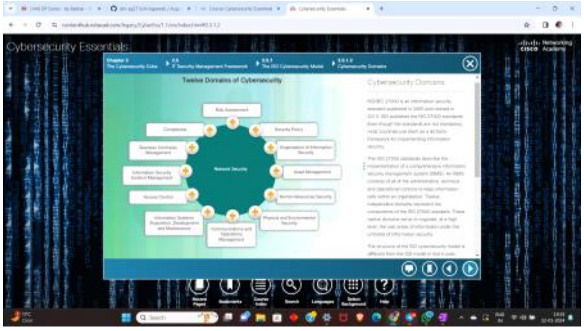
***Accounting*** keeps track of what users do, including what they access, the amount of time they access resources, and any changes made. For example, a bank keeps track of each customer account. An audit of that system can

reveal the time and amount of all transactions and the employee or system that executed the transactions.
Cybersecurity accounting services work the same way. The system tracks each data transaction and provides auditing results. An administrator can set up computer policies as shown in Figure 3 to enable system auditing.
The concept of AAA is similar to using a credit card, as indicated by Figure 4. The credit card identifies who can use it, how much that user can spend, and accounts for items or services the user purchased.
Cybersecurity accounting tracks and monitors in real time. Websites, like Norse, show attacks in real-time based on data collected as part of an accounting or tracking system.

## Overview of the 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.
Click each domain in the figure for a brief description.
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.


Cybersecurity Essentials
Networking Academy
Twelve Domains of Cybersecurity
Risk Assessment
Security Policy
Organization of Information Security
Asset Management
Human Resources Security
Physical and Environmental Security
Communications and Operations Management
Information Systems Acquisition, Development and Maintenance
Access Control
Information Security Incident Management
Business Continuity Management
Compliance
Network Security
Cybersecurity Domains

## Control Objectives

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 following is an example of a control objective:
*To control access to networks by using the appropriate authentication mechanisms for users and equipment.*

## Controls

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.

## The ISO Cybersecurity Model and the CIA Triad

The ISO 27000 is a universal framework for every type of organization. In order to use the framework effectively, an organization must narrow down which domains, control objectives, and controls apply to its environment and operations.
The ISO 27001 control objectives serve as a checklist. The first step an organization takes is to determine if these control objectives are applicable to the organization. Most organizations generate a document called the Statement of Applicability (SOA). The SOA defines which control objectives that the organization needs to use.
Different organizations place greater priority on confidentiality, integrity, and availability depending on the type of industry. For example, Google places the highest value on user data confidentiality and availability and less on integrity. Google does not verify user data. Amazon places high emphasis on availability. If the site is not available, Amazon does not make the sale. This does not mean that Amazon ignores confidentiality in favor of availability. Amazon just places a higher priority on availability. Therefore, Amazon may spend more resources ensuring that there are more servers available to handle customer purchases.
An organization tailors its use of the available control objectives and controls to best meet its priorities with regard to confidentiality, integrity and availability.

## The ISO Cybersecurity Model and the States of Data

Different groups within an organization may be responsible for data in each of the various states. For example, the network security group is responsible for data during transmission. Programmers and data entry people are responsible for data during processing. The hardware and server support specialists are responsible for stored data. The ISO Controls specifically address security objectives for data in each of the three states.

## 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.