# SECURITY OPERATIONS

*Chapter Summary:* This chapter provides a comprehensive overview of the day-to-day practices and strategies for implementing security controls and mitigating risks within an organization. Key points covered include:

1. **Data Security Practices**:
   - Emphasizes the importance of data security as a process and discipline in protecting the value of data throughout its lifecycle, from creation to destruction. This involves classifying, categorizing, labeling, retaining, and destroying data appropriately.
2. **Encryption and Hashing**:
   - Explains the process of encrypting data to convert plaintext into ciphertext using keys and algorithms, and decrypting it back to plaintext. Hashing is also discussed, which generates fixed-length hash values from input data.
3. **System Hardening and Configuration Management**:
   - Discusses system hardening, which involves applying secure configurations to reduce the attack surface and locking down various hardware, communication systems, and software. Configuration management ensures that only authorized changes are made to systems, involving identification, baseline, change control, and verification processes.
4. **Security Policies**:
   - Examines best practice security policies including data handling, password management, acceptable use, bring your own device (BYOD), privacy protection, and change management. These policies govern appropriate use of assets, devices, data, and the transition from current to future states.
5. **Change Management Practices**:
   - Describes the core activities of change management, including documentation, approval, and rollback. Change management starts with a request for change (RFC) and involves various development and testing stages before release to end users.
6. **Security Awareness Training**:
   - Highlights the importance of security awareness training in reducing internal threats to an organization. Training is tailored to specific security topics, organization, positions, or individuals, and emphasizes the significance of password protection.

Overall, Chapter 5 underscores the critical role of implementing security controls, practices, and policies to safeguard data and systems, while also emphasizing the importance of continuous training and awareness to mitigate security risks effectively.

## *Chapter Takeaways:*

The data handling process involves several key steps to ensure the proper management and security of data throughout its lifecycle:

1. **Create**:
   - Involves the generation or acquisition of new data through various means, such as data entry, data collection, or data acquisition from external sources.
2. **Store**:
   - Refers to the secure storage of data in appropriate locations, such as databases, file systems, or cloud storage platforms. Data storage should adhere to security and compliance requirements to prevent unauthorized access or loss of data.
3. **Share**:
   - Involves the controlled sharing of data with authorized users or entities, both within and outside the organization. This may include sharing data with colleagues, partners, or customers through secure communication channels or collaboration platforms.
4. **Use**:
   - Entails accessing and utilizing data for various purposes, such as analysis, decision-making, reporting, or operational activities. Data usage should comply with legal, ethical, and organizational policies to ensure data integrity and confidentiality.
5. **Modify**:
   - Allows authorized users to make changes or updates to data as needed. This may involve editing, appending, or deleting data records while maintaining data accuracy and consistency.
6. **Archive**:
   - Involves the long-term storage of data that is no longer actively used but may be required for future reference, compliance, or historical purposes. Archived data should be securely retained and properly indexed for efficient retrieval when needed.
7. **Destroy**:
   - Refers to the secure and irreversible removal of data at the end of its lifecycle or when it is no longer needed. Data destruction methods may

include data wiping, shredding, or degaussing to ensure that the data cannot be recovered or accessed by unauthorized parties.

By following these steps in the data handling process, organizations can effectively manage data while protecting its confidentiality, integrity, and availability throughout its lifecycle. Additionally, adherence to regulatory requirements and best practices ensures compliance with data protection laws and industry standards.

Logging plays a crucial role in monitoring network traffic and activities for both ingress (incoming) and egress (outgoing) data. Here's how various tools and data types are utilized for logging in both scenarios:

## Ingress Monitoring Tools:

1. **Firewalls**:
   - Firewalls log incoming traffic based on predefined rules and policies. These logs contain information about connection attempts, allowed/denied traffic, and potential threats.
2. **Gateways**:
   - Gateways, such as proxy servers or email gateways, log incoming traffic passing through them. These logs provide insights into the types of traffic, origin, destination, and potential security events.
3. **Remote Authentication Servers**:
   - Remote authentication servers log authentication attempts made by users or devices trying to access network resources. These logs help in tracking user activities and identifying unauthorized access attempts.
4. **IDS/IPS Tools** (Intrusion Detection/Prevention Systems):
   - IDS/IPS tools monitor incoming traffic for signs of suspicious or malicious activities. They generate logs for detected intrusions, attacks, or policy violations, helping in identifying and mitigating security threats.
5. **SIEM Solutions** (Security Information and Event Management):
   - SIEM solutions aggregate and analyze logs from various sources, including firewalls, gateways, authentication servers, and IDS/IPS tools. They correlate events, detect anomalies, and generate alerts for potential security incidents.
6. **Anti-Malware Solutions**:
   - Anti-malware solutions monitor incoming traffic for malware threats, such as viruses, worms, and trojans. They log detection events, quarantine actions, and remediation activities to protect the network from malware infections.

## Egress Monitoring Data Types:

1. **Email (Content and Attachments)**:
   - Egress monitoring logs email communications, including content and attachments, to detect sensitive data leaks, unauthorized access, or malicious activities.
2. **Copy to Portable Media**:
   - Logs track instances where data is copied to portable media devices, such as USB drives or external hard disks. This helps in preventing data exfiltration and enforcing data security policies.
3. **File Transfer Protocol (FTP)**:
   - FTP logs record file transfers made using FTP protocols, including the source, destination, and contents of transferred files. Monitoring FTP traffic helps in identifying unauthorized file transfers or data leakage.
4. **Posting to Web Pages/Websites**:
   - Logs capture activities involving posting content to web pages or websites, such as uploading files, publishing articles, or sharing information. This helps in monitoring web content and ensuring compliance with content policies.
5. **Applications/Application Programming Interfaces (APIs)**:
   - Logs from applications and APIs track data exchanges and interactions with external systems. Monitoring these logs helps in detecting abnormal behavior, unauthorized access, or data leakage through application interfaces.

By utilizing logging and monitoring tools effectively, organizations can enhance their cybersecurity posture by detecting and responding to security threats and ensuring compliance with data protection regulations.

1. **Symmetric Encryption**:
   - In symmetric encryption, the same key is used for both encryption and decryption. This means that both the sender and the receiver share a single, secret key that is used to both encrypt and decrypt the data. Symmetric encryption algorithms are typically faster and more efficient than asymmetric algorithms. However, the main challenge with symmetric encryption is securely sharing the secret key between the communicating parties.
2. **Asymmetric Encryption**:
   - In asymmetric encryption, also known as public-key encryption, different keys are used for encryption and decryption. This involves a pair of keys: a public key and a private key. The public key is freely distributed and can be used by anyone to encrypt data, while the private key is kept secret and is used by the intended recipient to decrypt the data. Asymmetric encryption provides a solution to the key distribution problem inherent in symmetric encryption. It

allows for secure communication between parties without requiring them to share a secret key beforehand.

Each type of encryption has its own advantages and use cases, and they are often used together in combination to provide secure communication and data protection in various scenarios.

## *Module 2: Understand system hardening*

Configuration management involves a set of procedures and elements aimed at ensuring the integrity, consistency, and security of an organization's IT systems and infrastructure. Here's a breakdown of configuration management procedures and elements:

### Configuration Management Procedures:

1. **Identification**:
    - Identifying and documenting all configuration items (CIs) within the IT environment. This includes hardware, software, documentation, network components, and other IT assets.
2. **Baseline**:
    - Establishing a baseline configuration that serves as a reference point for comparison. This baseline represents the known, stable state of the IT environment and is used to track changes over time.
3. **Change Control**:
    - Implementing controls and processes for managing changes to the IT environment. This involves evaluating proposed changes, assessing their impact, obtaining appropriate approvals, and implementing changes in a controlled manner.
4. **Verification & Audit**:
    - Verifying that implemented changes align with approved specifications and do not introduce unintended consequences or vulnerabilities. Regular audits are conducted to ensure compliance with configuration management policies and identify areas for improvement.

### Elements of Configuration Management:

1. **Inventory**:
    - Maintaining an accurate inventory of all IT assets, including hardware, software licenses, peripherals, and other components. The inventory provides visibility into the IT environment and facilitates effective management and tracking of resources.

2. **Baselines**:
    - Establishing baseline configurations for different types of IT assets, including servers, workstations, network devices, and applications. Baselines define the standard configuration settings and parameters for each asset type.
3. **Updates**:
    - Managing software and firmware updates to ensure that IT systems remain current, secure, and functional. This involves regularly applying patches, updates, and upgrades to address vulnerabilities, enhance performance, and add new features.
4. **Patches**:
    - Applying security patches and hotfixes to address known vulnerabilities and security threats in software and operating systems. Patch management processes include identifying applicable patches, testing them in a controlled environment, and deploying them across the IT infrastructure.

By implementing robust configuration management procedures and maintaining essential elements such as inventory, baselines, updates, and patches, organizations can effectively manage their IT assets, reduce security risks, and maintain the integrity and availability of their systems and data.

## *Module 3: Understand best practice security policies:*

## Data Handling Policy Procedures:

1. **Classify**:
    - Classify data based on its sensitivity and importance to the organization. This involves categorizing data into different levels of sensitivity, such as public, internal use, confidential, or highly confidential.
2. **Categorize**:
    - Categorize data based on its type, format, and intended use. This includes identifying the type of data (e.g., personal, financial, intellectual property) and assigning appropriate categories or tags to facilitate management and access control.
3. **Label**:
    - Label data with metadata or tags that indicate its classification, category, ownership, and other relevant attributes. This helps in identifying and managing data throughout its lifecycle and ensuring proper handling and protection.

4. **Store**:
    - Store data in secure and appropriate locations, such as databases, file servers, or cloud storage platforms. Implement access controls and encryption to protect data from unauthorized access or disclosure.
5. **Encrypt**:
    - Encrypt sensitive data to prevent unauthorized access or interception. Use encryption algorithms and cryptographic techniques to convert plaintext data into ciphertext, rendering it unreadable to unauthorized parties.
6. **Backup**:
    - Regularly back up data to ensure availability and resilience in case of data loss or corruption. Implement backup procedures and schedules to create copies of critical data and store them securely in off-site or redundant locations.
7. **Destroy**:
    - Establish procedures for securely destroying data that is no longer needed or has reached the end of its lifecycle. Use data destruction methods such as data wiping, shredding, or degaussing to ensure that the data cannot be recovered or accessed by unauthorized parties.

By following these data handling policy procedures, organizations can effectively manage and protect their data assets while complying with regulatory requirements and industry best practices. This ensures confidentiality, integrity, and availability of data throughout its lifecycle and helps mitigate risks associated with data breaches or unauthorized access.

Below are the procedures and elements typically included in an Acceptable Use Policy (AUP), along with information on Bring Your Own Device (BYOD) policy devices, and the types of data protected by a Privacy Policy, as well as examples of national and international privacy regulations/laws:

## Acceptable Use Policy (AUP) Procedures:

1. **Data Access**:
    - Define procedures for accessing organizational data, including permissions, authentication requirements, and restrictions on data access based on job roles or responsibilities.
2. **System Access**:
    - Establish guidelines for accessing and using organizational IT systems, including remote access, account management, and acceptable use of system resources.
3. **Data Disclosure**:

   - Outline rules and restrictions regarding the disclosure of sensitive or confidential information to external parties, including clients, partners, or third-party vendors.
4. **Passwords**:
   - Define password requirements, such as complexity, length, and expiration, to ensure secure access to systems and data. Encourage users to use strong, unique passwords and prohibit password sharing.
5. **Data Retention**:
   - Specify policies for retaining and disposing of organizational data in compliance with legal and regulatory requirements. Define data retention periods, archival procedures, and data destruction methods.
6. **Internet Usage**:
   - Establish guidelines for appropriate internet usage, including acceptable websites, prohibited activities (e.g., accessing inappropriate content, downloading unauthorized software), and monitoring of internet usage.
7. **Company Device Usage**:
   - Outline rules for using company-provided devices, including laptops, smartphones, tablets, and other hardware. Define acceptable use, security measures, and responsibilities for device maintenance and protection.

## Bring Your Own Device (BYOD) Policy Devices:

- Cell Phone
- Tablet
- Laptop
- Smartwatch
- Bluetooth Devices

## Privacy Policy Protects:

- Personally Identifiable Information (PII)
- Electronic Protected Health Information (ePHI)
- Bank/Credit Card Information

## Examples of National and International Privacy Regulations/Laws:

- **GDPR (General Data Protection Regulation)** in the EU: Enforces strict regulations on the processing and protection of personal data of EU citizens, including data collection, storage, and transfer.

- **Personal Information Protection and Electronic Documents Act (PIPEDA)** in Canada: Governs the collection, use, and disclosure of personal information by private sector organizations, including rules for obtaining consent, safeguarding data, and reporting data breaches.

By implementing and adhering to these policies and regulations, organizations can promote responsible use of IT resources, protect sensitive data, and maintain compliance with privacy laws and industry standards.

## *Module 4: Understand security awareness training:*

## Security Awareness Training Types:

1. **Education**:
    - Education focuses on providing employees with foundational knowledge and understanding of cybersecurity principles, best practices, policies, and procedures. It typically involves formal training sessions, seminars, or online courses covering various topics such as password security, data protection, and phishing awareness.
2. **Training**:
    - Training involves hands-on instruction and practical exercises designed to develop specific skills and competencies related to cybersecurity. This may include simulated phishing attacks, incident response drills, and cybersecurity simulations to help employees recognize and respond to security threats effectively.
3. **Awareness**:
    - Awareness aims to foster a culture of cybersecurity within the organization by promoting ongoing awareness and vigilance among employees. This includes regular communication, newsletters, posters, and reminders about security best practices, emerging threats, and reporting procedures.

## Social Engineering Techniques:

1. **Baiting**:
    - Baiting involves enticing individuals with a promise of reward or benefit to trick them into revealing sensitive information or performing an action that compromises security. For example, leaving infected USB drives in public places labeled as "Confidential" to entice users to plug them into their computers.
2. **Phone Phishing or Vishing**:

- Phone phishing, or vishing, involves using voice communication to deceive individuals into disclosing confidential information or performing fraudulent actions. This may include impersonating trusted entities, such as IT support or financial institutions, to trick victims into revealing sensitive data over the phone.

3. **Pretexting**:
    - Pretexting involves creating a fabricated scenario or pretext to manipulate individuals into disclosing information or performing actions they wouldn't typically do. This may include impersonating a colleague or authority figure to gain trust and extract sensitive information.
4. **Quid Pro Quo**:
    - Quid pro quo involves offering something of value in exchange for sensitive information or access. For example, offering free software or services in exchange for login credentials or access to a network.
5. **Tailgating**:
    - Tailgating, also known as piggybacking, involves unauthorized individuals following authorized personnel into restricted areas by closely trailing behind them. This exploits the natural inclination to hold doors open for others, bypassing physical security measures.
6. **False Flag or False Front Operations**:
    - False flag or false front operations involve creating a false identity or organization to deceive individuals into trusting and divulging sensitive information or resources. This may include creating fake websites, email addresses, or social media profiles to impersonate legitimate entities.

By educating employees about these social engineering techniques and providing them with the necessary knowledge and skills to recognize and respond to such threats, organizations can mitigate the risks posed by social engineering attacks and enhance their overall cybersecurity posture.

## *Important terms and their clarification:*

1. **Application Server**:
    - Definition: A computer that hosts applications accessed by user workstations.
    - Real-life Scenario: A company uses an application server to host its customer relationship management (CRM) software, allowing employees to access customer data and manage interactions from their computers.
2. **Asymmetric Encryption**:

- Definition: Encryption method using one key to encrypt and another to decrypt.
- Real-life Scenario: When a user sends an encrypted email, they use the recipient's public key to encrypt the message. The recipient then uses their private key to decrypt and read the email.

3. **Checksum**:
    - Definition: A digit representing the sum of correct digits in digital data to detect errors.
    - Real-life Scenario: When downloading a file from the internet, the computer calculates a checksum based on the received data. If the checksum doesn't match the expected value, it indicates that the file may be corrupted, triggering a re-download.
4. **Ciphertext**:
    - Definition: Encrypted form of a message, making it unreadable except for intended recipients.
    - Real-life Scenario: Secure messaging apps use ciphertext to encrypt messages before sending them. Only the intended recipient with the decryption key can read the message.
5. **Classification**:
    - Definition: Identifying the potential harm if information is disclosed to unauthorized parties, focusing on maintaining data confidentiality.
    - Real-life Scenario: A government agency classifies documents as "Top Secret," "Secret," or "Confidential" based on the level of sensitivity. This determines who can access and handle the information.
6. **Configuration Management**:
    - Definition: Process ensuring authorized and validated changes to a system.
    - Real-life Scenario: A software company uses configuration management to track changes to its codebase. Before deploying updates, developers must submit change requests, which are reviewed and approved to ensure code integrity.
7. **Cryptanalyst**:
    - Definition: One who studies and attempts to defeat cryptographic techniques and information systems security.
    - Real-life Scenario: A cryptanalyst analyzes encryption algorithms to identify weaknesses or vulnerabilities. Their findings help improve the security of cryptographic systems.
8. **Cryptography**:
    - Definition: Study or application of methods to secure information through disguise or transformation.
    - Real-life Scenario: Online banking uses cryptography to encrypt transactions, protecting sensitive financial information from unauthorized access.

9. **Data Loss Prevention (DLP)**:
    - Definition: Systems designed to detect and prevent unauthorized use and transmission of information.
    - Real-life Scenario: A company deploys DLP software to monitor outgoing emails for sensitive data like credit card numbers. If detected, the software blocks the email or alerts administrators to prevent data loss.
10. **Decryption**:
    - Definition: The process of converting encrypted data (ciphertext) back into its original, readable form (plaintext) using the appropriate decryption key.
    - Real-life Scenario: A recipient uses their private key to decrypt an encrypted email, allowing them to read the message sent by the sender.
11. **Degaussing**:
    - Definition: A method of erasing data from magnetic storage media by exposing it to a strong magnetic field, rendering the data irretrievable.
    - Real-life Scenario: A company uses a degaussing machine to wipe sensitive data from old hard drives before disposing of them to ensure data confidentiality.
12. **Digital Signature**:
    - Definition: A cryptographic transformation of data that provides origin authentication, data integrity, and non-repudiation when applied to digital documents.
    - Real-life Scenario: A person electronically signs a contract using a digital signature, verifying their identity and ensuring the integrity of the document.
13. **Egress Monitoring**:
    - Definition: Monitoring outgoing network traffic to detect unauthorized data transmission or suspicious activities.
    - Real-life Scenario: A network administrator sets up egress monitoring to identify and block attempts by employees to send sensitive company information to external email addresses.
14. **Encryption**:
    - Definition: The process of converting plaintext data into an unreadable format (ciphertext) using cryptographic algorithms and keys to protect it from unauthorized access.
    - Real-life Scenario: A user encrypts their laptop's hard drive to safeguard personal files and sensitive information from unauthorized access in case the device is lost or stolen.
15. **Encryption System**:

- Definition: A combination of algorithms, hardware, software, and procedures designed to provide encryption and decryption capabilities for protecting data.
- Real-life Scenario: An organization implements an encryption system to secure sensitive customer information stored in its database, ensuring compliance with data protection regulations.

16. **Hardening**:
    - Definition: The process of applying security configurations and measures to reduce vulnerabilities and strengthen the security posture of hardware, software, and systems.
    - Real-life Scenario: A system administrator hardens a web server by disabling unnecessary services, applying security patches, and configuring access controls to prevent unauthorized access and attacks.
17. **Hash Function**:
    - Definition: An algorithm that generates a unique fixed-size hash value (fingerprint) based on the input data, which is used to verify data integrity and identify duplicate files.
    - Real-life Scenario: A website stores passwords hashed using a hash function to protect user accounts. When a user logs in, their password is hashed and compared to the stored hash for authentication.

1. **Hashing**:
    - Definition: Using a mathematical algorithm to generate a unique numeric value representing data.
    - Real-life Scenario: When you create a password for an online account, the website hashes your password before storing it in its database to protect it from unauthorized access.
2. **Ingress Monitoring**:
    - Definition: Monitoring incoming network traffic for security purposes.
    - Real-life Scenario: An organization sets up an ingress monitoring system to detect and block suspicious network traffic attempting to enter its network, such as malware or unauthorized access attempts.
3. **Message Digest**:
    - Definition: A unique digital signature that identifies data, with any change in the data resulting in a completely different message digest.
    - Real-life Scenario: Digital signatures are used in email communication to verify the integrity and authenticity of messages. If an email's content is altered, its message digest changes, indicating tampering.
4. **Operating System**:
    - Definition: Software that controls and manages a computer's hardware and software resources.
    - Real-life Scenario: Windows, macOS, and Linux are examples of operating systems that manage computer resources, run applications, and provide user interfaces.

5. **Patch**:
    - Definition: A software update that modifies files or settings without changing the version number.
    - Real-life Scenario: Software vendors release patches to fix security vulnerabilities or bugs in their products. Users install these patches to update their software and protect their systems from exploitation.
6. **Patch Management**:
    - Definition: The systematic process of identifying, deploying, and verifying software updates.
    - Real-life Scenario: An IT department implements patch management procedures to regularly scan and update software across the organization's network, ensuring systems are protected against known vulnerabilities.
7. **Plaintext**:
    - Definition: Data in its natural, readable form, vulnerable to unauthorized access.
    - Real-life Scenario: Email messages sent without encryption are transmitted in plaintext, making them susceptible to interception and viewing by unauthorized individuals.
8. **Records Retention**:
    - Definition: The practice of retaining records for a specified period before securely disposing of them.
    - Real-life Scenario: A healthcare organization follows records retention policies to retain patient records for a certain number of years after treatment before securely destroying them to comply with privacy regulations.
9. **Remanence**:
    - Definition: Residual data remaining on storage media after attempting to clear it.
    - Real-life Scenario: Even after wiping a hard drive, traces of data may remain due to remanence, posing a security risk if not properly handled or disposed of.
10. **Request for Change (RFC)**:

- Definition: Initial stage of change management where a change in procedure or product is requested.
- Real-life Scenario: An employee submits an RFC to the IT department requesting a software update to address performance issues on their computer.

11. **Security Governance**:

- Definition: Policies, roles, and processes used by an organization to make security decisions.

- Real-life Scenario: A company establishes a security governance framework to define responsibilities, allocate resources, and establish security controls to protect its assets and information.

12. **Social Engineering**:

- Definition: Manipulating individuals to disclose sensitive information or perform actions through deception.
- Real-life Scenario: A hacker calls an employee posing as IT support, convincing them to reveal their login credentials, allowing unauthorized access to the company's network.

13. **Symmetric Encryption**:

- Definition: Encryption algorithm using the same key for both encryption and decryption.
- Real-life Scenario: Secure messaging apps use symmetric encryption to encrypt and decrypt messages between users, ensuring confidentiality and privacy.

14. **Web Server**:

- Definition: A computer providing World Wide Web services on the internet.
- Real-life Scenario: When you visit a website, your browser sends requests to the web server hosting the site, which then delivers the requested web pages for display on your screen.

15. **Whaling Attack**:

- Definition: Phishing attacks targeting high-ranking individuals or entities to authorize fraudulent fund transfers.
- Real-life Scenario: A CEO receives an email appearing to be from a company executive requesting urgent wire transfer of funds to a new account, falling victim to a whaling attack and resulting in financial loss

-

Some extra meterials you need to know:
https://drive.google.com/file/d/1onUUOeJU5Fj_xA0DVOzp8l6jdpV9_1r9/view?usp=drivesdk