Chapter 1: Today’s Security Professional

# Cybersecurity Objectives

Cybersecurity has 3 complementary objectives (CIA Triad):

* Confidentiality: Ensures that unauthorized individuals are not able to gain access to sensitive information. Ex. Firewalls, access control lists, and encryptions
* Integrity: Ensures that there are no unauthorized modifications to information or systems, either intentionally or unintentionally. Ex. Hashing and integrity monitoring
* Availability: Ensures that information and systems are ready to meet the needs of legitimate users at the time those users request them. Ex. Fault tolerance, clustering, and backups

**Nonrepudiation:** Someone performing an action cannot deny it later after doing the action. Ex digital footprint.

Nonrepudiation is not part of the CIA Triad but is still very important and is considered an objective.

# Data Breach Risks

Security incidents happen when an organization has a breach. This can be from malicious activity, accident, or from nature.

# DAD Triad

DAD Triad explains the 3 key threats to cybersecurity efforts:

* Disclosure: Is the exposure of data to unauthorized individuals (also known as data loss). This can lead to data exfiltration (the unauthorized transfer of data from a secure system to an external destination). Violates the Confidentiality principle.
* Alteration: Is the unauthorized modification of information and is a violation of the principle of integrity.
* Denial: Is the Disruption of an authorized user’s legitimate access to information and violates the principle of availability.

# Breach Impact

## Financial Risk

Risk of monetary damage.

## Reputation Risk

Risk of negative publicity from customers, employees, suppliers, and other stakeholders.

## Strategic Risk

Risk of becoming less effective to meet goals and objectives.

## Operational Risk

Risk an organization’s ability to carry out day-to-day functions.

## Compliance Risk

Risk of an organization runs into legal or regulatory requirements (legal issues, gets sued in court)

# Implementing Security Controls

Security controls are specific measures that fulfill the security objectives of an organization.

## Gap Analysis

Evaluates security controls. During Gap Analysis control objectives of an organization, system, or service are reviewed and then examine the controls designed to achieve those objectives. If there are any cases where the controls do not meet the control objective that is a gap. Gaps should be considered as potential risks and remediated as time and resources permit.

## Security Control Categories

Security controls are categorized based on their mechanism of action:

* Technical controls: Enforces Confidentiality, integrity and availability in the digital space. Ex. Firewall rules, access control lists, intrusion prevention systems, and encryption.
* Operational controls: Include the process that we put in place to manage technology in a secure manner. Includes user access reviews, log monitoring, and vulnerability management.
* Managerial Controls: Are procedural mechanisms that focus on the mechanics of the risk management process. Ex. Periodic risk assessments, security planning exercises, and incorporation of security into organization’s change management, service acquisition, and project management practice.
* Physical Controls: Impact from the outside world. Ex. Fences, locks, fire suppression systems, alarms, etc.

## Security Control Types

* Preventative Controls: Stop issues before they happen. Ex. Firewalls, encryption, etc.
* Deterrent Controls: Prevent attackers from breaching security policies. Ex. Fences, guard dogs, etc.
* Detective Controls: Identify security events that have already happened. Ex. Intrusion detective systems.
* Corrective Controls: Remediating issues that have already happened. Ex. Restoring backups.
* Compensating Controls: Mitigate risks associated with exceptions made to a security policy.
* Directive Controls: Inform employees and others what to do to achieve security objectives.

# Data Protection

3 states where data might exist:

* Data at Rest: Data stored on a hard drive.
* Data in Transit: Data in Transit over a network.
* Data in Use: Data actively being used on a computer system.

## Data Encryption

The use of math algorithms to protect information from prying eyes in rest and transit.

## Data Loss Prevention (DLP)

DLP Systems help organizations enforce information handling policies and procedures to prevent data loss and theft.

DLP has 2 different environments:

* Agent-Based DLP: uses software installed on systems that search those systems for the presence of sensitive information.
* Agentless-Based DLP: Systems are dedicated devices that sit on the network and monitor outbound network traffic, watching for any transmissions that contain unencrypted sensitive information.

DLP systems have 2 mechanisms:

* Pattern Matching: Where they watch for the telltale signs of sensitive information.
* Watermarking: Where systems or administrators apply electronic tags to sensitive documents and then the DLP system can monitor the systems and network for unencrypted content containing those tags.

## Data Minimization

Techniques seek to reduce risk by reducing the amount of sensitive information that we maintain on a regular basis. The best way to do it is to destroy data when it is no longer needed.

If data can’t be destroyed the next best thing is to **deidentify** the data (deidentification process removes the ability to link data back to an individual, reducing its sensitivity).

An alternative to deidentification process is **obfuscation** (transforming data into a format where the original information can’t be retrieved).

* Hashing: Uses hash functions to transform a value in our dataset to a corresponding hash value.
* Tokenization: Replaces sensitive values with a unique identifier using a lookup table.
* Masking: Partially redacts sensitive information by replacing some or all sensitive fields with blank characters.

**Rainbow table attack:** is an attack where the attacker computes the hashes of those candidate values and then checks to see if those hashes exist in our data file. This only works if the attacker has a list of possible values for a field.

## Access Restrictions

Security measures that limit the ability of individuals or systems to access sensitive information or resources.

2 types:

* Geographical Restriction: limits access based on physical location
* Permission Restriction: limits access based on user’s role or level of authorization

## Segmentation and Isolation

Segmentation: Puts sensitive systems on separate networks where they may communicate with each other but have strict restrictions on their ability to communicate with systems on the network.

Isolation: Cuts a system off from access to or from outside networks.