Introduction to Security Controls

Understanding the Foundations of Cybersecurity

Brendan Shea, PhD

March 11, 2025

Lecture Overview: Security Controls

- In this lecture, we will explore the fundamental concepts of **security controls** in cybersecurity.
- We will examine four major **categories** of controls: Technical, Managerial, Operational, and Physical.
- You will learn about six different **types** of controls: Preventive, Deterrent, Detective, Corrective, Compensating, and Directive.
- We will analyze real-world examples of how these controls work together to create effective security systems.

Learning Objectives

By the end of this lecture, you will understand how to identify, classify, and evaluate different security controls.

What is Information Security?

- **Information Security** is the practice of protecting information by mitigating risks and threats.
- The goal is to protect the **CIA triad**:
  - **Confidentiality**: Keeping information private
  - **Integrity**: Ensuring information hasn't been altered
  - **Availability**: Making information accessible when needed
- Information can be digital, physical, or knowledge-based.

Core Concept

Information security protects all forms of information throughout their entire lifecycle.

Understanding Security Terms

- A **threat** is any potential danger that could harm an asset or organization.
- A **vulnerability** is a weakness that could be exploited by a threat.
- An **exploit** is a specific way to take advantage of a vulnerability.
- A **risk** is the potential for loss or damage when a threat exploits a vulnerability.

Example Scenario

- Threat: A hacker
- Vulnerability: Weak password
- Exploit: Password guessing program
- Risk: Unauthorized account access

Types of Security Risks

Risk Category	Examples
Physical	Fire, theft, natural disasters
Technical	Malware, hacking, system failures
Human	User errors, social engineering
Organizational	Process failures, policy gaps

Understanding Impact

Risks can affect:

- Data confidentiality
- System integrity
- Service availability
- Organizational reputation

What is a Security Control?

- A **security control** is any measure designed to protect our systems, data, and resources from threats.
- Security controls work like the different security features in your home, such as locks, alarms, and security cameras.
- These measures can be physical objects, technical solutions, or rules and procedures that people follow.
- The goal of security controls is to **reduce risk** by protecting against threats, detecting problems, and helping us respond to security incidents.

Key Point

Security controls are the building blocks of a strong security program!

Why Do We Need Security Controls?

- Organizations need to protect valuable **assets**, which include data, systems, and physical resources from unauthorized access or damage.
- Security controls help manage and reduce **risks**, which are potential threats that could harm our systems or expose sensitive information.
- Many organizations must follow specific **compliance requirements** that mandate certain security measures to protect user privacy and data.
- Without proper security controls, organizations are vulnerable to various attacks that could result in financial losses, reputation damage, or legal consequences.

Overview of Security Control Categories

- Security controls can be divided into four main **categories**, each serving different aspects of an organization's security needs.
- **Technical controls** use technology to protect systems and data, such as firewalls and encryption.
- **Managerial controls** focus on security decisions and oversight, including policies and risk assessments.
- **Operational controls** and **physical controls** involve day-to-day procedures and tangible security measures.

Real World Example

A school's security system uses all four categories working together:

- Technical: Computer passwords
- Managerial: Security policies
- Operational: Security training
- Physical: Door locks

Technical Controls: Introduction

- **Technical controls** are security measures that are implemented and executed by computer systems and software.
- These controls form the technological foundation of modern cybersecurity practices.
- Technical controls operate with minimal human intervention once properly configured.
- They provide consistent and automated protection against many common security threats.

Key Characteristics

Automated, technology-based, and system-enforced protections

Technical Controls: Common Examples

- **Authentication systems** verify user identities through passwords, biometrics, or security tokens.
- **Encryption** protects data by converting it into a format that can only be read with the correct key.
- **Firewalls** monitor and control incoming and outgoing network traffic based on security rules.
- **Antivirus software** detects, prevents, and removes malicious software from computer systems.

Critical Point

Technical controls must be regularly updated to remain effective against new threats!

Technical Controls: Implementation

- Technical controls should be implemented in **layers** to provide defense in depth against various threats.
- Each technical control must be properly **configured** to match the organization's security requirements.
- Regular **maintenance** and updates are essential to ensure controls remain effective over time.
- Organizations should maintain **documentation** of all technical controls and their configurations.

Implementation Example

A laptop's security might include:

- Login password
- Disk encryption
- Firewall
- Antivirus

Technical Controls: Advantages and Limitations

Advantages

- Consistent operation
- Automated responses
- Scalable protection
- Measurable effectiveness

Limitations

- Initial setup costs
- Regular updates needed
- Technical expertise required
- Can be circumvented

Balance

Technical controls must be balanced with other control types for effective security.

Managerial Controls: Introduction

- **Managerial controls** are administrative measures that guide the implementation of security practices.
- These controls focus on managing risks and making decisions about security strategies.
- Managerial controls establish the framework for all other security controls within an organization.
- They require active involvement from leadership to ensure effective implementation.

Essential Role

Managerial controls provide direction and oversight for the entire security program.

Managerial Controls: Key Components

- **Security policies** establish the rules and guidelines that govern how an organization protects its assets.
- **Risk assessments** help identify potential threats and vulnerabilities to organizational resources.
- **Compliance programs** ensure the organization meets all relevant legal and regulatory requirements.
- **Resource allocation** determines how to distribute security resources effectively.

Policy Development
Risk Management
Resource Planning

Managerial Controls: Documentation

- Every organization should maintain comprehensive **security documentation** that outlines all policies and procedures.
- Documentation must be regularly **reviewed and updated** to reflect changes in the threat landscape.
- Security policies should clearly define **roles and responsibilities** for all members of the organization.
- Written procedures must provide clear guidance for implementing security measures.

Documentation Requirements

All security policies must be:

- Clear and understandable
- Regularly updated
- Easily accessible
- Formally approved

Managerial Controls: Decision Making

- Effective security management requires balancing **security needs** with business operations and resources.
- Managers must evaluate the **cost-effectiveness** of different security measures before implementation.
- Security decisions should be based on thorough **risk analysis** rather than reactive responses to incidents.
- Organizations need clear procedures for **escalating** security issues to appropriate decision-makers.

Decision Framework

When evaluating new security measures, consider:

- Risk level
- Implementation cost
- Operational impact
- Resource requirements

Operational Controls: Introduction

- **Operational controls** are the security procedures and tasks performed by people rather than automated systems.
- These controls focus on day-to-day activities that maintain and protect organizational security.
- Operational controls require consistent human execution and oversight to be effective.
- They bridge the gap between managerial policies and technical implementations.

Key Characteristic

Operational controls depend on people following established procedures correctly and consistently.

Operational Controls: Security Awareness

- **Security awareness training** educates employees about their role in maintaining organizational security.
- Regular training sessions ensure staff understand current threats and appropriate security responses.
- Employees must learn to recognize and report potential **security incidents** promptly.
- Training programs should include practical exercises and real-world examples.

Training Topics

Essential security awareness areas include:

- Password management
- Email security
- Social engineering
- Incident reporting

Operational Controls: Daily Procedures

Regular Tasks

- System monitoring
- Backup verification
- Log reviews
- Security updates

Periodic Tasks

- Security audits
- Access reviews
- Policy updates
- Disaster drills

Critical Point

Consistent execution of operational procedures is essential for maintaining security.

Operational Controls: Incident Response

- Organizations must maintain detailed **incident response procedures** for handling security breaches.
- Staff should be trained to recognize and properly report potential security incidents.
- **Response teams** need clear procedures for investigating and containing security threats.
- Regular practice drills help ensure effective response during actual security incidents.

Incident Response Steps

1. Identification
2. Containment
3. Eradication
4. Recovery

Physical Controls: Introduction

- **Physical controls** are tangible security measures that protect facilities, equipment, and resources.
- These controls create barriers between protected assets and potential threats.
- Physical controls often work in conjunction with technical and operational controls.
- They form the first line of defense against unauthorized physical access.

Remember

The strongest technical controls can be defeated by weak physical security!

Physical Controls: Access Control

- **Access control systems** manage and monitor entry to protected areas within a facility.
- Organizations must establish clear procedures for issuing and revoking physical access credentials.
- Different areas may require different levels of **access restriction** based on security needs.
- Physical access controls should maintain detailed logs of all entry and exit activities.

Common Access Controls

- ID badges
- Key cards
- Biometric scanners
- Security guards

Physical Controls: Environmental Protection

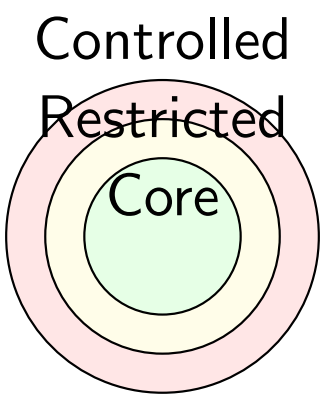
- Physical controls must protect against both human threats and **environmental hazards**.
- Critical systems require protection from fire, water damage, and power fluctuations.
- Environmental monitoring systems should track temperature, humidity, and other relevant conditions.
- Backup power systems must maintain essential security controls during power outages.

Environmental Systems

Fire Suppression	Temperature Control
Water Detection	Humidity Monitoring
Power Backup	Emergency Lighting

Physical Controls: Security Zones

- Organizations should implement **layered security zones** with increasing protection levels.
- Each security zone must have clearly defined boundaries and access requirements.
- Sensitive areas require multiple physical controls working together for adequate protection.
- Regular security assessments should verify the effectiveness of zone protections.



Types of Security Controls

- Security controls can be classified into six **functional types** based on their purpose.
- Each type of control serves a specific role in the overall security strategy.
- Organizations typically need multiple types of controls working together.
- The effectiveness of controls depends on choosing the right type for each security need.

Control Types

1. Preventive
2. Deterrent
3. Detective
4. Corrective
5. Compensating
6. Directive

Preventive Controls: Introduction

- **Preventive controls** are designed to stop security incidents before they occur.
- These controls create barriers that block unauthorized actions and access attempts.
- Preventive controls are the first line of defense in a security strategy.
- They work by eliminating vulnerabilities or blocking threat vectors.

Key Principle

It is generally more effective to prevent security incidents than to detect and respond to them after they occur.

Preventive Controls: Implementation

Technical Prevention

- Access controls
- Input validation
- Encryption
- Firewalls

Physical Prevention

- Door locks
- Security gates
- Cable locks
- Security cameras

Administrative Prevention

- Security policies
- Access procedures
- Security training

Preventive Controls: Effectiveness

- The effectiveness of preventive controls depends on proper **configuration** and maintenance.
- Organizations must regularly test and validate their preventive controls.
- Even strong preventive controls can be circumvented if not properly supported by other control types.
- Cost-benefit analysis should guide investments in preventive controls.

Measuring Effectiveness

- Number of blocked attempts
- Reduction in incidents
- System uptime
- Compliance rates

Deterrent Controls: Introduction

- **Deterrent controls** are designed to discourage potential attackers from attempting security violations.
- These controls work by making the target appear more difficult or risky to attack.
- Deterrent controls often have both psychological and practical effects on potential threats.
- They complement preventive controls by reducing the likelihood of attack attempts.

Key Principle

Effective deterrents make potential attackers decide that the risk isn't worth the potential reward.

Deterrent Controls: Implementation

- Deterrent controls must be visible enough to influence potential attacker behavior.
- Organizations should implement deterrents across physical, technical, and administrative domains.
- The strength of deterrent controls often depends on the perceived consequences of violation.
- Regular assessment ensures deterrents remain credible and effective.

Technical	**Physical**	**Administrative**
Warning banners	Warning signs	Security policies
Login monitors	Visible cameras	Legal notices
Access logs	Security lighting	Ethics training
Failed attempt limits	Guard patrols	Disciplinary procedures

Deterrent Controls: Psychological Aspects

- **Psychological deterrence** works by affecting the risk-reward calculations of potential attackers.
- Clear communication of security measures increases their deterrent value.
- The visibility of security controls often matters more than their actual strength.
- Organizations must maintain the credibility of their deterrent measures.

Effective Deterrence Examples

- Prominent security cameras
- Published security policies
- Visible security personnel
- Clear consequence statements

Deterrent Controls: Limitations

- Deterrent controls do not physically prevent security violations from occurring.
- The effectiveness of deterrents varies based on the attacker's motivation and risk tolerance.
- Over-reliance on deterrents can create a false sense of security.
- Organizations need to balance deterrence with actual protective measures.

Common Limitations

- May not affect determined attackers
- Requires perception of credible consequences
- Effectiveness hard to measure
- Cannot stand alone

Detective Controls: Introduction

- **Detective controls** are designed to identify and record security violations or attempts.
- These controls work by monitoring systems, networks, and physical spaces for suspicious activity.
- Detective controls are essential for identifying when preventive controls have failed.
- They provide valuable information for incident response and security improvement.

Key Principle

You can't respond to security incidents if you don't know they're happening!

Detective Controls: Types and Examples

- Detective controls must operate continuously to maintain security awareness.
- Different types of detective controls monitor different aspects of security.
- Most detective controls generate logs or alerts for security analysis.
- Real-time detection allows for faster incident response.

Control Type	**Examples**
System Monitoring	Log files, Audit trails
Network Monitoring	IDS, Traffic analysis
Physical Monitoring	Motion sensors, Cameras
Access Monitoring	Login tracking, Badge readers

Detective Controls: Monitoring Process

- **Security monitoring** requires a systematic approach to data collection and analysis.
- Organizations must establish baselines to identify abnormal activity effectively.
- Detective controls should generate appropriate alerts for different security events.
- Regular review of detection data helps identify security trends and patterns.

Monitoring Steps

1. Data Collection
2. Analysis
3. Alert Generation
4. Investigation
5. Response

Detective Controls: Effective Implementation

- Organizations must carefully configure detective controls to minimize false alarms.
- **Alert thresholds** should balance security awareness with operational efficiency.
- Detective controls require regular maintenance and tuning to remain effective.
- Staff must be trained to properly interpret and respond to detection alerts.

Configuration Considerations

- Logging level settings
- Alert sensitivity
- Storage requirements
- Response procedures

Corrective Controls: Introduction

- **Corrective controls** are measures designed to fix problems after a security incident occurs.
- These controls help restore systems and data to their normal operational state.
- Corrective controls often work in conjunction with detective controls.
- They are essential for maintaining business continuity after security breaches.

Key Principle

Even with strong prevention, organizations must be prepared to correct security incidents quickly.

Corrective Controls: Common Types

- Organizations need different types of corrective controls for various security scenarios.
- Each type of corrective control addresses specific aspects of incident recovery.
- The effectiveness of correction often depends on how quickly controls can be activated.
- Regular testing helps ensure corrective controls will work when needed.

Control Type	**Purpose**
Backup Systems	Restore lost or corrupted data
Antivirus Tools	Remove malware infections
Patch Management	Fix security vulnerabilities
System Recovery	Restore system functionality

Corrective Controls: Implementation Steps

- Organizations must develop clear procedures for implementing corrective controls.
- **Recovery priorities** should be established before incidents occur.
- Staff need proper training to execute corrective measures effectively.
- Regular testing and updates ensure corrective controls remain viable.

Recovery Process

1. Incident Assessment
2. Control Selection
3. Implementation
4. Verification
5. Documentation

Corrective Controls: Success Factors

- The success of corrective controls depends on proper preparation and quick response.
- Organizations must maintain updated documentation of all corrective procedures.
- Regular testing helps identify and address potential recovery issues.
- Staff must understand their roles in the correction process.

Critical Success Factors

- Current recovery plans
- Tested procedures
- Available resources
- Trained personnel
- Clear responsibilities

Compensating Controls: Introduction

- **Compensating controls** are alternative security measures used when primary controls are not feasible.
- These controls provide similar levels of protection through different means.
- Organizations implement compensating controls due to technical, operational, or cost limitations.
- The effectiveness must be equivalent to or greater than the original control.

Key Principle

Compensating controls must provide protection that is as strong as the original control they replace.

Compensating Controls: Use Cases

- Organizations need compensating controls when primary controls cannot be implemented.
- Each use case requires careful evaluation of security equivalence.
- The choice of compensating controls must be justified and documented.
- Regular assessment ensures continued effectiveness of alternative measures.

Primary Control	**Compensating Control**
Biometric access	Multi-factor authentication
Full disk encryption	File-level encryption
Network segmentation	Enhanced monitoring
Physical security	Video surveillance

Compensating Controls: Implementation

- Implementation of compensating controls requires careful planning and documentation.
- Organizations must demonstrate that alternative controls meet security requirements.
- **Risk assessment** is essential when evaluating compensating controls.
- Regular reviews ensure compensating controls remain appropriate and effective.

Implementation Steps

1. Identify limitations
2. Assess alternatives
3. Document justification
4. Implement control
5. Verify effectiveness

Compensating Controls: Evaluation Criteria

- Organizations must evaluate compensating controls against specific criteria.
- The evaluation process should consider both security effectiveness and operational impact.
- Documentation must demonstrate how compensating controls meet security objectives.
- Regular assessment helps identify when compensating controls need adjustment.

Evaluation Factors

- Security strength
- Implementation cost
- Operational impact
- Maintenance requirements
- Compliance alignment

Directive Controls: Introduction

- **Directive controls** are measures that guide and direct people's behavior regarding security.
- These controls establish the requirements for proper security practices and procedures.
- Directive controls form the foundation for security awareness and compliance.
- They help create a strong security culture within the organization.

Key Principle

Directive controls establish what people should do, rather than technically enforcing or preventing actions.

Directive Controls: Components

- Organizations need various types of directive controls to guide different aspects of security.
- Each component addresses specific security behaviors and requirements.
- Directive controls must be clear, accessible, and regularly updated.
- Staff need proper training to understand and follow directive controls.

Component	**Purpose**
Security Policies	Define requirements
Usage Guidelines	Direct daily activities
Security Procedures	Guide specific tasks
Standards	Set minimum expectations

Directive Controls: Implementation

- Effective implementation of directive controls requires clear communication and training.
- Organizations must ensure all staff understand their security responsibilities.
- **Regular updates** keep directive controls aligned with current security needs.
- Compliance monitoring helps ensure directive controls are being followed.

Key Elements

1. Clear documentation
2. Staff training
3. Regular updates
4. Compliance tracking
5. Performance feedback

Review: Control Types Working Together

- Different types of controls must work together to create effective security.
- Each control type serves a specific purpose in the overall security strategy.
- Organizations need a balanced mix of all control types.
- Regular assessment helps optimize the combination of controls.

Control Type Integration

- Preventive blocks threats
- Deterrent discourages attempts
- Detective identifies incidents
- Corrective fixes problems
- Compensating provides alternatives
- Directive guides behavior

Summary: Security Control Categories

- **Technical Controls** provide automated protection through technology solutions.
- **Managerial Controls** guide security through policies and risk management.
- **Operational Controls** involve day-to-day procedures performed by people.
- **Physical Controls** protect tangible assets and facilities.

Key Takeaway

Effective security requires all categories working together in a coordinated approach.

Summary: Security Control Types

Control Type	**Primary Purpose**
Preventive	Stop incidents before they occur
Deterrent	Discourage potential attacks
Detective	Identify security violations
Corrective	Fix problems after detection
Compensating	Provide alternative protection
Directive	Guide security behavior

Review Questions

Class Discussion

Consider these questions about security controls:

1. How do technical and physical controls work together to protect assets?
2. Why might an organization need to implement compensating controls?
3. What role do directive controls play in maintaining security?
4. How can detective controls support corrective controls?