Overview of Security Risks

- **Importance**: Understanding that security risks are diverse and attackers constantly seek ways to gain unauthorized access to systems.
- **Scope**: Protection extends beyond data to include physical systems, buildings, people, and the entire organization.

Categories of Security Controls

1. **Technical Controls**
   - **Definition**: Implemented through technical systems.
   - **Examples**:
     - Operating system policies (allow/disallow functions).
     - Firewalls, antivirus software.
   - **Role**: Create technical safeguards against unauthorized access.
2. **Managerial Controls**
   - **Definition**: Policies and procedures guiding the management of IT security.
   - **Examples**:
     - Security policy documentation.
     - Best practices for data management.
   - **Role**: Provide a framework for operationalizing security measures.
3. **Operational Controls**
   - **Definition**: Involve human actions to enforce security.
   - **Examples**:
     - Security guards, training sessions, awareness programs.
   - **Role**: Engage personnel in maintaining security protocols.
4. **Physical Controls**
   - **Definition**: Limit physical access to buildings, rooms, or devices.
   - **Examples**:
     - Guard shacks, fences, badge readers.
   - **Role**: Prevent unauthorized physical entry into secure areas.

Types of Security Controls

1. **Preventive Controls**
   - **Definition**: Aim to prevent security incidents before they occur.

- **Examples**:
  - Firewall rules, guard shacks.
- **Classification**:
  - Technical: Firewall rules.
  - Managerial: Onboarding policies.
  - Operational: Guard shack operations.
  - Physical: Door locks.

2. **Deterrent Controls**
   - **Definition**: Discourage potential attackers from attempting unauthorized access.
   - **Examples**:
     - Splash screens with security messages, disciplinary threats.
   - **Classification**:
     - Technical: Splash screens.
     - Managerial: Demotion warnings.
     - Operational: Reception desk.
     - Physical: Warning signs.
3. **Detective Controls**
   - **Definition**: Identify and log security breaches.
   - **Examples**:
     - Reviewing system logs, patrolling premises, motion detectors.
   - **Classification**:
     - Technical: System logs.
     - Managerial: Log-in report reviews.
     - Operational: Property patrols.
     - Physical: Motion detectors.
4. **Corrective Controls**
   - **Definition**: Respond to incidents after detection to minimize impact.
   - **Examples**:
     - Restoring from backups, reporting policies.
   - **Classification**:
     - Technical: Backup recovery.
     - Managerial: Reporting issue policies.
     - Operational: Contacting authorities.
     - Physical: Fire extinguishers.
5. **Compensating Controls**
   - **Definition**: Temporary measures used until a permanent solution is in place.
   - **Examples**:

        - Blocking traffic, separating duties.
    - **Classification**:
        - Technical: Firewall rules as temporary fixes.
        - Managerial: Separation of duties.
        - Operational: Multiple security staff.
        - Physical: Generators during power outages.
6. **Directive Controls**
    - **Definition**: Direct users to follow security practices rather than enforcing them.
    - **Examples**:
        - Compliance training, signage.
    - **Classification**:
        - Technical: File storage policies.
        - Managerial: Compliance policies.
        - Operational: Security training.
        - Physical: Authorized personnel signs.

Detailed Notes on the CIA Triad in IT Security

Overview

- **CIA Triad**: Stands for **Confidentiality, Integrity, and Availability**. It represents the core principles of IT security.
- Sometimes referred to as the **AIC Triad** to avoid confusion with the US Central Intelligence Agency.
- **Purpose**: To provide a foundational framework for securing systems and information in IT environments.

Components of the CIA Triad

1. **Confidentiality**
    - **Definition**: Ensuring that sensitive information is not accessed by unauthorized individuals.
    - **Techniques**:
        - **Encryption**: Scrambles data so only authorized parties can decode it.
        - **Access Controls**: Limits the access to information based on roles, e.g., marketing staff can access marketing documents but not accounting data.

        - **Multi-Factor Authentication (MFA)**: Adds extra layers of security, requiring more than just a password to gain access, increasing confidentiality.
    - **Examples**:
        - Encrypted data remains unreadable to anyone without the proper key.
        - Limiting access to sensitive information based on user roles.
        - Authentication mechanisms to verify user identity.
2. **Integrity**
    - **Definition**: Ensuring the data received is exactly the same as the data sent, without any unauthorized alterations.
    - **Techniques**:
        - **Hashing**: A mathematical function that creates a unique value (hash) from the original data. The sender sends the hash with the data. The receiver verifies it by generating a hash and comparing.
        - **Digital Signatures**: Uses asymmetric encryption to validate the sender and ensure the integrity of the message.
        - **Certificates**: Used to confirm the identity of devices or users and ensure data is not tampered with.
        - **Nonrepudiation**: Provides proof that the sender sent the data and ensures they cannot deny sending it.
    - **Examples**:
        - Verifying data integrity using hashes.
        - Using digital signatures for added security and authenticity.
        - Certificates ensuring secure device-to-device communication.
3. **Availability**
    - **Definition**: Ensuring that systems and data are accessible to authorized users when needed.
    - **Techniques**:
        - **Fault Tolerance**: Having backup systems or components that take over in case one component fails, ensuring continuous operation.
        - **System Patching and Updates**: Regular maintenance, such as applying patches, ensures that systems remain secure and operational, preventing downtime from attacks.
    - **Examples**:
        - Systems with built-in redundancy that maintain operations even during component failure.
        - Regular updates and patches to fix vulnerabilities that could lead to downtime or data breaches.

Importance

- **Confidentiality** protects against unauthorized access.
- **Integrity** ensures that data remains accurate and unchanged.
- **Availability** guarantees that users can access the systems and data they need, even during technical failures.

Table: CIA Triad Summary

Component	Definition	Key Techniques	Examples	
Confidentiality	Protecting information from unauthorized access.	- Encryption - Access Control - Multi-Factor Authentication (MFA)	- Encrypted communication - Role-based access - MFA for logging into sensitive systems	
Integrity	Ensuring data remains unchanged and accurate.	- Hashing - Digital Signatures - Certificates - Nonrepudiation	- Verifying data with hashes - Signed emails to ensure authenticity - Device certificates	
Availability	Ensuring systems and data are available when needed.	- Fault Tolerance - System Patching and Updates	- Redundant systems for continuity - Regular security patching to avoid exploits	