Data Protection

Objectives:

- 1.4 - Explain the importance of using appropriate cryptographic solutions
- 3.3 - Compare and contrast concepts and strategies to protect data
- 4.2 - Explain the security implications of proper hardware, software,and data asset management
- 4.4 - Explain security alerting and monitoring concepts and tools
- 5.1 - Summarize elements of effective security governance

- **Data Protection**
    - *Data Protection*
        - Safeguarding information from corruption, compromise, or loss
    - Data Classifications
        - Types
            - Sensitive
            - Confidential
            - Public
            - Restricted
            - Private
            - Critical
    - Data Ownership Roles
        - Data Owners
        - Data Controllers
        - Data Processors

        - Data Custodians
        - Data Stewards
    - Data States
        - States
            - Data at rest
            - Data in transit
            - Data in use
        - Protection Methods
            - Disk encryption
            - Communication tunneling
    - Data Types
        - Examples
            - Regulated data
            - Trade secrets
            - Intellectual property
            - Legal information
            - Financial information
            - Human vs non-human readable data
    - *Data Sovereignty*
        - Information subject to laws and governance structures within the nation it is collected
    - Securing Data Methods
        - Geographic Restrictions
        - Encryption
        - Hashing
        - Masking

        - Tokenization
        - Obfuscation
        - Segmentation
        - Permission Restriction
    - *Data Loss Prevention (DLP)*
        - Strategy to prevent sensitive information from leaving an organization

- **Data Classifications**
    - *Data Classification*
        - Based on the value to the organization and the sensitivity of the information, determined by the data owner
    - *Sensitive Data*
        - Information that, if accessed by unauthorized persons, can result in the loss of security or competitive advantage for a company
        - Over classifying data leads to protecting all data at a high level
    - Importance of Data Classification
        - Helps allocate appropriate protection resources
        - Prevents over-classification to avoid excessive costs
        - Requires proper policies to identify and classify data accurately
    - Commercial Business Classification Levels
        - *Public*
            - No impact if released; often publicly accessible data
        - *Sensitive*
            - Minimal impact if released, e.g., financial data
        - *Private*

        - Contains internal personnel or salary information
    - *Confidential*
        - Holds trade secrets, intellectual property, source code, etc.
    - *Critical*
        - Extremely valuable and restricted information
- Government Classification Levels
    - *Unclassified*
        - Generally releasable to the public
    - *Sensitive but Unclassified*
        - Includes medical records, personnel files, etc.
    - *Confidential*
        - Contains information that could affect the government
    - *Secret*
        - Holds data like military deployment plans, defensive postures
    - *Top Secret*
        - Highest level, includes highly sensitive national security information
- Legal Requirements
    - Depending on the organization's type, there may be legal obligations to maintain specific data for defined periods
- Documentation
    - Organizational policies should clearly outline data classification, retention, and disposal requirements
- Note: Understanding data classifications and their proper handling is vital for protecting sensitive information and complying with relevant regulations

- **Data Ownership**
  - *Data Ownership*
    - Process of identifying the individual responsible for maintaining the confidentiality, integrity, availability, and privacy of information assets
  - *Data Owner*
    - A senior executive responsible for labeling information assets and ensuring they are protected with appropriate controls
  - *Data Controller*
    - Entity responsible for determining data storage, collection, and usage purposes and methods, as well as ensuring the legality of these processes
  - *Data Processor*
    - A group or individual hired by the data controller to assist with tasks like data collection and processing
  - *Data Steward*
    - Focuses on data quality and metadata, ensuring data is appropriately labeled and classified, often working under the data owner
  - *Data Custodian*
    - Responsible for managing the systems on which data assets are stored, including enforcing access controls, encryption, and backup measures
  - *Privacy Officer*
    - Oversees privacy-related data, such as personally identifiable information (PII), sensitive personal information (SPI), or protected health information (PHI), ensuring compliance with legal and regulatory frameworks
  - Data Ownership Responsibility
    - The IT department (CIO or IT personnel) should not be the data owner; data

owners should be individuals from the business side who understand the data's content and can make informed decisions about classification

- Selection of Data Owners
  - Data owners should be designated within their respective departments based on their knowledge of the data and its significance within the organization
- Note: Proper data ownership is essential for maintaining data security, compliance, and effective data management within an organization. Different roles contribute to safeguarding and managing data appropriately

- **Data States**
  - *Data at Rest*
    - Data stored in databases, file systems, or storage systems, not actively moving
    - Encryption Methods
      - *Full Disk Encryption (FDE)*
        - Encrypts the entire hard drive
      - *Partition Encryption*
        - Encrypts specific partitions, leaving others unencrypted
      - *File Encryption*
        - Encrypts individual files
      - *Volume Encryption*
        - Encrypts selected files or directories
      - *Database Encryption*
        - Encrypts data stored in a database at column, row, or table levels
      - *Record Encryption*
        - Encrypts specific fields within a database record

- *Data in Transit (Data in Motion)*
  - Data actively moving from one location to another, vulnerable to interception
  - Transport Encryption Methods
    - *SSL (Secure Sockets Layer) and TLS (Transport Layer Security)*
      - Secure communication over networks, widely used in web browsing and email
    - *VPN (Virtual Private Network)*
      - Creates secure connections over less secure networks like the internet
    - *IPSec (Internet Protocol Security)*
      - Secures IP communications by authenticating and encrypting IP packets
- *Data in Use*
  - Data actively being created, retrieved, updated, or deleted
  - Protection Measures
    - Encryption at the Application Level
      - Encrypts data during processing
    - Access Controls
      - Restricts access to data during processing
    - Secure Enclaves
      - Isolated environments for processing sensitive data
    - Mechanisms like INTEL Software Guard
      - Encrypts data in memory to prevent unauthorized access
- Note: Understanding the three data states (data at rest, data in transit, and data in use) and implementing appropriate security measures for each is essential for comprehensive

data protection

- **Data Types**
  - *Regulated Data*
    - Controlled by laws, regulations, or industry standards
    - Compliance requirements
      - General Data Protection Regulation (GDPR)
      - Health Insurance Portability and Accountability Act (HIPAA)
  - *PII (Personal Identification Information)*
    - Information used to identify an individual (e.g., names, social security numbers, addresses)
    - Targeted by cybercriminals and protected by privacy laws
  - *PHI (Protected Health Information)*
    - Information about health status, healthcare provision, or payment linked to a specific individual
    - Protected under HIPAA
  - *Trade Secrets*
    - Confidential business information giving a competitive edge (e.g., manufacturing processes, marketing strategies, proprietary software)
    - Legally protected; unauthorized disclosure results in penalties
  - *Intellectual Property (IP)*
    - Creations of the mind (e.g., inventions, literary works, designs)
    - Protected by patents, copyrights, trademarks to encourage innovation
    - Unauthorized use can lead to legal action
  - *Legal Information*
    - Data related to legal proceedings, contracts, regulatory compliance

        - Requires high-level protection for client confidentiality and legal privilege
    - *Financial Information*
        - Data related to financial transactions (e.g., sales records, tax documents, bank statements)
        - Targeted by cybercriminals for fraud and identity theft
        - Subject to PCI DSS (Payment Card Industry Data Security Standard)
    - *Human-Readable Data*
        - Understandable directly by humans (e.g., text documents, spreadsheets)
    - *Non-Human-Readable Data*
        - Requires machine or software to interpret (e.g., binary code, machine language)
        - Contains sensitive information and requires protection

- **Data Sovereignty**
    - *Data Sovereignty*
        - Digital information subject to laws of the country where it's located
        - Gained importance with cloud computing's global data storage
    - *GDPR (General Data Protection Regulation)*
        - Protects EU citizens' data within EU and EEA borders
        - Compliance required regardless of data location
        - Non-compliance leads to significant fines
    - Data Sovereignty Laws (e.g., China, Russia)
        - Require data storage and processing within national borders
        - Challenge for multinational companies and cloud services
    - Access Restrictions
        - Cloud services may restrict access from multiple geographic locations
    - Data sovereignty and geographical considerations pose complex challenges, but

organizations can navigate them successfully with planning, legal guidance, and strategic technology use, ensuring compliance and data protection

- **Securing Data**
  - *Geographic Restrictions (Geofencing)*
    - Virtual boundaries to restrict data access based on location
    - Compliance with data sovereignty laws
    - Prevent unauthorized access from high-risk locations
  - *Encryption*
    - Transform plaintext into ciphertext using algorithms and keys
    - Protects data at rest and in transit
    - Requires decryption key for data recovery
  - *Hashing*
    - Converts data into fixed-size hash values
    - Irreversible one-way function
    - Commonly used for password storage
  - *Masking*
    - Replace some or all data with placeholders (e.g., "x")
    - Partially retains metadata for analysis
    - Irreversible de-identification method
  - *Tokenization*
    - Replace sensitive data with non-sensitive tokens
    - Original data stored securely in a separate database
    - Often used in payment processing for credit card protection
  - *Obfuscation*
    - Make data unclear or unintelligible

        - Various techniques, including encryption, masking, and pseudonyms
        - Hinder unauthorized understanding
    - *Segmentation*
        - Divide network into separate segments with unique security controls
        - Prevent lateral movement in case of a breach
        - Limits potential damage
    - *Permission Restrictions*
        - Define data access and actions through ACLs or RBAC
        - Restrict access to authorized users
        - Reduce risk of internal data breaches

- **Data Loss Prevention (DLP)**
    - *Data Loss Prevention (DLP)*
        - Aims to monitor data in use, in transit, or at rest to detect and prevent data theft
    - DLP systems are available as software or hardware solutions
    - Types of DLP Systems
        - *Endpoint DLP System*
            - Installed as software on workstations or laptops
            - Monitors data in use on individual computers
            - Can prevent or alert on file transfers based on predefined rules
        - *Network DLP System*
            - Software or hardware placed at the network perimeter
            - Focuses on monitoring data entering and leaving the network
            - Detects unauthorized data leaving the network
        - *Storage DLP System*
            - Installed on a server in the data center

- Inspects data at rest, especially encrypted or watermarked data
- Monitors data access patterns and flags policy violations

■ *Cloud-Based DLP System*

- Offered as a software-as-a-service solution
- Protects data stored in cloud services