Co-funded by
the European Union

Course: Security Analysis and Risk Management

Project: Cyber Security 4 ALL(CS4ALL)

Chapter 4

Security Controls and Mitigation Strategies

Overview

- Overview of security controls (preventive, detective, corrective)
- Best practices for developing and managing security policies
- Implementation of security controls in cyber systems
- Incident response planning and execution
- Business continuity and disaster planning practices
- Case studies on incident response

Overview of Security Control

- **Security Control:**
  - A safeguard or countermeasure applied to manage and reduce the risk that a threat can exploit a vulnerability and protect an organization's information, assets, and infrastructure
  - These controls can be technical, physical, or administrative
  - They are designed to prevent, detect, correct, or mitigate security risks.

Co-funded by the European Union

Overview of Security Control

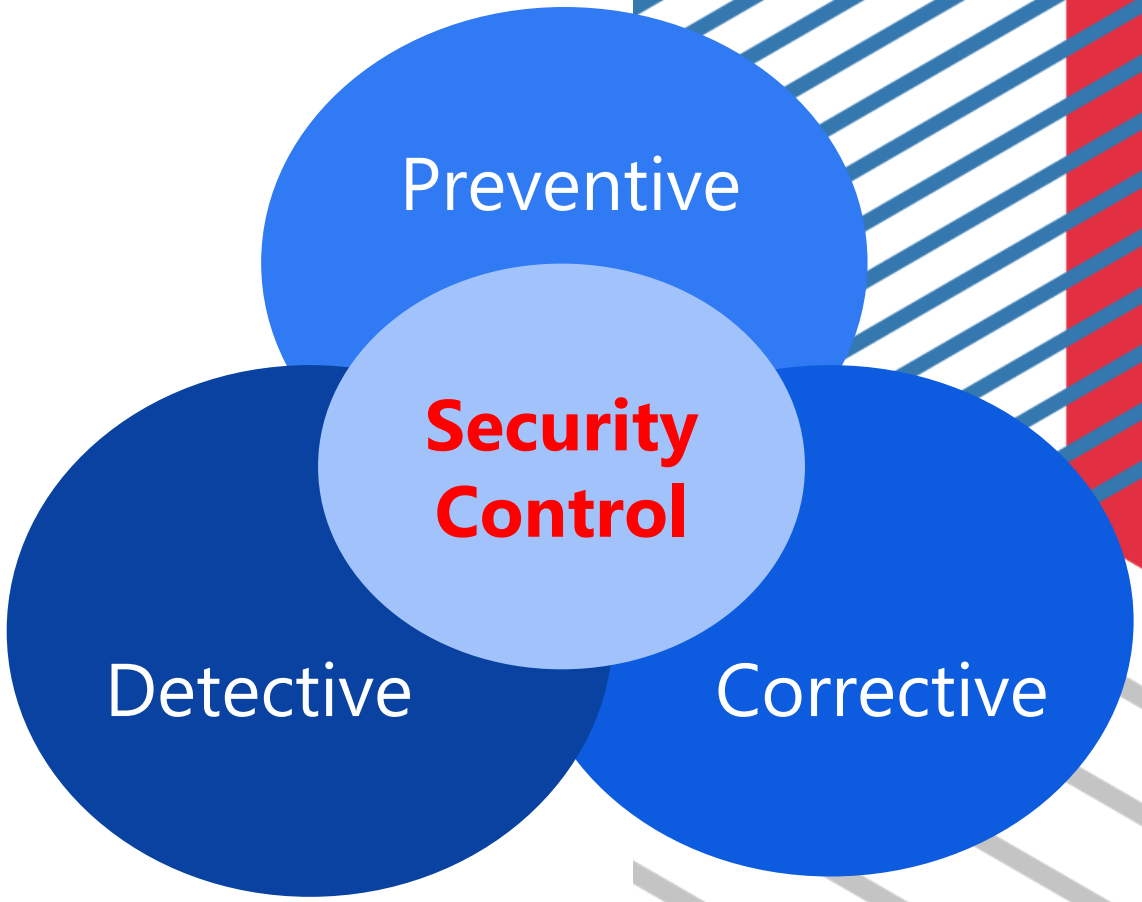
- **A Simple Example:**
  - An awareness training to minimize the risk of a social engineering attack on your system, network etc.
- **Why Security Control and Mitigation Strategies?:**
  - To reduce risks, respond to incidents, and ensure business continuity.

*"The act we perform to reduce a risk is also called **risk mitigation.**"*

Co-funded by the European Union

Types of Security Control

- **Preventive Controls:**
- **Detective Controls:**
- **Corrective Controls:**



Co-funded by the European Union

Preventive Controls

- These are the frontline defender to stop or reduce the malicious threads/activities.
- Attempt to prevent a security incident from occurring.
- Examples:
  - Firewalls
  - Access Control Systems
  - Encryption
  - Multi-Factor Authentication

Co-funded by the European Union

Preventive Controls

- **Firewalls**
  - Protect networks from unauthorized access by filtering incoming and outgoing traffic.
- **Access Control Systems**
  - Use principles like least privilege and role-based access control (RBAC) to restrict access to sensitive systems.
- **Encryption**
  - Secures data ensuring it cannot be accessed by unauthorized parties.
- **Multi-Factor Authentication**
  - Requires users to present multiple forms of identification, preventing unauthorized access even if passwords are compromised.

Co-funded by the European Union

Detective Controls

- Attempt to detect and report incidents after they have occurred.
- They detects suspicious activity and triggers responses.
- Examples:
  - Intrusion Detection Systems (IDS)
  - Security Information and Event Management (SIEM)
  - Log Monitoring
  - Audit Trails

Co-funded by the European Union

Detective Controls

- **Intrusion Detection Systems (IDS)**
  - monitor network or system activities for malicious behavior or policy violations.
- **Security Information and Event Management (SIEM)**
  - aggregates and analyzes security data from various sources to identify potential threats.
- **Log Monitoring**
  - checks system logs for unusual behavior, providing real-time alerts to security teams.
- **Audit Trails**
  - Provide a record of user activities that can be reviewed to trace the source of a security breach.

Co-funded by the European Union

Corrective Controls

- Mitigate the damage and restore systems to their normal state after a security incident has occurred.
- Aim to minimize the impact of a security breach and prevent its recurrence.
- Examples:
  - Incident Response Plans
  - Patch Management
  - Backups
  - Quarantine Mechanisms

Co-funded by the European Union

Corrective Controls

- **Incident Response Plans**
  - Guide the steps to be taken after a security incident, ensuring quick and effective mitigation.
- **Patch Management**
  - Involves updating systems to fix vulnerabilities and prevent future attacks.
- **Backups**
  - Enable recovery of data that has been lost or corrupted during a breach.
- **Quarantine Mechanisms**
  - Isolate compromised systems or networks to prevent further spread of malicious activity.

Co-funded by the European Union

Types of Security Control- Comparison

TYPES OF SECURITY CONTROLS	CONTROL FUNCTIONS: PREVENTATIVE	DETECTIVE	CORRECTIVE
PHYSICAL CONTROLS	• Fences • Gates • Locks	• CCTV • Surveillance Cameras	• Repair physical damage • Re-issue access cards
TECHNICAL CONTROLS	• Firewall • IPS • MFA • Antivirus	• IDS • Honeypots	• Vulnerability patching • Reboot a system • Quarantine a virus
ADMINISTRATIVE CONTROLS	• Hiring & termination policies • Separation of duties • Data classification	• Review access rights • Audit logs and unauthorized changes	• Implement a business continuity plan • Have an incident response plan

Source: https://purplesec.us/learn/security-controls/

Co-funded by the European Union

Best Practices for Security Policy Management

- **Security Policies**
  - are the foundation of strong cyber security programs
  - establish guidelines and procedures that govern how security is maintained and enforced within an organization
- **Best Practices for developing and managing security policies**
  - Policy Development
  - Regular Updates
  - Enforcement
  - Employee Training

Co-funded by the European Union

Best Practices for Security Policy Management

- **Policy Development**
  - ***Define Clear Objectives***: that align with the organization's overall risk management strategy
  - ***Involve Key Stakeholders***: to develop effective policies it requires input from all departments, including IT, legal, human resources, etc
  - ***Compliance with Regulations and Standards***: Security policies should incorporate relevant legal, regulatory, and industry standards.

Co-funded by the European Union

Best Practices for Security Policy Management

- **Regular Updates**
  - New threats and technologies constantly emerges
  - So, security policies should be regularly reviewed and updated to reflect the latest risks, regulatory requirements, and organizational changes
  - ***Annual Reviews***: Conduct at least an annual review of all security policies.
  - ***Incident-Driven Updates***: Revise policies in response to significant security incidents or after identifying new vulnerabilities.

Co-funded by the European Union

Best Practices for Security Policy Management

- **Enforcement**
  - Implement policies with a compliance and audit process.
- **Employee Training**
  - A security policy is only effective if employees understand and follow it.
  - Engage staff in understanding and adhering to policies
  - Regularly train employees on security best practices, phishing detection, and password management

Co-funded by the European Union

Implementation of Security Controls in Cyber Systems

- involves strategically integrating preventive, detective, and corrective measures into an organization's infrastructure to address specific risks
- Security Controls can be categories in the following implementation
  - Network Security
  - End-Point Security
  - Application Security
  - Data Security

Co-funded by the European Union

Implementation of Security Controls in Cyber Systems

- **Network Security**
  - firewalls, VPNs, and network segmentation to protect against external and internal threats
  - **Perimeter Security**: uses Firewalls and IPS (intrusion prevention systems) for monitoring and filtering traffic to block malicious activity.
  - **Network Segmentation**: Isolating different parts of the network limits the spread of attacks, ensuring that even if one area is compromised.
  - **Secure Remote Access**: Implementing secure VPNs and MFA for remote users is essential

Co-funded by the European Union

Implementation of Security Controls in Cyber Systems

- **Endpoint Security**
  - Endpoints: laptops, mobile devices and workstations which are prime targets for cyberattacks.
  - ***Antivirus Software***: Protects devices from malware, ransomware, and other threats.
  - ***Device Encryption***: Ensures that sensitive data on endpoints is encrypted, preventing unauthorized access in case of device theft or loss.
  - ***Patch Management***: Regularly updates systems to patch known vulnerabilities.

Co-funded by the European Union

Implementation of Security Controls in Cyber Systems

- **Application Security**
  - focuses on safeguarding software from exploitation, using controls such as:
    - Secure Coding Practices
    - Application Firewalls
    - Input Validation
- **Data Security**
  - Encryption
  - Access Control
  - Data Loss Prevention (DLP)

Co-funded by the European Union

Incident Response Planning and Execution

- **Incidence Response (IR)**
  - is an approach that addresses and manages the aftermath of a cybersecurity incident
- **An Incident Response Plan (IRP)**
  - when well-defined, ensures the security incidents are handled quickly, efficiently and with minimal damage.
- **Incident Response Team** includes representatives from
  - IT and Security
  - Legal and Compliance
  - Public Relations
  - Leadership

Co-funded by the European Union

Incident Response Planning and Execution

- **Phases of Incident Response**
  - ***Preparation***: Develop an incident response plan (IRP), train staff, and run simulations.
  - ***Identification***: Detect potential incidents through monitoring systems, logs, and alerts.
  - ***Containment***: Limit the damage by isolating affected systems or networks.
  - ***Eradication***: Identify the root cause of the incident and eliminate it
  - ***Recovery***: estore affected systems to full functionality and ensure that no residual threats remain
  - ***Post-Incident Analysis***: understand how the incident occurred and identify improvements to prevent in future

Co-funded by the European Union

Business Continuity and Disaster Planning Practices

- Business continuity and disaster recovery (BC/DR) planning
  - ensures that critical operations can continue in the event of a security incident, natural disaster, or system failure.

- BC/DR plans
  - focus on minimizing downtime and ensuring that the organization can recover essential functions quickly.

Co-funded by the European Union

Business Continuity and Disaster Planning Practices

- **Components of a BC/DR Plan**
  - ***Business Impact Analysis*** (BIA): Identifies critical business functions and the potential impact of disruptions.
  - ***Recovery Time Objectives*** (RTOs) and ***Recovery Point Objectives*** (RPOs): Determine acceptable downtime (RTO) and acceptable data loss (RPO) for each business function.
  - ***Data Backups***: Regular backups of critical data should be stored in secure, offsite locations etc.
  - ***Redundancy***: ensure that operations can continue even if primary systems fail.

Co-funded by the European Union

Case Studies on Incident Response

- **Case 1:** Response to a ransomware attack on a healthcare system.
- **Case 2:** Cyber breach in financial services and its containment.
- **Case 3:** Lessons from a data leakage incident in e-commerce.

Co-funded by the European Union

Conclusion

- A strong cybersecurity framework requires a well-rounded approach involving preventive, detective, and corrective controls.
- Properly developed security policies, effective incident response planning, and business continuity strategies are essential for minimizing the impact of cyber incidents and ensuring organizational resilience in the face of evolving threats.

Thank You

Co-funded by
the European Union

References

1. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
2. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf
3. https://www.iso.org/isoiec-27001-information-security.html
4. https://www.nist.gov/cyberframework
5. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
6. https://www.iso.org/iso-22301-business-continuity.html
7. https://purplesec.us/learn/security-controls/
8. https://www.cybermaxx.com/resources/what-are-the-different-types-of-security-controls-in-cybersecurity/

Questions & answers

Invite questions from the audience.

Co-funded by
the European Union