Today's Security Professional

Cyber Security Objectives

Usually called the CIA Triad

Confidentiality

Ensures that unauthorized individuals are not able to gain access to sensitive information

Integrity

Ensures that there are no unauthorized modifications to information or systems, either intentionally or unintentionally

Availability

Ensures that information and systems are ready to meet the needs of legitimate users at the time those users request them

Data Breach Risks

Security incidents occur when an organization experiences a breach of the confidentiality, integrity, and/or availability of information or information systems

The DAD triad is a model that explains the 3 threats to cyber security efforts

Disclosure

It is the exposure of sensitive information to unauthorized individuals, otherwise known as data loss

It is a violation of the principle of confidentiality

Alteration

It is the unauthorized modification of information

It is violation of the principle of integrity

Denial

It is the unintended disruption of an authorized user's legitimate access to information

Denial events violate the principle of availability

Breach Impact

In most cases a risk will cross multiple risk categories.

The impacts of a security incident may be wide-ranging, depending upon the nature of the incident and the type of organization affected.

Financial Risk

It is the risk of monetary damage to the organization as the result of a data breach and it can be direct or indirect.

Reputational Risk

It is the negative publicity surrounding a security breach causes the loss of goodwill among customers, employees, suppliers, and other stakeholders.

Strategic Risk

It is the risk that an organization will become less effective in meeting its major goals and objectives as a result of the breach.

Operational Risk

It is the risk related to an organization's ability to carry out its day-to-day functions

Compliance Risk

It is when a security breach causes an organization to run afoul of legal or regulatory requirements.

Identity Theft
It's the most common impact on the stakeholders related to a breach by the exposure of personally identifiable information (PII) to unscrupulous individuals.

Implementing Security Controls

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

Organizations should select a set of security controls that meets their control objectives based on the criteria and parameters that they either select for their environment or have imposed on them by outside regulators.

Many control objectives require a combination of technical, operational, and management controls.

Security Control Categories

Technical Controls

Enforce confidentiality, integrity, and availability in the digital space.

Examples: Firewall Rules, Access Control Lists, etc..

Operational Controls

Include the processes that we put in place to manage technology in a secure manner.

Examples: Log Monitoring, Vulnerability Management, etc..

Managerial Controls

Procedural mechanisms that focus on the mechanics of the risk management process.

Example: Periodic Risk Assements, Project Management Practices, etc..

These control categories and types are unique to CompTIA.

Security Control Types

Preventive controls

Intend to stop a security issue before it occurs.
Example: Firewall and Encryption

Detective controls

Identify security events that have already occurred.
Example: Intrusion detection systems

Corrective controls

Remediate security issues that have already occurred.
Example: Restoring backups

Deterrent controls

Seek to prevent an attacker from attempting to violate security policies.
Example: Guard Dogs

Physical controls

Security controls that impact the physical world.
Example: Locks

Compensating controls

Controls designed to mitigate the risk associated with exceptions made to a security policy

Data Protection

3 Types of Data

Data at rest

Stored data that resides on hard drives, tapes, in the cloud, or on other storage media.

Data in motion

Data that is in transit over a network.

Data in processing

Data that is actively in use by a computer system.

Data Loss Prevention (DLP)

Encryption technology uses mathematical algorithms to protect information

Encrypted data is unintelligible to anyone who does not have access to the appropriate decryption key

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

They can act quickly to block the transmission before damage is done and alert administrators to the attempted breach.

2 Different Environments

Host-based DLP

Uses software agents installed on systems that search those systems for the presence of sensitive information.

Host-based DLP can also monitor system configuration and user actions, blocking undesirable actions. (i.e. blocking users from accessing USB-based removable media devices)

Network DLP

Systems are dedicated devices that sit on the network and monitor outbound network traffic, watching for any transmissions that contain unencrypted sensitive information.

They can then block those transmissions

DLP systems may simply block traffic that violates the organization's policy, or in some cases, they may automatically apply encryption to the content.

2 Mechanisms of Action

Pattern matching, where they watch for the telltale signs of sensitive information (i.e, Number that is formatted like a credit card or Social Security number)

Watermarking, where systems or administrators apply electronic tags to sensitive documents and then the DLP system can monitor systems and networks for unencrypted content containing those tags.

Data Minimization

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 achieve data minimization is to simply destroy data when it is no longer necessary to meet our original business purpose.

If the data can't be removed then transform it into a format where the original sensitive information is de-identified.

The de-identification process removes the ability to link data back to an individual, reducing its sensitivity.

An alternative is data obfuscation which is converting the data into a format that can't be retrieved

Hashing

Uses a hash function 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.