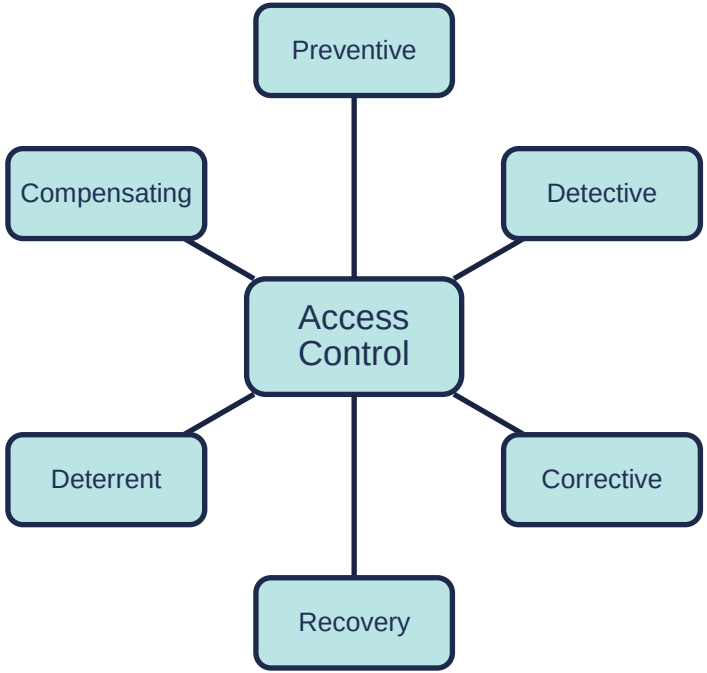
Access Control

Access Control Basics

- Access control protects against a wide variety of threats:
  - Unauthorized Access
  - Unapproved Modification of Data
  - Lack of Data Confidentiality
- CIA triad is the cornerstone of cyber security and access control.

Access Control Categories & Types



Access Control Categories & Types

Preventative Controls prevent actions.

- Background check before approving a tenant ensures a qualified tenant.
- Drug test before employment prevents the hiring of employees that use illegal drugs.

Detective Controls send alerts during or after an attack.

- Building alarm triggered during a break-in.
- Network intrusion detection system (IDS) alerting network administrators of an attack.

Access Control Categories & Types

Corrective Controls "correct" a damaged system or process.

- Anti-virus can quarantine and delete malicious software from a computer system.
- Intrusion prevention system (IPS) can stop a network attack by blocking it.

Recovery Controls are needed to restore functionality.

- Restoring corrupted data with a data backup.
- A secondary office site can restore business functionality after a natural disaster to the business's primary site.

Access Control Categories & Types

Deterrent Controls deter users from performing actions.

- Security guards.
- A “beware of dog” sign.
- A fence around your building.

Compensating Controls add additional security.

- Defense In Depth
- Multiple Layers of Security

Physical & Logical Access Control

- **Physical** security includes implementing different access control methods with technology you can touch.
  - Physically locking down the equipment and securing the building.

- **Logical** security methods include those elements that are implemented through technological means.
  - Password policies, logical access control lists, etc.

Common Physical Access Controls

- Employee ID Badges
- Physical Access Logs
- Door Access Systems
- Proximity Cards
- Mantraps
- Hardware Locks
- Video Surveillance
- Security Guards
- Building Alarms
- Fences

Common Logical Access Controls

- Access Control Lists
- Windows Group Policies
- Password Policies
- Account Policies
- Device Policies

Physical and Logical Access Controls

INSTRUCTOR
ALTON

Physical Security Methods

- **Hardware Locks**
- **ID Badges** are commonly used to provide visual confirmation that someone is authorized.
- **Physical Access Logs & Lists** can be used to verify exactly when someone enters or exits.
- **Door Access Systems** are ones that only open after some access control mechanisms is used. This includes cipher locks and proximity cards.

INSTRUCTOR
ALTON

Physical Security Methods

- **Proximity Cards** are credit card-sized access cards that only need to be waved or placed in close proximity to a card reader.
- **Security Guards** deter would-be intruders and verify access.
- **Mantrap** is a physical mechanism designed to control access to a secure area from a non-secure area through the use of a buffer zone. Mantraps are commonly used to prevent the social engineering tactic known as tailgating or piggybacking.
- **Video Cameras**

Logical Security Methods

- **Access Control Lists (ACLs)**
  - Used to specifically identify what is allowed and what is not allowed.
  - An ACL can define what is allowed based on permissions or based on traffic.
  - ACLs typically operate using an implicit deny policy.

- **Password Policies**
  - Maximum Password Age
  - Minimum Password Age
  - Enforce Password History
  - Minimum Password Length
  - Password Complexity Requirements

Logical Security Methods

- **Device Policy**
  - Disable Autorun
  - Prevent the installation of small devices (USB flash drive, MP3 player, etc.)
  - Detect the use of small devices.

- **Accounts**
  - Centralized Over Decentralized
  - Time-of-day Restrictions
  - Account Expiration

Access Control Models

Access Control Models

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role & Rule Based Access Control (RBAC)

Subjects Access Objects

- **Subjects**
  - Users and groups of users that access an object.
- **Objects**
  - Objects are things such as files, folders, network shares, printers, applications, etc.

Mandatory Access Control (MAC)

- The strictest of all access control models
- Designed to be used by the Government
- Military makes wide use of MAC
- Both subjects and objects are given "sensitivity" labels.
- When labels match, the appropriate permissions is granted.

Discretionary Access Control (DAC)

- Every object has an owner.
- The object's owner decides who gets access.
- Most operating systems follow this model.

Role & Rule Based Access Control (RBAC)

- **Role-Based**
  - Uses roles to manage user permissions.
  - Example: Accounting department has access to QuickBooks Software.
- **Rule-Based**
  - Uses rules to define when users should be granted access.
  - Designed to complement role-based access control.