COMPTIA SECURITY+ (SY0-701)

CompTIA Security+ (SY0-701)

Study Notes

Introduction

- **Introduction**
  - CompTIA Security+ (SY0-701) certification is considered an intermediate level information technology certification and an entry level cyber security certification that focuses on your ability to assess the security posture of an enterprise environment
  - This certification is designed for information technology professionals or aspiring cybersecurity professionals who have already earned their CompTIA A+ and Network+ certifications, but this is a recommendation from CompTIA and not a strict requirement
    - If you have the equivalent of 1-2 years of working with hardware, software, and networks, then you will do fine in this course
  - This course is designed as a full textbook replacement, but if you would like to get a textbook to study from as well, we recommend the official CompTIA Security+ Student Guide available directly from CompTIA
  - CompTIA Security+ (SY0-701) certification exam consists of five domains or areas of knowledge
    - 12% of General Security Concepts
    - 22% of Threats, Vulnerabilities, and Mitigations
    - 18% of Security Architecture
    - 28% of Security Operations

        - 20% of Security Program Management and Oversight
    - When taking the CompTIA Security+ certification exam at the testing center or online using the web proctoring service, you are going to have 90 minutes to answer up to 90 questions
        - You're going to be answering multiple-choice questions, but you may get a few multiple-select questions where they ask you to pick 2 or 3 correct answers for a single question
        - You will also get a handful of performance-based questions
    - To pass the Security+ certification exam, you must score at least 750 points out of 900 on their 100 to 900 point scale
    - To take the exam, you do have to pay an exam fee to cover the cost of testing, and you do that by buying an exam voucher
        - How do you sign up and schedule your exam?
            - CompTIA Store
                - You can do this by going to store.comptia.org and buying it from their web store
                - The price does vary depending on which country you will be taking your exam from since CompTIA uses region based pricing
            - Dion Training
                - You can go to diontraining.com/vouchers and purchase your voucher directly from us, because we are a certified Platinum Level CompTIA Delivery Partner
                - You'll save an extra 10% or so off the regular CompTIA price
                - We'll give you free access to our searchable video library as a bonus for buying your voucher from us

- 4 tips for success in this course
  - Turn on closed captioning
  - Control the playback speed
  - Join our FB or Discord group
    - facebook.com/groups/diontraining
    - diontraining.com/discord
  - Download and print the study guide

- **Exam Tips**
  - There will be no trick questions
    - Always be on the lookout for distractors or red herrings
    - At least one of the four listed possible answer choices that are written to try and distract you from the correct answer
  - Pay close attention to words in bold, italics, or all uppercase
  - Answer the questions based on CompTIA Security+ knowledge
    - In cybersecurity, there really is no 100% correct answers in the real world because everything is situational
    - When in doubt, choose the answer that is correct for the highest number of situations
  - Understand the key concepts of the test questions
  - Do not memorize the terms word for word, try to understand them instead
  - During the exam, the answers will be from multiple-choice style questions

Fundamentals of Security

Objectives:

- 1.1 - Compare and contrast various types of security controls
- 1.2 - Summarize fundamental security concepts

- **Fundamentals of Security**
  - *Information Security*
    - Protecting data and information from unauthorized access, modification, disruption, disclosure, and destruction
  - *Information Systems Security*
    - Protecting the systems (e.g., computers, servers, network devices) that hold and process critical data
  - CIA Triad
    - *Confidentiality*
      - Ensures information is accessible only to authorized personnel (e.g., encryption)
    - *Integrity*
      - Ensures data remains accurate and unaltered (e.g., checksums)
    - *Availability*
      - Ensures information and resources are accessible when needed (e.g., redundancy measures)
  - *Non-Repudiation*
    - Guarantees that an action or event cannot be denied by the involved parties (e.g., digital signatures)

- *CIANA Pentagon*
  - An extension of the CIA triad with the addition of non-repudiation and authentication
- Triple A's of Security
  - *Authentication*
    - Verifying the identity of a user or system (e.g., password checks)
  - *Authorization*
    - Determining actions or resources an authenticated user can access (e.g., permissions)
  - *Accounting*
    - Tracking user activities and resource usage for audit or billing purposes
- Security Control Categories
  - Technical
  - Managerial
  - Operational
  - Physical
- Security Control Types
  - Preventative
  - Deterrent
  - Detective
  - Corrective
  - Compensating
  - Directive
- *Zero Trust Model*
  - Operates on the principle that no one should be trusted by default

        - To achieve zero trust, we use the control plane and the data plane
            - *Control Plane*
                - Adaptive identity, threat scope reduction, policy-driven access control, and secured zones
            - *Data Plane*
                - Subject/system, policy engine, policy administrator, and establishing policy enforcement points

- **Threats and Vulnerabilities**
    - *Threat*
        - Anything that could cause harm, loss, damage, or compromise to our information technology systems
        - Can come from the following
            - Natural disasters
            - Cyber-attacks
            - Data integrity breaches
            - Disclosure of confidential information
    - *Vulnerability*
        - Any weakness in the system design or implementation
        - Come from internal factors like the following
            - Software bugs
            - Misconfigured software
            - Improperly protected network devices
            - Missing security patches
            - Lack of physical security

- Where threats and vulnerabilities intersect, that is where the risk to your enterprise systems and networks lies
  - If you have a threat, but there is no matching vulnerability to it, then you have no risk
  - The same holds true that if you have a vulnerability but there's no threat against it, there would be no risk
- *Risk Management*
  - Finding different ways to minimize the likelihood of an outcome and achieve the desired outcome

- **Confidentiality**
  - *Confidentiality*
    - Refers to the protection of information from unauthorized access and disclosure
    - Ensure that private or sensitive information is not available or disclosed to unauthorized individuals, entities, or processes
  - Confidentiality is important for 3 main reasons
    - To protect personal privacy
    - To maintain a business advantage
    - To achieve regulatory compliance
  - To ensure confidentiality, we use five basic methods
    - *Encryption*
      - Process of converting data into a code to prevent unauthorized access
    - Access Controls
      - By setting up strong user permissions, you ensure that only authorized personnel can access certain types data

- *Data Masking*
    - Method that involves obscuring specific data within a database to make it inaccessible for unauthorized users while retaining the real data's authenticity and use for authorized users
- Physical Security Measures
    - Ensure confidentiality for both physical types of data, such as paper records stored in a filing cabinet, and for digital information contained on servers and workstations
- Training and Awareness
    - Conduct regular training on the security awareness best practices that employees can use to protect their organization's sensitive data

- **Integrity**
    - *Integrity*
        - Helps ensure that information and data remain accurate and unchanged from its original state unless intentionally modified by an authorized individual
        - Verifies the accuracy and trustworthiness of data over the entire lifecycle
    - Integrity is important for three main reasons
        - To ensure data accuracy
        - To maintain trust
        - To ensure system operability
    - To help us maintain the integrity of our data, systems, and networks, we usually utilize five methods
        - *Hashing*
            - Process of converting data into a fixed-size value

- Digital Signatures
    - Ensure both integrity and authenticity
- *Checksums*
    - Method to verify the integrity of data during transmission

- Access Controls
    - Ensure that only authorized individuals can modify data and this reduces the risk of unintentional or malicious alterations
- Regular Audits
    - Involve systematically reviewing logs and operations to ensure that only authorized changes have been made, and any discrepancies are immediately addressed

- **Availability**
    - *Availability*
        - Ensure that information, systems, and resources are accessible and operational when needed by authorized users
    - As cybersecurity professionals, we value availability since it can help us with the following
        - Ensuring Business Continuity
        - Maintaining Customer Trust
        - Upholding an Organization's Reputation
    - To overcome the challenges associated with maintaining availability, the best strategy is to use redundancy in your systems and network designs
        - *Redundancy*
            - Duplication of critical components or functions of a system with the

intention of enhancing its reliability

- There are various types of redundancy you need to consider when designing your systems and networks
  - *Server Redundancy*
    - Involves using multiple servers in a load balanced or failover configuration so that if one is overloaded or fails, the other servers can take over the load to continue supporting your end users
  - *Data Redundancy*
    - Involves storing data in multiple places
  - *Network Redundancy*
    - Ensures that if one network path fails, the data can travel through another route
  - *Power Redundancy*
    - Involves using backup power sources, like generators and UPS systems

- **Non-repudiation**
  - *Non-repudiation*
    - Focused on providing undeniable proof in the world of digital transactions
    - Security measure that ensures individuals or entities involved in a communication or transaction cannot deny their participation or the authenticity of their actions
  - *Digital Signatures*
    - Considered to be unique to each user who is operating within the digital domain
    - Created by first hashing a particular message or communication that you want to digitally sign, and then it encrypts that hash digest with the user's private key using asymmetric encryption

- Non-repudiation is important for three main reasons
  - To confirm the authenticity of digital transactions
  - To ensure the integrity of critical communications
  - To provide accountability in digital processes

- **Authentication**
  - *Authentication*
    - Security measure that ensures individuals or entities are who they claim to be during a communication or transaction
  - 5 commonly used authentication methods
    - Something you know (Knowledge Factor)
      - Relies on information that a user can recall
    - Something you have (Possession Factor)
      - Relies on the user presenting a physical item to authenticate themselves
    - Something you are (Inherence Factor)
      - Relies on the user providing a unique physical or behavioral characteristic of the person to validate that they are who they claim to be
    - Something you do (Action Factor)
      - Relies on the user conducting a unique action to prove who they are
    - Somewhere you are (Location Factor)
      - Relies on the user being in a certain geographic location before access is granted
  - *Multi-Factor Authentication System (MFA)*
    - Security process that requires users to provide multiple methods of identification to verify their identity

- Authentication is critical to understand because of the following
  - To prevent unauthorized access
  - To protect user data and privacy
  - To ensure that resources are accessed by valid users only

- **Authorization**
  - *Authorization*
    - Pertains to the permissions and privileges granted to users or entities after they have been authenticated
  - Authorization mechanisms are important to help us with the following
    - To protect sensitive data
    - To maintain the system integrity in our organizations
    - To create a more streamlined user experience

- **Accounting**
  - *Accounting*
    - Security measure that ensures all user activities during a communication or transaction are properly tracked and recorded
  - Your organization should use a robust accounting system so that you can create the following
    - Create an audit trail
      - Provides a chronological record of all user activities that can be used to trace changes, unauthorized access, or anomalies back to a source or point in time
    - Maintain regulatory compliance
      - Maintains a comprehensive record of all users' activities

- Conduct forensic analysis
    - Uses detailed accounting and event logs that can help cybersecurity experts understand what happened, how it happened, and how to prevent similar incidents from occurring again

- Perform resource optimization
    - Organizations can optimize system performance and minimize costs by tracking resource utilization and allocation decisions
- Achieve user accountability
    - Thorough accounting system ensures users' actions are monitored and logged , deterring potential misuse and promoting adherence to the organization's policies

- To perform accounting, we usually use different technologies like the following
    - *Syslog Servers*
        - Used to aggregate logs from various network devices and systems so that system administrators can analyze them to detect patterns or anomalies in the organization's systems
    - *Network Analysis Tools*
        - Used to capture and analyze network traffic so that network administrators can gain detailed insights into all the data moving within a network
    - *Security Information and Event Management (SIEM) Systems*
        - Provides us with a real-time analysis of security alerts generated by various hardware and software infrastructure in an organization

- **Security Control Categories**
  - 4 Broad Categories of Security Controls
    - *Technical Controls*
      - Technologies, hardware, and software mechanisms that are implemented to manage and reduce risks
    - *Managerial Controls*
      - Sometimes also referred to as administrative controls
      - Involve the strategic planning and governance side of security
    - *Operational Controls*
      - Procedures and measures that are designed to protect data on a day-to-day basis
      - Are mainly governed by internal processes and human actions
    - *Physical Controls*
      - Tangible, real-world measures taken to protect assets

- **Security Control Types**
  - 6 Basic Types of Security Controls
    - *Preventive Controls*
      - Proactive measures implemented to thwart potential security threats or breaches
    - *Deterrent Controls*
      - Discourage potential attackers by making the effort seem less appealing or more challenging
    - *Detective Controls*
      - Monitor and alert organizations to malicious activities as they occur or

shortly thereafter

- *Corrective Controls*
  - Mitigate any potential damage and restore our systems to their normal state
- *Compensating Controls*
  - Alternative measures that are implemented when primary security controls are not feasible or effective
- *Directive Controls*
  - Guide, inform, or mandate actions
  - Often rooted in policy or documentation and set the standards for behavior within an organization

- **Gap Analysis**
  - *Gap Analysis*
    - Process of evaluating the differences between an organization's current performance and its desired performance
  - Conducting a gap analysis can be a valuable tool for organizations looking to improve their operations, processes, performance, or overall security posture
  - There are several steps involved in conducting a gap analysis
    - Define the scope of the analysis
    - Gather data on the current state of the organization
    - Analyze the data to identify any areas where the organization's current performance falls short of its desired performance
    - Develop a plan to bridge the gap

- 2 Basic Types of Gap Analysis
  - Technical Gap Analysis
    - Involves evaluating an organization's current technical infrastructure
    - identifying any areas where it falls short of the technical capabilities required to fully utilize their security solutions
  - Business Gap Analysis
    - Involves evaluating an organization's current business processes
    - Identifying any areas where they fall short of the capabilities required to fully utilize cloud-based solutions
  - *Plan of Action and Milestones (POA&M)*
    - Outlines the specific measures to address each vulnerability
    - Allocate resources
    - Set up timelines for each remediation task that is needed

- **Zero Trust**
  - Zero Trust demands verification for every device, user, and transaction within the network, regardless of its origin
  - To create a zero trust architecture, we need to use two different planes
    - Control Plane
      - Refers to the overarching framework and set of components responsible for defining, managing, and enforcing the policies related to user and system access within an organization
      - Control Plane typically encompasses several key elements
        - *Adaptive Identity*
          - Relies on real-time validation that takes into account the user's behavior, device, location, and more

- *Threat Scope Reduction*
  - Limits the users' access to only what they need for their work tasks because this reduces the network's potential attack surface
  - Focused on minimizing the "blast radius" that could occur in the event of a breach
- *Policy-Driven Access Control*
  - Entails developing, managing, and enforcing user access policies based on their roles and responsibilities
- *Secured Zones*
  - Isolated environments within a network that are designed to house sensitive data

- Data Plane
  - Ensures the policies are properly executed
  - Data plane consists of the following
    - *Subject/System*
      - Refers to the individual or entity attempting to gain access
    - *Policy Engine*
      - Cross-references the access request with its predefined policies
    - *Policy Administrator*
      - Used to establish and manage the access policies
    - *Policy Enforcement Point*
      - Where the decision to grant or deny access is actually execute

Threat Actors

Objectives:

- 1.2 - Summarize fundamental security concepts
- 2.1 - Compare and contrast common threat actors and motivations
- 2.2 - Explain common threat vectors and attack surfaces

- **Threat Actors**
    - Threat Actor Motivations
        - Data Exfiltration
        - Blackmail
        - Espionage
        - Service Disruption
        - Financial Gain,
        - Philosophical/Political Beliefs
        - Ethical Reasons
        - Revenge
        - Disruption/Chaos
        - War
    - Threat Actor Attributes
        - Internal vs. External Threat Actors
        - Differences in resources and funding
        - Level of sophistication
    - Types of Threat Actors
        - *Unskilled Attackers*
            - Limited technical expertise, use readily available tools

- *Hacktivists*
  - Driven by political, social, or environmental ideologies
- *Organized Crime*
  - Execute cyberattacks for financial gain (e.g., ransomware, identity theft)
- *Nation-state Actor*
  - Highly skilled attackers sponsored by governments for cyber espionage or warfare
- *Insider Threats*
  - Security threats originating from within the organization

- *Shadow IT*
  - IT systems, devices, software, or services managed without explicit organizational approval
- Threat Vectors and Attack Surfaces
  - Message-based
  - Image-based
  - File-based
  - Voice Calls
  - Removable Devices
  - Unsecured Networks
- Deception and Disruption Technologies
  - *Honeypots*
    - Decoy systems to attract and deceive attackers
  - *Honeynets*
    - Network of decoy systems for observing complex attacks
  - *Honeyfiles*
    - Decoy files to detect unauthorized access or data breaches

        - *Honeytokens*
            - Fake data to alert administrators when accessed or used

- **Threat Actor Motivations**
    - There is a difference between the intent of the attack and the motivation that fuels that attack
        - *Threat Actors Intent*
            - Specific objective or goal that a threat actor is aiming to achieve through their attack
        - *Threat Actors Motivation*
            - Underlying reasons or driving forces that pushes a threat actor to carry out their attack
    - Different motivations behind threat actors
        - *Data Exfiltration*
            - Unauthorized transfer of data from a computer
        - Financial Gain
            - Achieved through various means, such as ransomware attacks, or through banking trojans that allow them to steal financial information in order to gain unauthorized access into the victims' bank accounts
        - Blackmail
            - Attacker obtains sensitive or compromising information about an individual or an organization and threatens to release this information to the public unless certain demands are met
        - Service Disruption
            - Some threat actors aim to disrupt the services of various organizations, either to cause chaos, make a political statement, or to demand a ransom

- Philosophical or Political Beliefs
    - Attacks that are conducted due to the philosophical or political beliefs of the attackers is known as hacktivism
    - Common motivation for a specific type of threat actor known as a hacktivist
- Ethical Reasons
    - Contrary to malicious threat actors, ethical hackers, also known as Authorized hackers, are motivated by a desire to improve security
- Revenge
    - It can also be a motivation for a threat actor that wants to target an entity that they believe has wronged them in some way
- Disruption or Chaos
    - Creating and spreading malware to launching sophisticated cyberattacks against the critical infrastructure in a populated city
- *Espionage*
    - Spying on individuals, organizations, or nations to gather sensitive or classified information
- War
    - Cyber warfare can be used to disrupt a country's infrastructure, compromise its national security, and to cause economic damage

- **Threat Actor Attributes**
    - 2 Most Basic Attributes of a Threat Actor
        - *Internal Threat Actors*
            - Individuals or entities within an organization who pose a threat to its security

        - *External Threat Actors*
            - Individuals or groups outside an organization who attempt to breach its cybersecurity defenses
    - Resources and funding available to the specific threat actor
        - Tools, skills, and personnel at the disposal of a given threat actor
    - Level of sophistication and capability of the specific threat actor
        - Refers to their technical skill, the complexity of the tools and techniques they use, and their ability to evade detection and countermeasures
        - In the world of cybersecurity, we usually classify the lowest skilled threat actors as "script kiddies"
            - *Script Kiddie*
                - Individual with limited technical knowledge
                - use pre-made software or scripts to exploit computer systems and networks
        - Nation-state actors, Advanced Persistent Threats and others have high levels of sophistication and capabilities and possess advanced technical skills
            - Use sophisticated tools and techniques

- **Unskilled Attackers**
    - *Unskilled Attacker (Script Kiddie)*
        - Individual who lacks the technical knowledge to develop their own hacking tools or exploits
        - These low-skilled threat actors need to rely on scripts and programs that have been developed by others
    - How do these unskilled attackers cause damage?
        - One way is to launch a DDoS attack

        - An unskilled attacker can simply enter in the IP address of the system they want to target, and then click a button to launch an attacker against that target

- **Hacktivists**
    - *Hacktivists*
        - Individuals or groups that use their technical skills to promote a cause or drive social change instead of for personal gain
    - *Hacktivism*
        - Activities in which the use of hacking and other cyber techniques is used to promote or advance a political or social cause
    - To accomplish their objectives, hacktivists use a wide range of techniques to achieve their goals
        - Website Defacement
            - Form of electronic graffiti and is usually treated as an act of vandalism
        - Distributed Denial of Service (DDoS) Attacks
            - Attempting to overwhelm the victim's systems or networks so that they cannot be accessed by the organization's legitimate users
        - *Doxing*
            - Involves the public release of private information about an individual or organization
        - Leaking of Sensitive Data
            - Releasing sensitive data to the public at large over the internet
    - Hacktivists are primarily motivated by their ideological beliefs rather than trying to achieve financial gains

- Most well-known hacktivist groups is known as "Anonymous"
  - Anonymous
    - Loosely affiliated collective that has been involved in numerous high-profile attacks over the years for targeting organizations that they perceive as acting unethically or against the public interest at large

- **Organized Crime**
  - Organized cybercrime groups are groups or syndicates that have banded together to conduct criminal activities in the digital world
    - Sophisticated and well structured
    - Use resources and technical skills for illicit gain
  - In terms of their technical capabilities, organized crime groups possess a very high level of technical capability and they often employ advanced hacking techniques and tools
    - Custom Malware
    - Ransomware
    - Sophisticated Phishing Campaigns
  - These criminal groups will engage in a variety of illicit activities to generate revenue for their members
    - Data Breaches
    - Identity Theft
    - Online Fraud
    - Ransomware Attacks
  - Unlike hacktivists or nation state actors, organized cybercrime groups are not typically driven by ideological or political objectives
    - These groups may be hired by other entities, including governments, to conduct cyber operations and attacks on their behalf

        - Money, not other motivations is the objective of their attacks even if the attack takes place in the political sphere

- **Nation-state Actor**
    - *Nation-state Actor*
        - Groups or individuals that are sponsored by a government to conduct cyber operations against other nations, organizations, or individuals
    - Sometimes, these threat actors attempt what is known as a false flag attack
        - *False Flag Attack*
            - Attack that is orchestrated in such a way that it appears to originate from a different source or group than the actual perpetrators, with the intent to mislead investigators and attribute the attack to someone else
    - Nation-state actors possess advanced technical skills and extensive resources, and they are capable of conducting complex, coordinated cyber operations that employ a variety of techniques such as
        - Creating custom malware
        - Using zero-day exploits
        - Becoming an advanced persistent threats
    - *Advanced Persistent Threat (APT)*
        - Term that used to be used synonymously with a nation-state actor because of their long-term persistence and stealth
        - A prolonged and targeted cyberattack in which an intruder gains unauthorized access to a network and remains undetected for an extended period while trying to steal data or monitor network activities rather than cause immediate damage
        - These advanced persistent threats are often sponsored by a nation-state or its proxies, like organized cybercrime groups

- What motivates a nation-state actor?
  - Nation-state actors are motivated to achieve their long-term strategic goals, and they are not seeking financial gain

- **Insider Threats**
  - *Insider Threats*
    - Cybersecurity threats that originate from within the organization
    - Will have varying levels of capabilities
  - Insider threats can take various forms
    - Data Theft
    - Sabotage
    - Misuse of access privileges
  - Each insider threat is driven by different motivations
    - Some are driven by financial gain and they want to profit from the sale of sensitive organizational data to others
    - Some may be motivated by revenge and are aiming to harm the organization due to some kind of perceived wrong levied against the insider
    - Some may take actions as a result of carelessness or a lack of awareness of cybersecurity best practices
  - <u>Remember</u>
    - Insider threat refers to the potential risk posed by individuals within an organization who have access to sensitive information and systems, and who may misuse this access for malicious or unintended purposes
    - To mitigate the risk of an insider threat being successful, organizations should implement the following
      - Zero-trust architecture

- Employ robust access controls
- Conduct regular audits
- Provide effective employee security awareness programs

- **Shadow IT**
  - *Shadow IT*
    - Use of information technology systems, devices, software, applications, and services without explicit organizational approval
    - IT-related projects that are managed outside of, and without the knowledge of, the IT department
  - Why does Shadow IT exist?
    - An organization's security posture is actually set too high or is too complex for business operations to occur without be negatively affected
  - *Bring Your Own Devices (BYOD)*
    - Involves the use of personal devices for work purposes

- **Threat Vectors and Attack Surfaces**
  - *Threat Vector*
    - Means or pathway by which an attacker can gain unauthorized access to a computer or network to deliver a malicious payload or carry out an unwanted action
  - *Attack Surface*
    - Encompasses all the various points where an unauthorized user can try to enter data to or extract data from an environment
    - Can be minimized by
      - Restricting Access

        - Removing unnecessary software
        - Disabling unused protocols
    - Think of threat vector as the "how" of an attack, whereas the attack surface is the "where" of the attack
    - Several different threat vectors that could be used to attack your enterprise networks
        - Messages
            - Message-based threat vectors include threats delivered via email, simple message service (SMS text messaging), or other forms of instant messaging
            - Phishing campaigns are commonly used as part of a message-based threat vector when an attacker impersonates a trusted entity to trick its victims into revealing their sensitive information to the attacker
        - Images
            - Image-based threat vectors involve the embedding of malicious code inside of an image file by the threat actor
        - Files
            - The files, often disguised as legitimate documents or software, can be transferred as email attachments, through file-sharing services, or hosted on a malicious website
        - Voice Calls
            - *Vhishing*
                - Use of voice calls to trick victims into revealing their sensitive information to an attacker

- Removable Devices
  - One common technique used with removable devices is known as baiting
    - *Baiting*
      - Attacker might leave a malware-infected USB drive in a location where their target might find it, such as in the parking lot or the lobby of the targeted organization
- Unsecure Networks
  - Unsecure networks includes wireless, wired, and Bluetooth networks that lack the appropriate security measures to protect these networks
  - If wireless networks are not properly secured, unauthorized individuals can intercept the wireless communications or gain access to the network
  - Wired networks tend to be more secure than their wireless networks, but they are still not immune to threats
    - Physical access to the network infrastructure can lead to various attacks
      - MAC Address Cloning
      - VLAN Hopping
  - By exploiting vulnerabilities in the Bluetooth protocol, an attacker can carry out their attacks using techniques like the BlueBorne or BlueSmack exploits
    - *BlueBorne*
      - Set of vulnerabilities in Bluetooth technology that can allow an attacker to take over devices, spread malware, or even establish an on-path attack to intercept communications without any user interaction

- *BlueSmack*
  - Type of Denial of Service attack that targets Bluetooth-enabled devices by sending a specially crafted Logical Link Control and Adaptation Protocol packet to a target device

- **Outsmarting Threat Actors**
  - One of the most effective ways to learn from the different threat actors that are attacking your network is to set up and utilize deception and disruption technologies
  - *Tactics, Techniques, and Procedures (TTPs)*
    - Specific methods and patterns of activities or behaviors associated with a particular threat actor or group of threat actors
  - *Deceptive and Disruption Technologies*
    - Technologies designed to mislead, confuse, and divert attackers from critical assets while simultaneously detecting and neutralizing threats
    - *Honeypots*
      - Decoy system or network set up to attract potential hackers
    - *Honeynets*
      - Network of honeypots to create a more complex system that is designed to mimic an entire network of systems
        - Servers
        - Routers
        - Switches
    - *Honeyfiles*
      - Decoy file placed within a system to lure in potential attackers

- *Honeytokens*
  - Piece of data or a resource that has no legitimate value or use but is monitored for access or use
- Some disruption technologies and strategies to help secure our enterprise networks
  - Bogus DNS entries
    - Fake Domain Name System entries introduced into your system's DNS server
  - Creating decoy directories
    - Fake folders and files placed within a system's storage
  - Dynamic page generation
    - Effective against automated scraping tools or bots trying to index or steal content from your organization's website
  - Use of port triggering to hide services
    - *Port Triggering*
      - Security mechanism where specific services or ports on a network device remain closed until a specific outbound traffic pattern is detected
  - Spoofing fake telemetry data
    - When a system detects a network scan is being attempted by an attacker, it can be configured to respond by sending out fake telemetry or network data

Physical Security

Objectives:

- 1.2 - Summarize fundamental security concepts
- 2.4 - Analyze indicators of malicious activity

- **Physical Security**
    - *Physical Security*
        - Measures to protect tangible assets (buildings, equipment, people) from harm or unauthorized access
    - Security Controls
        - Fencing and Bollards
            - *Bollards*
                - Short, sturdy vertical posts controlling or preventing vehicle access
            - *Fences*
                - Barriers made of posts and wire or boards to enclose or separate areas
        - Brute Force Attacks
            - Forcible entry
            - Tampering with security devices
            - Confronting security personnel
            - Ramming a barrier with a vehicle
        - *Surveillance Systems*
            - An organized strategy to observe and report activities
            - Components
                - Video surveillance

        - Security guards
        - Lighting
        - Sensors
    - *Access Control Vestibules*
        - Double-door system electronically controlled to allow only one door open at a time
        - Prevents piggybacking and tailgating
    - Door Locks
        - Padlocks
        - Pin and tumbler locks
        - Numeric locks
        - Wireless locks
        - Biometric locks
        - Cipher locks
        - Electronic access control systems
    - Access Badges
        - Use of Radio Frequency Identification (RFID) or Near Field Communication (NFC) for access

- **Fencing and Bollards**
    - Fencing and bollards stand out as some of the most primitive tools that are employed to safeguard assets and people
    - *Fence*
        - Structure that encloses an area using interconnected panels or posts
        - In terms of physical security, fences serve several purposes
            - Provides a visual deterrent by defining a boundary that should not be

violated by unauthorized personnel
        - Establish a physical barrier against unauthorized entry
        - Effectively delay intruders which helps provide our security personnel a longer window of time to react
    - *Bollards*
        - Robust, short vertical posts, typically made of steel or concrete, that are designed to manage or redirect vehicular traffic
    - Fencing is considered to be more adaptable and well-suited for safeguarding large perimeters around the entire building
    - Bollards are really designed to counter vehicular threats in a specific area instead

- **Attacking with Brute Force**
    - *Brute Force*
        - Type of attack where access to a system is gained by simply trying all of the possibilities until you break through
    - In terms of physically security, brute force focuses on the following
        - *Forcible Entry*
            - Act of gaining unauthorized access to a space by physically breaking or bypassing its barriers, such as windows, doors, or fences
            - Use high-strength doors with deadbolt locks, metal frames, or a solid core
        - Tampering with security devices
            - Involves manipulating security devices to create new vulnerabilities that can be exploited
            - To protect against tampering with security devices, have redundancy in physical security measures

- Confronting security personnel
  - Involves the direct confrontation or attack of your organization's security personnel
  - Security personnel should undergo rigorous conflict resolution and self-defense training to mitigate risks
- Ramming barriers with vehicles
  - Uses a car, truck, or other motorized vehicle to ram into the organization's physical security barriers, such as a fence, a gate, or even the side of your building
  - Install bollards or reinforced barriers to prevent vehicles from driving into your facilities

- **Surveillance Systems**
  - *Surveillance System*
    - Organized strategy or setup designed to observe and report activities in a given area
  - Surveillance is often comprised of four main categories
    - Video Surveillance
      - Can include the following
        - Motion detection
        - Night vision
        - Facial recognition
      - Remote access
      - Provides real-time visual feedback
      - A wired solution security camera is physically cabled from the device back to the central monitoring station

- A wireless solution relies on Wi-Fi to send its signal back to the central monitoring station
- *Pan-Tilt-Zoom (PTZ) System*
  - Can move the camera or its angle to better detect issues during an intrusion
- Best places to have cameras
  - Data center
  - Telecommunications closets
  - Entrance or exit areas
- Cameras should be configured to record what they're observing

- Security Guards
  - Flexible and adaptable forms of surveillance that organizations use
  - Helps to reassure your staff or your customers that they are safe
- Lighting
  - Proper lighting is crucial for conducting effective surveillance using both video and security guards
  - If you create well-lit areas, this can deter criminals, reduce shadows and hiding spots, and enhance the quality of your video recordings
- Sensors
  - Devices that detect and respond to external stimuli or changes in the environment
  - There are four categories of sensors
    - Infrared Sensors
      - Detect changes in infrared radiation that is often emitted by warm bodies like humans or animals

- Pressure Sensors
  - Activated whenever a specified minimum amount of weight is detected on the sensor that is embedded into the floor or a mat
- Microwave Sensors
  - Detect movement in an area by emitting microwave pulses and measuring their reflection off moving objects
- Ultrasonic Sensors
  - Measures the reflection of ultrasonic waves off moving objects

- **Bypassing Surveillance Systems**
  - Some of the different methods used by attackers to bypass your organization's surveillance systems
    - Visual Obstruction
      - Blocking the camera's line of sight
      - Can involve the following
        - spraying paint or foam onto the camera lens
        - placing a sticker or tape over the lens
        - positioning objects like balloons or umbrellas in front of the camera to block its view
    - Blinding Sensors and Cameras
      - Involves overwhelming the sensor or camera with a sudden burst of light to render it ineffective for a limited period of time
    - Interfering with Acoustics
      - Acoustic systems are designed to listen to the environment to detect if

someone is in the area or to eavesdrop on their conversations

- Jamming or playing loud music to disrupt the microphone's functionality

- Interfering with Electromagnetic
  - *Electromagnetic Interference (EMI)*
    - Involves jamming the signals that surveillance system relies on to monitor the environment
- Attacking the Physical Environment
  - Exploit the environment around the surveillance equipment to compromise their functionality

- Physical tampering, like cutting wires or physically disabling devices, is an effective strategy to bypass surveillance systems
- Modern systems are equipped with countermeasures to help protect surveillance systems

- **Access Control Vestibules**
  - *Access Control Vestibules*
    - Double-door system that is designed with two doors that are electronically controlled to ensure that only one door can be open at a given time
  - These access control vestibules can also help prevent piggybacking and tailgating
    - *Piggybacking*
      - Involves two people working together with one person who has legitimate access intentionally allows another person who doesn't have proper authorization to enter a secure area with them
    - *Tailgating*
      - Occurs whenever an unauthorized person closely follows someone through the access control vestibule who has legitimate access into the

secure space without their knowledge or consent

- The key difference between Piggybacking and Tailgating
  - Piggybacking uses social engineering to gain consent of the person with legitimate access
  - Tailgating doesn't use or obtain the consent of the person with legitimate access.

- Access control vestibules are usually integrated with electronic badges and operated by a security guard at the entrance to a secure facility or office building
  - Badges contain
    - RFID (Radio-Frequency Identification)
    - NFC (Near-field Communication)
    - Magnetic strips
- Security guards are often at access control vestibules because they provide
  - Visual deterrent
  - Assistance
  - Check identity
  - Response

- **Door Locks**
  - *Door Locks*
    - Critical physical security control measure designed to restrict and regulate access to specific spaces or properties, preventing unauthorized intrusions and safeguarding sensitive data and individuals
  - Types of Door Locks
    - Traditional Padlocks
      - Easily defeated and offer minimal protection

- Basic Door Locks
  - Vulnerable to simple techniques like lock picking
- Modern Electronic Door Locks
  - Utilize various authentication methods for enhanced security
  - Authentication Methods
    - Identification Numbers
      - Require entry of a unique code, providing a balance of security and convenience
    - Wireless Signals
      - Utilize technologies like NFC, Wi-Fi, Bluetooth, or RFID for unlocking
    - Biometrics
      - Rely on physical characteristics like fingerprints, retinal scans, or facial recognition for authentication
      - Biometric Challenges
        - *False Acceptance Rate (FAR)*
          - Occurs when the system erroneously authenticates an unauthorized user
          - Lower FAR by increasing scanner sensitivity
        - *False Rejection Rate (FRR)*
          - Denies access to an authorized user. Adjusting sensitivity can increase FRR
        - *Crossover Error Rate (CER)*
          - A balance between FAR and FRR for optimal authentication effectiveness

- Some electronic door locks use multiple factors, such as an identification number and fingerprint, to increase security
- *Cipher Locks*
  - Mechanical locks with numbered push buttons, requiring a correct combination to open
  - Commonly used in high-security areas like server rooms
- Secure entry areas in office buildings, often using electronic access systems with badges and PINs for authentication

- **Access Badge Cloning**
  - Radio Frequency Identification (RFID) and Near Field Communication (NFC) are popular technologies used for contactless authentication in various applications
  - *Access Badge Cloning*
    - Copying the data from an RFID or NFC card or badge onto another card or device
  - How does an attacker clone an access badge?
    - Step 1: Scanning
      - Scanning or reading the targeted individual's access badge
    - Step 2: Data Extraction
      - Attackers extract the relevant authentication credentials from the card, such as a unique identifier or a set of encrypted data
    - Step 3: Writing to a new card or device
      - Attacker will then transfers the extracted data onto a blank RFID or NFC card or another compatible device
    - Step 4: Using the cloned access badge
      - Attackers gain unauthorized access to buildings, computer systems, or even make payments using a cloned NFC-enabled credit card

- Access badge cloning is common because of its
  - Ease of execution
  - Ability to be stealthy when conducting the attack
  - Potentially widespread use in compromising physical security
- How can you stop access badge cloning?
  - Implement advanced encryption in your card-based authentication systems
  - Implement Multi-Factor Authentication (MFA)
  - Regularly update your security protocols
  - Educate your users
  - Implement the use of shielded wallets or sleeves with your RFID access badges
  - Monitor and audit your access logs

Social Engineering

Objectives:

- 2.2 - Explain common threat vectors and attack surfaces
- 5.6 - Given a scenario, you must be able to implement security awareness practices

- **Social Engineering**
  - *Social Engineering*
    - Manipulative strategy exploiting human psychology for unauthorized access to systems, data, or physical spaces
  - Motivational Triggers
    - Used by Social Engineers
      - Familiarity and Likability
      - Consensus and Social Proof
      - Authority and Intimidation
      - Scarcity and Urgency
  - Social Engineering Techniques
    - *Impersonation*
      - Pretending to be someone else
      - Includes brand impersonation, typo-squatting, and watering hole attacks
    - *Pretexting*
      - Creating a fabricated scenario to manipulate targets
      - Impersonating trusted figures to gain trust

- Types of Phishing Attacks
  - Phishing
  - Vishing
  - Smishing
  - Spear Phishing
  - Whaling
  - Business Email Compromise
- *Frauds and Scams*
  - Deceptive practices to deceive people into parting with money or valuable information
  - Identifying and training against frauds and scams
- *Influence Campaigns*
  - Spreading misinformation and disinformation, impacting politics, economics, etc.
- Other Social Engineering Attacks
  - Diversion Theft
  - Hoaxes
  - Shoulder Surfing
  - Dumpster Diving
  - Eavesdropping
  - Baiting
  - Piggybacking
  - Tailgating

- **Motivational Triggers**
  - Six main types of motivational triggers that social engineers use
    - Authority
      - Most people are willing to comply and do what you tell them to do if they believe it is coming from somebody who is in a position of authority to make that request
    - Urgency
      - Compelling sense of immediacy or time-sensitivity that drives individuals to act swiftly or prioritize certain actions
    - Social Proof
      - Psychological phenomenon where individuals look to the behaviors and actions of others to determine their own decisions or actions in similar situations
    - Scarcity
      - Psychological pressure people feel when they believe a product, opportunity, or resource is limited or in short supply
    - Likability
      - Most people want to interact with people they like, and social engineers realize this
      - Can be
        - Sexual attraction
        - Pretending to be a friend
        - Common interest
    - Fear
      - These types of attacks generally are focused on "if you don't do what I tell you, then this bad thing is going to happen to you"

- **Impersonation**
  - Four main forms of impersonation used by attackers
    - *Impersonation*
      - Attack where an adversary assumes the identity of another person to gain unauthorized access to resources or steal sensitive data
      - Requires the attacker to collect information about the organization so that they can more easily earn the trust of their targeted users
      - Attackers provide details to help make the lies and the impersonation more believable to a potential victim
      - Consequences
        - Unauthorized access
        - Disruption of services
        - Complete system takeover
      - To mitigate against these types of attacks, organizations must provide security awareness training to their employees on a regular basis so that they remain vigilant against future attacks
    - *Brand Impersonation*
      - More specific form of impersonation where an attacker pretends to represent a legitimate company or brand
      - Attackers use the brand's logos, language, and information to create deceptive communications or website
      - To protect against brand impersonation, organizations should do the following
        - Educate their users about these types of threats
        - Use secure email gateways to filter out phishing emails

        - Regularly monitor their brand's online presence to detect any fraudulent activities as soon as they occur
- *Typosquatting*
    - Also known as URL hijacking or cybersquatting
    - Form of cyber attack where an attacker will register a domain name that is similar to a popular website but contain some kind of common typographical errors
    - To combat typosquatting, organizations will often do the following
        - Register common misspellings of their own domain names
        - Use services that monitor for similar domain registrations
        - Conduct user security awareness training to educate users about the risks of typosquatting
- *Watering Hole Attacks*
    - Targeted form of cyber attack where attackers compromise a specific website or service that their target is known to use
    - The term is a metaphor for a naturally occurring phenomenon
        - In the world of cybersecurity, the "watering hole" the attacker chooses to utilize will usually be a trusted website or online service
    - To mitigate watering hole attacks, organizations should do the following
        - Keep their systems and software updated
        - Use threat intelligence services to stay informed about new threats
        - Employ advanced malware detection and prevention tools

- **Pretexting**
  - *Pretexting*
    - Gives some amount of information that seems true so that the victim will give more information
  - Mitigation involves training the employees not to fall for pretext and not to fill in the gaps for people when they are calling

- **Phishing Attacks**
  - Different Types of Phishing Attacks
    - *Phishing*
      - Sending fraudulent emails that appear to be from reputable sources with the aim of convincing individuals to reveal personal information, such as passwords and credit card numbers
    - *Spear Phishing*
      - More targeted form of phishing that is used by cybercriminals who are more tightly focused on a specific group of individuals or organizations
      - Has a higher success rate
    - *Whaling*
      - Form of spear phishing that targets high-profile individuals, like CEOs or CFOs
      - Attacker isn't trying to catch the little fish in an organization, but instead they want to catch one of the executives, board members, or higher level managers in the company since the rewards are potentially much greater
      - Often used as an initial step to compromise an executive's account for subsequent attacks within their organization

- *Business Email Compromise (BEC)*
    - Sophisticated type of phishing attack that usually targets businesses by using one of their internal email accounts to get other employees to perform some kind of malicious actions on behalf of the attacker
    - Taking over a legitimate business email accounts through social engineering or cyber intrusion techniques to conduct unauthorized fund transfers, redirect payments, or steal sensitive information
- *Vishing (Voice Phishing)*
    - Attacker tricks their victims into sharing personal or financial information over the phone
- *Smishing (SMS Phishing)*
    - Involves the use of text messages to trick individuals into providing their personal information

- **Preventing Phishing Attacks**
    - By implementing the right strategies and providing user security awareness training, the threat of a successful phishing campaign against your organization can be mitigated effectively
    - *Anti-phishing Campaign*
        - Essential user security awareness training tool that can be used to educate individuals about the risks of phishing and how to best identify potential phishing attempts
        - Should offer remedial training for users who fell victim to simulated phishing emails

- To help prevent phishing your organization should regularly conduct user security awareness training that contains coverage of the various phishing techniques
  - Phishing
  - Spear Phishing
  - Whaling
  - Business Email Compromise
  - Vishing
  - Smishing
  - Along with other relevant cyber threats and attacks that may affect your organization
- There are some commonly used key indicators that are associated with phishing attacks
  - Urgency
    - Phishing emails often create a sense of urgency by prompting the recipient to act immediately
  - Unusual Requests
    - If your receive an email requesting sensitive information, such as passwords or credit card numbers, you should treat these emails with a lot of suspicion
  - Mismatched URLs
    - When you are looking at an HTML-based email, the words you are reading are called the display text, but the underlying URL of the weblink could be set to anything you want
    - To check if the text-based link matches the underlying URL, you should always hover your mouse over the link in the email for a few seconds and this will reveal the actual URL that the link is connected to

        - Strange Email Addresses
            - If the real email address and the displayed email address don't match, then the email should be treated as suspicious and possibly part of a phishing campaign
        - Poor Spelling or Grammar
            - If an email has a lot of "broken English", poor grammar, or numerous spelling errors, it is likely to be part of a phishing campaign
    - Mitigation
        - Training
        - Report suspicious messages to protect your organization from potential phishing attacks
        - Analyze the threat
        - Inform all users about the threat
            - If the phishing email was opened, conduct a quick investigation and triage the user's system
        - An organization should revise its security measures for every success phishing attack

- **Frauds and Scams**
    - *Fraud*
        - Wrongful or criminal deception that is intended to result in financial or personal gain for the attacker
        - One of the most common types of fraud that you will see online is known as identity fraud or identity theft
            - *Identity Fraud and Identity Theft*
                - Involves the use of another person's personal information without

their authorization to commit a crime or to deceive or defraud that other person or some other third party

- Difference between identity fraud and identity theft
  - In identity fraud, the attacker takes the victim's credit card number and charges items to the card
  - In identity theft, the attacker tries to fully assume the identity of their victim

- *Scams*
  - Fraudulent or deceptive act or operation
  - Most common scam is called the invoice scam
    - *Invoice Scam*
      - In which a person is tricked into paying for a fake invoice for a product or service that they did not actually order

- **Influence Campaigns**
  - *Influence Campaigns*
    - Coordinated efforts to affect public perception or behavior towards a particular cause, individual, or group
    - Are a powerful tool for shaping public opinion and behavior
    - Foster misinformation and disinformation
  - *Misinformation*
    - False or inaccurate information shared without harmful intent
  - *Disinformation*
    - Involves the deliberate creation and sharing of false information with the intent to deceive or mislead
  - <u>Remember</u>, misinformation and disinformation can have serious consequences because

they can undermine public trust in institutions, fuel social divisions, and even influence the outcomes of elections

- **Other Social Engineering Attacks**
  - Some of the common other social engineering attacks
    - *Diversion Theft*
      - Involves manipulating a situation or creating a distraction to steal valuable items or information
    - *Hoaxes*
      - Malicious deception that is often spread through social media, email, or other communication channels
      - Often paired with phishing attacks and impersonation attacks
      - To prevent hoaxes people must fact check and use good critical thinking skills
    - *Shoulder Surfing*
      - Involves looking over someone's shoulder to gather personal information
      - Includes the use of high powered cameras or closed-circuit television cameras to steal information from a distance
      - To prevent shoulder surfing, users must be aware of their surroundings when providing any sensitive information
    - *Dumpster Diving*
      - Involves searching through trash to find valuable information
      - Commonly used to find discarded documents containing personal or corporate information
      - Use clean desk and clean desktop policies

- *Eavesdropping*
  - Involves the process of secretly listening to private conversations
  - perpetrator intercepts the communication of parties without their knowledge
  - Prevent this by encrypting data in transit
- *Baiting*
  - Involves leaving a malware-infected physical device, like a USB drive, in a place where it will be found by a victim, who will then hopefully use the device to unknowingly install malware on their organization's computer system
  - To prevent baiting, train users to not use devices they find
- *Piggybacking and Tailgating*
  - Involve an unauthorized person following an authorized person into a secure area
  - *Tailgating*
    - Attacker attempts to follow an employee through an access control vestibule or access control point without their knowledge
  - *Piggybacking*
    - Involves an attacker convincing an authorized employee to let them into the facility by getting the authorized employee to swipe their own access badge and allow the attacker inside the facility

Malware

Objective 2.4: Given a scenario, analyze indicators of malicious activity

- **Malware**
  - *Malware*
    - Malicious software designed to infiltrate computer systems and potentially damage them without user consent
  - Categories
    - Viruses
    - Worms
    - Trojans
    - Ransomware
    - Spyware
    - Rootkits
    - Spam
  - Threat Vector vs. Attack Vector
    - *Threat Vector*
      - Method used to infiltrate a victim's machine
      - Examples
        - Unpatched software
        - USB drive installation
        - Phishing campaigns
    - *Attack Vector*
      - *Means by which the attacker gains access and infects the system*
      - *Combines both infiltration method and infection process*

- Types of Malware Attacks
  - *Viruses*
    - Attach to clean files, spread, and corrupt host files
  - *Worms*
    - Standalone programs replicating and spreading to other computers
  - *Trojans*
    - Disguise as legitimate software, grant unauthorized access
  - *Ransomware*
    - Encrypts user data, demands ransom for decryption
  - *Zombies and Botnets*
    - Compromised computers remotely controlled in a network for malicious purposes
  - *Rootkits*
    - Hide presence and activities on a computer, operate at the OS level
  - *Backdoors and Logic Bombs*
    - Backdoors allow unauthorized access, logic bombs execute malicious actions
  - *Keyloggers*
    - Record keystrokes, capture passwords or sensitive information
  - *Spyware and Bloatware*
    - Spyware monitors and gathers user/system information, bloatware consumes resources without value
- Malware Techniques and Infection Vectors
  - Evolving from file-based tactics to modern fileless techniques
  - Multi-stage deployment, leveraging system tools, and obfuscation techniques

- Indications of Malware Attack
  - Recognizing signs like the following
    - Account lockouts
    - Concurrent session utilization
    - Blocked content
    - Impossible travel
    - Resource consumption
    - Inaccessibility
    - Out-of-cycle logging
    - Missing logs
    - Documented attacks

- **Viruses**
  - *Computer Virus*
    - Made up of malicious code that's run on a machine without the user's knowledge and this allows the code to infect the computer whenever it has been run
  - 10 Different Types of Viruses
    - *Boot Sector*
      - One that is stored in the first sector of a hard drive and is then loaded into memory whenever the computer boots up
    - *Macro*
      - Form of code that allows a virus to be embedded inside another document so that when that document is opened by the user, the virus is executed

- *Program*
  - Try to find executables or application files to infect with their malicious code
- *Multipartite*
  - Combination of a boot sector type virus and a program virus
  - Able to place itself in the boot sector and be loaded every time the computer boots
  - It can install itself in a program where it can be run every time the computer starts up
- *Encrypted*
  - Designed to hide itself from being detected by encrypting its malicious code or payloads to avoid detection by any antivirus software
- *Polymorphic*
  - Advanced version of an encrypted virus, but instead of just encrypting the contents it will actually change the viruses code each time it is executed by altering the decryption module in order for it to evade detection
- *Metamorphic*
  - Able to rewrite themselves entirely before it attempts to infect a given file
- *Stealth*
  - Technique used to prevent the virus from being detected by the anti-virus software
- *Armored*
  - Have a layer of protection to confuse a program or a person who's trying to analyze it
- *Hoax*
  - Form of technical social engineering that attempts to scare our end users

into taking some kind of undesirable action on their system

- **Worms**
  - *Worm*
    - Piece of malicious software, much like a virus, but it can replicate itself without any user interaction
    - Able to self-replicate and spread throughout your network without a user's consent or their action
  - Worms are dangerous for two reasons
    - Infect your workstation and other computing assets
    - Cause disruptions to your normal network traffic since they are constantly trying to replicate and spread themselves across the network
  - Worms are best known for spreading far and wide over the internet in a relative short amount of time

- **Trojans**
  - *Trojan*
    - Piece of malicious software that is disguised as a piece of harmless or desirable software
    - Claims that it will perform some needed or desired function for you
  - *Remote Access Trojan (RAT)*
    - Widely used by modern attackers because it provides the attacker with remote control of a victim machine
  - Trojans are commonly used today by attackers to exploit a vulnerability in your workstation and then conducting data exfiltration to steal your sensitive documents,

creating backdoors to maintain persistence on your systems, and other malicious activities

- **Ransomware**
  - *Ransomware*
    - Type of malicious software that is designed to block access to a computer system or its data by encrypting it until a ransom is paid to the attacker
  - How can we protect ourselves and our organizations against ransomware?
    - Always conduct regular backups
    - Install software updates regularly
    - Provide security awareness training to your users
    - Implement Multi-Factor Authentication (MFA)
  - What should you do if you find yourself or your organization as the victim of a ransomware attack?
    - Never pay the ransom
      - Paying the ransom doesn't actually guarantee that you will ever get your data back
    - If you suspect ransomware has infected your machine, you should disconnect it from the network
    - Notify the authorities
    - Restore your data and systems from known good backups

- **Zombies and Botnets**
  - *Botnet*
    - Network of compromised computers or devices controlled remotely by malicious actors

- *Zombie*
  - Name of a compromised computer or device that is part of a botnet
  - Used to perform tasks using remote commands from the attacker without the user's knowledge
- *Command and Control Node*
  - Computer responsible for managing and coordinating the activities of other nodes or devices within a network
- Botnets are used
  - as pivot points
  - disguise the real attacker
  - to host illegal activities
  - to spam others by sending out phishing campaigns and other malware
- Most common use for a botnet is to conduct a DDoS (Distributed Denial-of-Service) attack
  - *Distributed Denial-of-Service (DDoS) Attack*
    - Occurs when many machines target a single victim and attack them at the exact same time
- Botnets are used by attackers to combine processing power to break through different types of encryption schemes
- Attackers usually only use about 20-25% of any zombie's power

- **Rootkits**
  - *Rootkit*
    - Designed to gain administrative level control over a given computer system without being detected

- Account with the highest level of permissions is called the Administrator account
  - Allows the person to install programs, delete programs, open ports, shut ports, and do whatever it is they want to do on that system
  - In a UNIX, Linux, or MacOS computer, this type of administrator account is actually called the root account
- A computer system has several different rings of permissions throughout the system
  - *Ring 3 (Outermost Ring)*
    - Where user level permissions are used
  - *Ring 0 (Innermost or Highest Permission Levels)*
    - Operating in Ring 0 is called "kernel mode"
    - *Kernel Mode*
      - Allows a system to control access to things like device drivers, your sound card, your video display or monitor, and other similar things
- If you login as the administrator or root user on a system, you have root permission and you will be operating at Ring 1 of the operating system
  - <u>Remember</u>, the closer the malicious code is to the kernel, the more permissions it will have and the more damage it can cause on your system
- When a rootkit is installed on a system, it tries to move from Ring 1 to Ring 0 so that it can hide from other functions of the operating system to avoid detection
- One technique used by rootkits to gain this deeper level of access is a DLL injection
  - *DLL Injection*
    - Technique used to run arbitrary code within the address space of another process by forcing it to load a dynamic-link library
  - *Dynamic Link Library (DLL)*
    - Collection of code and data that can be used by multiple programs simultaneously to allow for code reuse and modularization in software

development

- *Shim*
  - Piece of software code that is placed between two components and that intercepts the calls between those components and can be used redirect them
- Rootkits are extremely powerful, and they are very difficult to detect because the operating system is essentially blinded to them
  - To detect them, the best way is to boot from an external device and then scan the internal hard drive to ensure that you can detect those rootkits using a good anti-malware scanning solution from a live boot Linux distribution

- **Backdoors and Logic Bombs**
  - *Backdoor*
    - Originally placed in computer programs to bypass the normal security and authentication functions
    - Most often put into systems by designers and programmers
    - Remote Access Trojan (RAT) acts just like a backdoor in our modern networks
      - Can be placed by a threat actor on your computer to help them maintain persistent access to that system
  - *Easter egg*
    - a hidden feature or novelty within a program that is typically inserted by the software developers as an inside joke
    - Code often has significant vulnerabilities
  - *Logic Bombs*
    - Malicious code that's inserted into a program, and the malicious code will only execute when certain conditions have been met

- **Keylogger**
  - *Keylogger*
    - Piece of software or hardware that records every single keystroke that is made on a computer or mobile device
  - Keyloggers can be either software-based or hardware-based
    - *Software Keyloggers*
      - Malicious programs that get installed on a victim's computer
      - Often bundled with other software or delivered through social engineering attacks, like phishing or pretexting attacks
    - *Hardware Keyloggers*
      - Physical devices that need to be plugged into a computer
      - These will resemble a USB drive or they can be embedded within a keyboard cable itself
  - To protect your organization from keyloggers, ensure the following
    - Perform regular updates and patches
    - Rely on quality antivirus and antimalware solutions
    - Conduct phishing awareness training for your users
    - Implement multi-factor authentication systems
    - Encrypt keystrokes being sent to your systems
    - Perform physical checks of your desktops, laptops, and servers

- **Spyware and Bloatware**
  - *Spyware*
    - Malicious software that is designed to gather and send information about a user or organization without their knowledge

- Spyware can get installed on a system in several different ways
  - Bundled with other software
  - Installed through a malicious website
  - Installed when users click on a deceptive pop-up advertisement
- To help protect yourself against spyware, you should only use reputable antivirus and anti-spyware tools that are regularly updated detect and remove any potential threats

- *Bloatware*
  - Any software that comes pre-installed on a new computer or smartphone that you, as the user, did not specifically request, want, or need
  - Other examples of bloatware are things like unnecessary toolbars or applications that promote certain services
  - Bloatware isn't malicious, but it can
    - waste your storage space
    - slow down the performance of your devices
    - introduce security vulnerabilities into your systems
  - <u>Remember</u>, anytime a piece of software is installed, that is one more potential threat vector for an attacker to exploit if you don't properly update that application
  - To remove bloatware, you can either do the following
    - Do a manual removal process
    - Use bloatware removal tools to uninstall the unwanted applications
    - Perform a clean operating system installation

- **Malware Attack Techniques**
  - *Malware Exploitation Technique*
    - Specific method by which malware code penetrates and infects a targeted system
  - Some malware focuses on infecting the system's memory to leverage remote procedure calls over the organization's network
    - Most modern malware uses fileless techniques to avoid detection by signature-based security software
    - Fileless Malware is used to create a process in the system memory without relying on the local file system of the infected host
  - How does this modern malware work?
    - When a user accidentally clicks on a malicious link or opens a malicious file, the specific type of malware being installed is known as a stage one dropper or downloader
      - *Stage 1 Dropper or Downloader*
        - Piece of malware that is usually created as a lightweight shellcode that can be executed on a given system
      - *Dropper*
        - Specific malware type designed to initiate or run other malware forms within a payload on an infected host
      - *Downloader*
        - Retrieve additional tools post the initial infection facilitated by a dropper
      - The primary function of a stage one dropper or downloader is to retrieve additional portions of the malware code and to trick the user into activating it

- *Shellcode*
    - Broader term that encompasses lightweight code meant to execute an exploit on a given target
- *Stage 2: Downloader*
    - Downloads and installs a remote access Trojan to conduct command and control on the victimized system
- "Actions on Objectives" Phase
    - Threat actors will execute primary objectives to meet core objectives like
        - data exfiltration
        - file encryption
- Concealment
    - Used to help the threat actor prolong unauthorized access to a system by
        - hiding tracks
        - erasing log files
        - hiding any evidence of malicious activity
    - *"Living off the Land"*
        - A strategy adopted by many Advanced Persistent Threats and criminal organizations
        - the threat actors try to exploit the standard tools to perform intrusions

- **Indications of Malware Attacks**
  - 9 Common Indicators of Malware Attacks
    - *Account Lockouts*
      - Malware, especially those designed for credential theft or brute force attacks, can trigger multiple failed login attempts that would result in a user's account being locked out
    - Concurrent Session Utilization
      - If you notice that a single user account has multiple simultaneous or concurrent sessions open, especially from various geographic locations
    - Blocked Content
      - If there is a sudden increase in the amount of blocked content alerts you are seeing from your security tools
    - *Impossible Travel*
      - Refers to a scenario where a user's account is accessed from two or more geographically separated locations in an impossibly short period of time
    - Resource Consumption
      - If you are observing any unusual spikes in CPU, memory, or network bandwidth utilization that cannot be linked back to a legitimate task
    - Resource Inaccessibility
      - *Ransomware*
        - Form of malware that encrypts user files to make them inaccessible to the user
      - If a large number of files or critical systems suddenly become inaccessible or if users receive messages demanding payment to decrypt their data

- Out-of-Cycle Logging
  - If you are noticing that your logs are being generated at odd hours or during times when no legitimate activities should be taking place (such as in the middle of the night when no employees are actively working)
- Missing Logs
  - If you are conducting a log review as a cybersecurity analyst and you see that there are gaps in your logs or if the logs have been cleared without any authorized reason
- Published or Documented Attacks
  - If a cybersecurity research or reporter published a report that shows that your organization's network has been infected as part of a botnet or other malware-based attack

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
  - <u>Note</u>: 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
- <u>Note</u>: 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

Cryptographic Solutions

Objectives:

- 1.4 - Explain the importance of using appropriate cryptographic solutions
- 2.3 - Explain various types of vulnerabilities
- 2.4 - Given a scenario, you must be able to analyze indicators of malicious activity

- **Cryptographic Solutions**
    - *Cryptography*
        - Practice and study of writing and solving codes
        - Encryption to hide information's true meaning
    - *Encryption*
        - Converts plaintext to ciphertext
        - Provides data protection at rest, in transit, and in use
    - Data States
        - *Data at Rest*
            - Inactive data on storage devices
        - *Data in Transit*
            - Moving across networks
        - *Data in Use*
            - Currently undergoing change
    - Algorithm and Key
        - *Algorithm (Cipher)*
            - Performs encryption or decryption

        - *Key*
            - Essential for determining cipher output
    - Key Strength and Rotation
        - *Key Length*
            - Proportional to security
        - *Key Rotation*
            - Best practice for security longevity
    - Symmetric and Asymmetric Encryption
        - *Symmetric*
            - Uses same key for encryption and decryption
        - *Asymmetric*
            - Uses a pair of keys for encryption and decryption
    - Symmetric Algorithms
        - DES
        - Triple DES
        - IDEA
        - AES
        - Blowfish
        - Twofish
        - Rivest Cipher
    - Asymmetric Algorithms
        - Diffie-Hellman
        - RSA
        - Elliptic Curve Cryptography
    - *Hashing*
        - Converts data into fixed-size string (digest) using hash functions

        - Algorithms
            - MD5
            - SHA Family
            - RIPEMD
            - HMAC
    - *Public Key Infrastructure (PKI)*
        - Framework managing digital keys and certificates for secure data transfer
    - *Digital Certificates*
        - Electronic credentials verifying entity identity for secure communications
    - *Blockchain*
        - Decentralized, immutable ledger ensuring data integrity and transparency
    - Encryption Tools
        - TPM
        - HSM
        - Key Management Systems
        - Secure Enclave
    - Obfuscation
        - Steganography
        - Tokenization
        - Data Masking
    - Cryptographic Attacks
        - Downgrade Attacks
        - Collision Attacks
        - Quantum Computing Threats

- **Symmetric vs Asymmetric**
  - *Symmetric Encryption*
    - Uses a single key for both encryption and decryption
    - Often referred to as private key encryption
    - Requires both sender and receiver to share the same secret key
    - Offers confidentiality but lacks non-repudiation
    - Challenges with key distribution in large-scale usage
      - More people means more sharing of the keys
  - *Asymmetric Encryption*
    - Uses two separate keys
      - Public key for encryption
      - Private key for decryption
    - Often called "Public Key Cryptography"
    - No need for shared secret keys
    - Commonly used algorithms include Diffie-Hellman, RSA, and Elliptic Curve Cryptography (ECC)
    - Slower compared to symmetric encryption but solves key distribution challenges
  - *Hybrid Approach*
    - Combines both symmetric and asymmetric encryption for optimal benefits
    - Asymmetric encryption used to encrypt and share a secret key
    - Symmetric encryption used for bulk data transfer, leveraging the shared secret key
    - Offers security and efficiency
  - *Stream Cipher*
    - Encrypts data bit-by-bit or byte-by-byte in a continuous stream
    - Uses a keystream generator and exclusive XOR function for encryption

        - Suitable for real-time communication data streams like audio and video
        - Often used in symmetric algorithms
    - *Block Cipher*
        - Breaks input data into fixed-size blocks before encryption
            - Usually 64, 128, or 256 bits at a time
        - Padding added to smaller data blocks to fit the fixed block size
        - Advantages include ease of implementation and security
        - Can be implemented in software, whereas stream ciphers are often used in hardware solutions

- **Symmetric Algorithms**
    - *DES (Data Encryption Standard)*
        - Uses a 64-bit key (56 effective bits due to parity)
        - Encrypts data in 64-bit blocks through 16 rounds of transposition and substitution
        - Widely used from the 1970s to the early 2000s
    - *Triple DES (3DES)*
        - Utilizes three 56-bit keys
        - Encrypts data with the first key, decrypts with the second key, and encrypts again with the third key
        - Provides 112-bit key strength but is slower than DES
    - *IDEA (International Data Encryption Algorithm)*
        - A symmetric block cipher with a 64-bit block size
        - Uses a 128-bit key, faster and more secure than DES
        - Not as widely used as AES

- *AES (Advanced Encryption Standard)*
  - Replaced DES and 3DES as the US government encryption standard
  - Supports 128-bit, 192-bit, or 256-bit keys and matching block sizes
  - Widely adopted and considered the encryption standard for sensitive unclassified information
- *Blowfish*
  - A block cipher with key sizes ranging from 32 to 448 bits
  - Developed as a DES replacement but not widely adopted
- *Twofish*
  - A block cipher supporting 128-bit block size and key sizes of 128, 192, or 256 bits
  - Open source and available for use
- *RC Cipher Suite (RC4, RC5, RC6)*
  - Created by cryptographer, Ron Rivest
  - RC4 is a stream cipher with variable key sizes from 40 to 2048 bits, used in SSL and WEP
  - RC5 is a block cipher with key sizes up to 2048 bits
  - RC6, based on RC5, was considered as a DES replacement
- Classification
  - All the mentioned algorithms are symmetric
  - Most are block ciphers except for RC4, which is a stream cipher
- <u>Note</u>: When working with encryption, identify if it's symmetric or asymmetric and whether it's a block or stream cipher

- **Asymmetric Algorithms**
  - Public Key Cryptography
    - No shared secret key required

        - Uses a key pair
            - Public key for encryption
            - Private key for decryption
        - Provides confidentiality, integrity, authentication, and non-repudiation
    - Confidentiality with Public Key
        - Encrypt data using the receiver's public key
        - Only the recipient with the corresponding private key can decrypt it
    - Non-Repudiation with Private Key
        - Encrypt data using the sender's private key
        - Anyone with access to the sender's public key can verify the sender's identity
    - Integrity and Authentication with Digital Signature
        - Create a hash digest of the message
        - Encrypt the hash digest with the sender's private key
            - *Digital Signature*
                - A hash digest of a message encrypted with the sender's private key to let the recipient know the document was created and sent by the person claiming to have sent it
        - Encrypt the message with the receiver's public key
        - Ensures message integrity, non-repudiation, and confidentiality
    - Common Asymmetric Algorithms
        - *Diffie-Hellman*
            - Used for key exchange and secure key distribution
            - Vulnerable to man-in-the-middle attacks, requires authentication
            - Commonly used in VPN tunnel establishment (IPSec)
        - *RSA (Ron Rivest, Adi Shamir, Leonard Adleman)*
            - Used for key exchange, encryption, and digital signatures

        - Relies on the mathematical difficulty of factoring large prime numbers
        - Supports key sizes from 1024 to 4096 bits
        - Widely used in organizations and multi-factor authentication
    - *Elliptic Curve Cryptography (ECC)*
        - Efficient and secure, uses algebraic structure of elliptical curves
        - Commonly used in mobile devices and low-power computing
        - Six times more efficient than RSA for equivalent security
        - Variants include
            - ECDH (Elliptic Curve Diffie-Hellman)
            - ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)
            - ECDSA (Elliptic Curve Digital Signature Algorithm)

- **Hashing**
    - *Hashing*
        - One-way cryptographic function that produces a unique message digest from an input
    - *Hash Digest*
        - Like a digital fingerprint for the original data
        - Always of the same length regardless of the input's length
    - Common Hashing Algorithms
        - *MD5 (Message Digest Algorithm 5)*
            - Creates a 128-bit hash value
            - Limited unique values, leading to collisions
            - Not recommended for security-critical applications due to vulnerabilities

- SHA (Secure Hash Algorithm) Family
  - *SHA-1*
    - Produces a 160-bit hash digest, less prone to collisions than MD5
  - *SHA-2*
    - Offers longer hash digests (SHA-224, SHA-256, SHA-348, SHA-512)
  - *SHA-3*
    - Uses 224-bit to 512-bit hash digests, more secure, 120 rounds of computations
- *RIPEMD (RACE Integrity Primitive Evaluation Message Digest)*
  - Versions available
    - 160-bit (Most common)
    - 256-bit
    - 320-bit
  - Open-source competitor to SHA but less popular
- *HMAC (Hash-based Message Authentication Code)*
  - Checks message integrity and authenticity
  - Utilizes other hashing algorithms (e.g., HMAC-MD5, HMAC-SHA1, HMAC-SHA256)

- *Digital Signatures*
  - Uses a hash digest encrypted with a private key
  - Sender hashes the message and encrypts the hash with their private key
  - Recipient decrypts the digital signature using the sender's public key
  - Verifies integrity of the message and ensures non-repudiation
- Common Digital Signature Algorithms
  - *DSA (Digital Security Algorithm)*
    - Utilized for digital signatures

            - Uses a 160-bit message digest created by DSS (Digital Security Standard)
        - *RSA (Rivest-Shamir-Adleman)*
            - Supports digital signatures, encryption, and key distribution
            - Widely used in various applications, including code signing
    - Hashes change drastically even with minor changes in input
    - Hashing is used to verify data integrity and detect any changes

- **Increasing Hash Security**
    - Common Hashing Attacks
        - *Pass the Hash Attack*
            - A hacking technique that allows the attacker to authenticate to a remote server or service by using the underlying hash of a user's password instead of requiring the associated plaintext password
            - Hashes can be obtained by attackers to impersonate users without cracking the password
            - Difficult to defend against due to various Windows vulnerabilities and applications
            - Penetration tools like Mimikatz automate hash harvesting
            - Prevention
                - Ensure trusted OS
                - Proper Windows domain trusts
                - Patching
                - Multi-factor authentication
                - Least privilege

- *Birthday Attack*
  - Occurs when two different messages result in the same hash digest (collision)
  - Named after the Birthday Paradox, where shared birthdays become likely in a group
  - Collisions in hashes can be exploited by attackers to bypass authentication systems
  - Use longer hash output (e.g., SHA-256) to reduce collisions and mitigate the attack
- Increasing Hash Security
  - *Key Stretching*
    - Technique that is used to mitigate a weaker key by creating longer, more secure keys (at least 128 bits)
      - increases the time needed to crack the key
    - Used in systems like Wi-Fi Protected Access, Wi-Fi Protected Access version 2, and Pretty Good Privacy
  - *Salting*
    - Adds random data (salt) to passwords before hashing
    - Ensures distinct hash outputs for the same password due to different salts
    - Thwarts dictionary attacks, brute-force attacks, and rainbow tables
  - *Nonces (Number Used Once)*
    - Adds unique, often random numbers to password-based authentication processes
    - Prevents attackers from reusing stolen authentication data
    - Adds an extra layer of security against replay attacks

        - Limiting Failed Login Attempts
            - Restricts the number of incorrect login attempts a user can make
            - Increases security by deterring attackers attempting to guess passwords
            - Typically, lock the account after three incorrect attempts

- **Public Key Infrastructure (PKI)**
    - PKI Components
        - An entire system involving hardware, software, policies, procedures, and people
        - Based on asymmetric encryption
        - Facilitates secure data transfer, authentication, and encrypted communications
        - Used in HTTPS connections on websites
    - Establishing a Secure Connection
        - User connects to a website via HTTPS
        - Web browser contacts a trusted certificate authority for the web server's public key
        - A random shared secret key is generated for symmetric encryption
        - The shared secret is securely transmitted using public key encryption
        - The web server decrypts the shared secret with its private key
        - Both parties use the shared secret for symmetric encryption (e.g., AES) to create a secure tunnel
    - Security Benefits
        - Confidentiality
            - Data is encrypted using a shared secret
        - Authentication
            - The web server's identity is verified using its private key

        - Visual indicators like a padlock show secure communication
    - Public Key Infrastructure vs. Public Key Cryptography
        - *Public Key Infrastructure (PKI)*
            - Encompasses the entire system for managing key pairs, policies, and trust
            - Involves generating, validating, and managing public and private key pairs that are used in the encryption and decryption process
            - Ensures the security and trustworthiness of keys
        - *Public Key Cryptography*
            - Refers to the encryption and decryption process using public and private keys
            - Only a part of the overall PKI architecture
    - *Key Escrow*
        - Storage of cryptographic keys in a secure, third-party location (escrow)
        - Enables key retrieval in cases of key loss or for legal investigations
        - Relevance in PKI
            - In PKI, key escrow ensures that encrypted data is not permanently inaccessible
            - Useful when individuals or organizations lose access to their encryption keys
        - Security Concerns
            - Malicious access to escrowed keys could lead to data decryption
            - Requires stringent security measures and access controls

- **Digital Certificates**
    - *Digital Certificates*
        - Digitally signed electronic documents

- Bind a public key with a user's identity
- Used for individuals, servers, workstations, or devices
- Use the *X.509 Standard*
  - Commonly used standard for digital certificates within PKI
  - Contains owner's/user's information and certificate authority details

- Types of Digital Certificates
  - *Wildcard Certificate*
    - Allows multiple subdomains to use the same certificate
    - Easier management, cost-effective for subdomains
    - Compromise affects all subdomains
  - *SAN (Subject Alternate Name) field*
    - Certificate that specifies what additional domains and IP addresses are going to be supported
    - Used when domain names don't have the same root domain
  - Single-Sided and Dual-Sided Certificates
    - *Single-sided*
      - Only requires the server to be validated
    - *Dual-sided*
      - Both server and user validate each other
      - Dual-sided for higher security, requires more processing power
  - *Self-Signed Certificates*
    - Digital certificate that is signed by the same entity whose identity it it certifies
    - Provides encryption but lacks third-party trust
    - Used in testing or closed systems
  - *Third-Party Certificates*

        - Digital certificate issued and signed by trusted certificate authorities (CAs)
        - Trusted by browsers and systems
        - Preferred for public-facing websites
    - Key Concepts
        - *Root of Trust*
            - Highest level of trust in certificate validation
            - Trusted third-party providers like Verisign, Google, etc.
            - Forms a certification path for trust
        - *Certificate Authority (CA)*
            - Trusted third party that issues digital certificates
            - Certificates contain CA's information and digital signature
            - Validates and manages certificates
        - *Registration Authority (RA)*
            - Requests identifying information from the user and forwards certificate request up to the CA to create a digital certificate
            - Collects user information for certificates
            - Assists in the certificate issuance process
        - *Certificate Signing Request (CSR)*
            - A block of encoded text with information about the entity requesting the certificate
            - Includes the public key
            - Submitted to CA for certificate issuance
            - Private key remains secure with the requester
        - *Certificate Revocation List (CRL)*
            - Maintained by CAs
            - List of all digital certificates that the certificate authority has already

revoked

- Checked before validating a certificate

- *Online Certificate Status Protocol (OCSP)*
  - Determines certificate revocation status or any digital certificate using the certificate's serial number
  - Faster but less secure than CRL
- *OCSP Stapling*
  - Alternative to OCSP
  - Allows the certificate holder to get the OCSP record from the server at regular intervals
  - Includes OCSP record in the SSL/TLS handshake
  - Speeds up the secure tunnel creation
- *Public Key Pinning*
  - Allows an HTTPS website to resist impersonation attacks from users who are trying to present fraudulent certificates
  - Presents trusted public keys to browsers
  - Alerts users if a fraudulent certificate is detected
- *Key Escrow Agents*
  - Securely store copies of private keys
  - Ensures key recovery in case of loss
  - Requires strong access controls
- *Key Recovery Agents*
  - Specialized type of software that allows the restoration of a lost or or corrupted key to be performed
  - Acts as a backup for certificate authority keys

- Trust in Digital Certificates

        - Trust is essential in digital certificates
        - Compromised root CAs can impact all issued certificates
        - Commercially trusted CAs are more secure
        - Self-managed CAs must be vigilant against compromises

- **Blockchain**
    - *Blockchain*
        - Shared immutable ledger for transactions and asset tracking
        - Builds trust and transparency
        - Widely associated with cryptocurrencies like Bitcoin
        - Is essentially a really long series of information with each block containing information in it
            - Each block has the hash for the block before it
        - Block Structure
            - Chain of blocks, each containing
                - Previous block's hash
                - Timestamp
                - Root transactions (hashes of individual transactions)
            - Blocks are linked together in a chronological order
        - *Public Ledger*
            - Secure and anonymous record-keeping system
            - Maintains participants' identities
            - Tracks cryptocurrency balances
            - Records all genuine transactions in a network
    - Blockchain Applications
        - *Smart Contracts*

        - Self-executing contracts with code-defined terms
        - Execute actions automatically when conditions are met
        - Transparent, tamper-proof, and trust-enhancing
    - Commercial Uses
        - Companies like IBM promote blockchain for commercial purposes
        - Permissioned blockchain used for business transactions
        - Enhances trust and transparency with immutable public ledger
    - *Supply Chain Management*
        - Transparency and traceability in the supply chain
        - Immutable records of product origin, handling, and distribution
        - Ensures compliance and quality control
- Broad Implications of Blockchain
    - Versatility
        - Beyond finance and cryptocurrencies
        - Applications across various industries
        - Promises transparency, efficiency, and trust
    - Decentralization
        - Key feature of blockchain
        - Eliminates need for central authorities
        - Empowers peer-to-peer networks
    - Immutable Ledger
        - Ensures data integrity
        - Records cannot be altered or deleted
        - Reinforces trust in transactions and information
    - Digital Evolution
        - Blockchain's impact on technology and industries

        - Potential to reshape traditional systems
        - Offers transparency, efficiency, and trust in the digital era

- **Encryption Tools**
    - Encryption Tools for Data Security
        - *TPM (Trusted Platform Module)*
            - Dedicated microcontroller for hardware-level security
            - Protects digital secrets through integrated cryptographic keys
            - Used in BitLocker drive encryption for Windows devices
            - Adds an extra layer of security against software attacks
        - *HSM (Hardware Security Module)*
            - Physical device for safeguarding and managing digital keys
            - Ideal for mission-critical scenarios like financial transactions
            - Performs encryption operations in a tamper-proof environment
            - Ensures key security and regulatory compliance
        - *Key Management System*
            - Manages, stores, distributes, and retires cryptographic keys
            - Centralized mechanism for key lifecycle management
            - Crucial for securing data and preventing unauthorized access
            - Automates key management tasks in complex environments
        - *Secure Enclaves*
            - Coprocessor integrated into the main processor of some devices
            - Isolated from the main processor for secure data processing and storage
            - Safeguards sensitive data like biometric information
            - Enhances device security by preventing unauthorized access

- **Obfuscation**
  - Obfuscation Techniques in Data Security
    - *Steganography*
      - Conceals a message within another to hide its very existence
      - Involves altering image or data elements to embed hidden information
      - Primary goal is to prevent the suspicion that there's any hidden data at all
      - Used alongside encryption for added security
      - Detection is challenging due to hiding data in plain sight
    - *Tokenization*
      - Substitutes sensitive data with non-sensitive tokens
      - Original data securely stored elsewhere
      - Tokens have no intrinsic value
      - Reduces exposure of sensitive data during transactions
      - Commonly used for payment systems to comply with security standards
    - *Data Masking (Data Obfuscation)*
      - Disguises original data to protect sensitive information
      - Maintains data authenticity and usability
      - Used in testing environments, especially for software development
      - Reduces the risk of data breaches in non-production settings
      - Common in industries handling personal data
      - Masks portions of sensitive data for privacy, e.g., credit card digits, social security numbers

- **Cryptographic Attacks**
  - *Cryptographic Attacks*

        - Techniques and strategies that adversaries employ to exploit vulnerabilities in cryptographic systems with the intent to compromise the confidentiality, integrity, or authenticity of data
    - *Downgrade Attacks*
        - Force systems to use weaker or older cryptographic standards or protocols
        - Exploit known vulnerabilities or weaknesses in outdated versions
        - Example: POODLE attack on SSL 3.0
        - Countermeasures include phasing out support for insecure protocols and version-intolerant checks
    - *Collision Attacks*
        - Find two different inputs producing the same hash output
        - Undermine data integrity verification relying on hash functions
        - Vulnerabilities in hashing algorithms, e.g., MD5, can lead to collisions
        - Birthday Paradox or Birthday Attack
            - The probability that two distinct inputs, when processed through a hashing function, will produce the same output, or a collision
    - *Quantum Computing Threat*
        - *Quantum computing*
            - A computer that uses quantum mechanics to generate and manipulate quantum bits in order to access enormous processing powers.
            - Uses quantum bits (qubits) instead of using ones and zeros
        - *Quantum Communication*
            - A communications network that relies on qubits made of photons (light) to send multiple combinations of ones and zeros simultaneously which results in tamper resistant and extremely fast communications
        - *Qubit*

    - A quantum bit composed of electrons or photons that can represent numerous combinations of ones and zeros at the same time through superposition
    - Enable simultaneous processing of multiple combinations
- Quantum computing is designed for very specific use cases
    - Complex math problems
    - Trying to do something like the modeling of an atom or atomic structure
- Threat to traditional encryption algorithms (RSA, ECC) by rapid factorization of large prime numbers
- *Post-quantum cryptography*
    - A new kind of cryptographic algorithm that can be implemented using today's classic computers but is also impervious to attacks from future quantum computers
    - Aims to create algorithms resistant to quantum attacks
    - First method is to create post-quantum cryptography is to increase the key size
        - Increases the number of permutations that are needed to be brute-forced
    - Second method is to create something like lattice-based cryptography and super singular isogeny key exchange
- NIST selected four post-quantum cryptography standards
    - CRYSTALS-Kyber - general encryption needs
    - Digital signatures
        - CRYSTALS-Dilithium
        - FLACON
        - SPHINCS+

Risk Management

Objective 5.2: Explain elements of the risk management process

- **Risk Management**
  - *Risk Management*
    - Fundamental process involving identification, analysis, treatment, monitoring, and reporting of risks
  - Risk Management Lifecycle
    - *Risk Identification*
      - Proactive process recognizing potential risks
      - Goal
        - Create a comprehensive list based on events hindering objectives
    - *Risk Analysis*
      - Evaluate likelihood and potential impact
      - Qualitative or quantitative methods
      - Outcome
        - Prioritized list for guiding risk treatment
    - *Risk Treatment*
      - Develop strategies
        - Avoidance
        - Reduction
        - Sharing
        - Acceptance

- Strategy choice based on potential impact and risk tolerance
- Goal
  - Reduce potential impact to an acceptable level

- *Risk Monitoring*
  - Ongoing process tracking identified risks
  - Monitor residual risks, identify new risks, and review risk management effectiveness
  - Ensures dynamic responsiveness to organizational changes
- *Risk Reporting*
  - Communicate risk information and effectiveness of risk management to stakeholders
  - Various forms
    - Dashboards
    - Heat Maps
    - Detailed Reports
  - Crucial for accountability and informed decision-making

- Risk Assessment Frequency
  - Types
    - Ad-hoc
    - Recurring
    - One-time
    - Continuous
  - Varies
    - Based on organization nature and types of risks involved

- Risk Identification
  - Process
    - Identify potential risks; perform business impact analysis.
  - Concepts
    - Recovery Time Objective
    - Recovery Point Objective
    - Mean Time to Repair
    - Mean Time Before Failure
- *Qualitative Risk Analysis*
  - Assess and prioritize risks based on likelihood and impact
- *Quantitative Risk Analysis*
  - Numerically estimate probability and potential impact
- Risk Management Strategies
  - Types
    - Risk Transfer
    - Risk Acceptance
    - Risk Avoidance
    - Risk Mitigation
- Risk Monitoring and Reporting
  - Crucial Steps
    - Continuous tracking and regular reporting
  - Long-Term Impact
    - Significant for the effectiveness of the risk management process

- **Risk Assessment Frequency**
  - *Risk Assessment Frequency*
    - Regularity with which risk assessments are conducted within an organization
  - Four main types of risk assessment frequencies
    - *Ad-Hoc Risk Assessments*
      - Conducted as needed, often in response to specific events or situations
      - Address potential new risks or changes in existing risks
    - *Recurring Risk Assessments*
      - Conducted at regular intervals (e.g., annually, quarterly, monthly)
      - Part of standard operating procedures for continual risk identification and management
    - *One-Time Risk Assessments*
      - Conducted for specific projects or initiatives
      - Not repeated, associated with a particular purpose
    - *Continuous Risk Assessments*
      - Ongoing monitoring and evaluation of risks
      - Enabled by technology, involving real-time data collection and analysis
      - Used for proactive threat and vulnerability monitoring, facilitating quick responses

- **Risk Identification**
  - *Risk Identification*
    - Crucial first step in risk management
    - Involves recognizing potential risks that could impact an organization
    - Risks can vary from financial and operational to strategic and reputational

- Techniques
  - Brainstorming
  - Checklists
  - Interviews
  - Scenario Analysis
- Organization should consider a wide range of risks, including operational, financial, strategic, and reputational risks
- Document and analyze risks based on impact and likelihood

- *Business Impact Analysis (BIA)*
  - Evaluates effects of disruptions on business functions
  - Identifies and prioritizes critical functions
  - Assesses impact of risks on functions
  - Determines required recovery time for functions
  - Key Metrics in BIA
    - *Recovery Time Objective (RTO)*
      - Maximum acceptable time before severe impact
      - Target time for restoring a business process
    - *Recovery Point Objective (RPO)*
      - Maximum acceptable data loss measured in time
      - Point in time data must be restored to
    - *Mean Time to Repair (MTTR)*
      - Average time to repair a failed component or system
      - Indicator of repair speed and downtime minimization
    - *Mean Time Between Failures (MTBF)*
      - Average time between system or component failures
      - Measure of reliability

- **Risk Register**
  - *Risk Management*
    - Crucial for projects and business, it involves the identification and assessment of uncertainties that may impact objectives
  - *Risk Register*
    - Records identified risks, descriptions, impacts, likelihoods, and mitigation actions
    - Key tool in risk management
    - May resemble a heat map risk matrix
    - Facilitates communication and risk tracking
    - Key component of project and business operations
  - Components of Risk Register
    - *Risk Description*
      - Identifies and describes the risk
      - Clear and concise description
    - *Risk Impact*
      - Potential consequences of risk occurrence
      - Rated on a scale (e.g., low, medium, high)
    - *Risk Likelihood*
      - Probability of risk occurrence
      - Rated on a scale (e.g., numerical or descriptive)
    - *Risk Outcome*
      - Result of the risk if it occurs
      - Related to impact and likelihood
    - *Risk Level or Threshold*
      - Determined by combining the impact and likelihood

        - Prioritizes risks (e.g., high, medium, low)
    - *Cost*
        - Financial impact on the project
        - includes potential expenses if it occurs or the cost of risk mitigation
  - Risk Tolerance and Risk Appetite
    - *Risk Tolerance/Risk Acceptance*
        - An organization or individual's willingness to deal with uncertainty in pursuit of their goals
        - Maximum amount of risk they are willing to accept
        - Acceptance without countermeasures
    - *Risk Appetite*
        - Willingness to pursue or retain risk
        - Types
            - Expansionary
            - Conservative
            - Neutral
  - *Key Risk Indicators (KRIs)*
    - Predictive metrics signaling increasing risk exposure
    - Provide early warning of potential risks
    - Tied to the organization's objectives
    - Used to monitor risk changes and take proactive steps
  - *Risk Owner*
    - Responsible for managing the risk
    - Monitors, implements mitigation actions, and updates Risk Register
    - Accountable for risk management

- **Qualitative Risk Analysis**
  - *Qualitative Risk Analysis*
    - Primary method in risk management
    - Assesses risks based on potential impact and likelihood
    - Categorizes risks as high, medium, or low
    - Subjective and relies on expertise and experience
    - Avoids quantitative complexity
  - Key Components
    - *Likelihood/Probability*
      - Chance of risk occurrence
      - Qualitatively expressed as low, medium, or high
      - Based on past experience, statistical analysis, or expert judgment
    - *Impact*
      - Potential consequences if risk occurs
      - Qualitatively rated as low, medium, or high
      - Assess damage to project or business objectives
      - Impact Levels
        - *Low Impact*
          - Minor damage, essential functions operational
        - *Medium Impact*
          - Significant damage, loss to assets
        - *High Impact*
          - Major damage, essential functions impaired

- **Quantitative Risk Analysis**
  - *Quantitative Risk Analysis*
    - Provides objective and numerical evaluation of risks
    - Used for financial, safety, and scheduling decisions
    - Utilizes key components
      - Single Loss Expectancy (SLE)
      - Exposure Factor (EF)
      - Annualized Rate of Occurrence (ARO)
      - Annualized Loss Expectancy (ALE)
  - Key Components
    - *Exposure Factor (EF)*
      - Proportion of asset lost in an event (0% to 100%)
      - Indicates asset loss severity
    - *Single Loss Expectancy (SLE)*
      - Monetary value expected to be lost in a single event
      - Calculated as Asset Value x Exposure Factor (EF)
    - *Annualized Rate of Occurrence (ARO)*
      - Estimated frequency of threat occurrence within a year
      - Provides a yearly probability
    - *Annualized Loss Expectancy (ALE)*
      - Expected annual loss from a risk
      - Calculated as SLE x ARO

- **Risk Management Strategies**
  - Four primary risk management strategies
    - *Risk Transference*
      - Shifts risk to another party
      - Common methods
        - Insurance
        - *Contract indemnity clauses*
          - A contractual agreement where one party agrees to cover the other's harm, liability, or loss stemming from the contract
      - Doesn't remove the risk
        - Shifts the responsibility for handling the risk's financial consequences
    - *Risk Acceptance*
      - Acknowledge and deal with risk if it occurs
      - Used when cost of managing the risk outweighs potential loss or risk is unlikely to have a significant impact
      - No actions to mitigate the risk are taken
      - Methods
        - Exemption (excludes party from a rule)
          - The organization doesn't have to obey a specific rule or requirement
          - There is no risk of not complying with the rule or requirement
          - There may be a benefit or mitigation offered by the rule or requirement which exempted organizations won't receive

because they are exempt

- Exception (allows party to avoid rule under specific conditions)

- In both Exemption and Exception, the organization assumes risk either by operating without the safeguards or mitigations offered by a rule (exemption), or by operating in a way that lets them evade the risk (exception).

- *Risk Avoidance*
  - Change plans or strategies to eliminate a specific risk
  - Chosen when the risk is too great to accept or transfer
- *Risk Mitigation*
  - Take steps to reduce likelihood or impact of risk
  - Common strategy involving various actions

- **Risk Monitoring and Reporting**
  - *Risk Monitoring*
    - Process of
      - Tracking identified risks
      - Monitoring residual risks
      - Identifying new risks
      - Evaluating risk response plans
    - Involves ongoing tracking of risks and their response actions
    - Helps determine Residual Risk and Control Risk
      - *Residual Risk*
        - The likelihood and impact of the risk after mitigation, transference, or acceptance measures have been taken on the initial risk

- *Control Risk*
    - Assessment of how a security measure has lost effectiveness over time

- *Risk Reporting*
    - Communicating information about risk management activities to stakeholders
    - Includes results of risk identification, assessment, response, and monitoring
    - Often presented in the form of a risk report
- Risk Monitoring and Reporting are essential for
    - Informed decision making
        - Offer insights for informed decisions on resource allocation, project timelines, and strategic planning
    - Risk mitigation
        - Recognize when a risk is escalating so it can be mitigated before becoming an issue
    - Stakeholder communication
        - Assist in setting expectations and showing effective risk management
    - Regulatory compliance
        - Demonstrate compliance with these regulations

Third-party Vendor Risks

Objectives:

- 2.2 - Explain common threat vectors and attack surfaces
- 2.3 - Explain various types of vulnerabilities
- 5.3 - Explain the processes associated with third-party risk assessment and management

- **Third-party Vendor Risks**
    - *Third-party Vendor Risks*
        - Potential security and operational challenges from external collaborators
        - Scope
            - Encompasses vendors, suppliers, or service providers
        - Risks
            - Impact on integrity, data security, and overall business continuity
    - Common Threat Vectors and Attack Surfaces
        - *Threat Vectors*
            - Paths attackers use to gain access
        - *Attack Surfaces*
            - Points where an unauthorized user can try to enter
    - Various Types of Vulnerabilities
        - *Hardware Vulnerabilities*
            - Components with vulnerabilities
        - *Software Vulnerabilities*
            - Applications with hidden backdoors
        - *Operational Vulnerabilities*
            - Lack of cybersecurity protocols

- Vendor Assessments
  - Evaluation
    - Pre-partnership assessment
  - Penetration Testing
    - Testing vendor security
  - Audit Rights
    - Right to audit vendors
  - Evidence Collection
    - Internal and external audit evidence
- Vendor Selection and Monitoring
  - Importance
    - Meticulous selection process
  - Vigilance
    - Ongoing monitoring of vendor performance
- Contracts and Agreements
  - Basic Contracts
    - Forming relationships
  - Nuanced Agreements
    - SLAs, MOUs, NDAs for specific safeguards

- **Supply Chain Risks**
  - Hardware Manufacturers
    - Products like routers and switches are composed of many components from various suppliers
    - Component tampering or untrustworthy vendors can introduce vulnerabilities
    - Rigorous supply chain assessments needed to trace origins and component

integrity

- Trusted foundry programs ensure secure manufacturing

- Secondary/Aftermarket Sources
  - Risk of acquiring counterfeit or tampered devices
  - Devices may contain malware or vulnerabilities
  - Budget-friendly but high-risk option
- Software Developers/Providers
  - Software developers and software providers are integral cogs in the supply chain
    - However, software can introduce vulnerabilities
  - Check for proper licensing, authenticity, known vulnerabilities, and malware
  - Open-source software allows source code review
  - Proprietary software can be scanned for vulnerabilities
- Service Providers/MSPs
  - *Managed Service Providers*
    - Organizations that provide a range of technology services and support to businesses and other clients
  - Security challenges with Software-as-a-Service (SaaS) providers
    - Data confidentiality and integrity concerns
    - Assess provider's cybersecurity protocols and support for security incidents
    - Vendor selection should consider due diligence, historical performance, and commitment to security
  - Considerations
    - Evaluate data security measures
    - Ensure confidentiality and integrity
    - Assess cybersecurity protocols

        - Response to a security breach

- **Supply Chain Attacks**
    - *Supply Chain Attacks*
        - An attack that targets a weaker link in the supply chain to gain access to a primary target
        - Exploit vulnerabilities in suppliers or service providers to access more secure systems
    - *CHIPS Act of 2022*
        - U.S. federal statute providing funding to boost semiconductor research and manufacturing in the U.S.
        - Aims to reduce reliance on foreign-made semiconductors, strengthen the domestic supply chain, and enhance security
        - *Semiconductors*
            - Essential components in a wide range of products, from smartphones and cars to medical devices and defense systems
    - Safeguarding Against Supply Chain Attacks
        - Vendor Due Diligence
            - Rigorous evaluation of vendor cybersecurity and supply chain practices
        - Regular Monitoring & Audits
            - Continuous monitoring and periodic audits of supply chains to detect suspicious activities
        - Education and Collaboration
            - Sharing threat information and best practices within the industry
            - Collaborating with organizations and industry groups for joint defense

        - Incorporating Contractual Safeguards
            - Embedding cybersecurity clauses in contracts with suppliers or service providers
            - Ensuring adherence to security standards with legal repercussions for non-compliance

- **Vendor Assessment**
    - *Vendor Assessments*
        - Process to evaluate the security, reliability, and performance of external entities
        - Crucial due to interconnectivity and potential impact on multiple businesses
    - Entities in Vendor Assessment
        - *Vendors*
            - Provide goods or services to organizations
        - *Suppliers*
            - Involved in production and delivery of products or parts
        - *Managed Service Providers (MSPs)*
            - Manage IT services on behalf of organizations
    - Penetration Testing of Suppliers
        - *Penetration Testing*
            - Simulated cyberattacks to identify vulnerabilities in supplier systems
        - Validates supplier's cybersecurity practices and potential risks to your organization
    - *Right-to-Audit Clause*
        - Contract provision allowing organizations to evaluate vendor's internal processes for compliance
        - Ensures transparency and adherence to standards

- *Internal Audits*
  - Vendor's self-assessment of practices against industry or organizational requirements
  - Demonstrates commitment to security and quality
- *Independent Assessments*
  - Evaluations conducted by third-party entities without a stake in the organization or vendor
  - Provides a neutral perspective on adherence to security or performance standards
- *Supply Chain Analysis*
  - Assessment of an entire vendor supply chain for security and reliability
  - Ensures integrity of the vendor's entire supply chain, including sources of parts or products

- **Vendor Selection and Monitoring**
  - Vendor Selection Process
    - Similar to hiring a team member
    - Due diligence
      - A rigorous evaluation that goes beyond surface-level credentials
      - Includes the following
        - Evaluating financial stability
        - Operational history
        - Client testimonials
        - On-the-ground practices to ensure cultural alignment
    - Check for conflicts of interest that could bias the selection process

- *Vendor Questionnaires*
  - Comprehensive documents filled out by potential vendors
  - Vendor questionnaires provide insights into operations, capabilities, and compliance
  - Standardized criteria for fair and informed decision-making
- *Rules of Engagement*
  - Guidelines for interaction between organization and vendors
  - Cover communication protocols, data sharing, and negotiation boundaries
  - Ensure productive and compliant interactions
- *Vendor Monitoring*
  - Mechanism used to ensure that the chosen vendor still aligns with organizational needs and standards
  - Performance reviews assess deliverables against agreed-upon standards and objectives
  - *Feedback loops*
    - Involve a two-way communication channel where both the organization and the vendor share feedback

- **Contracts and Agreements**
  - Types of Contracts and Agreements
    - *Basic Contract*
      - Versatile tool that formally establishes a relationship between two parties
      - Defines roles, responsibilities, and consequences for non-compliance
      - Specifies terms like payment structure, delivery timelines, and product specifications

- *Service Level Agreement (SLA)*
  - Defines the standard of service a client can expect from a provider
  - Includes performance benchmarks and penalties for deviations
- Memorandum of Agreement (MOA) and Memorandum of Understanding (MOU)
  - *MOA*
    - Formal, outlines specific responsibilities and roles
  - *MOU*
    - Less binding, expresses mutual intent without detailed specifics
- *Master Service Agreement (MSA)*
  - Covers general terms of engagement across multiple transactions
  - Used for recurring client relationships, supplemented by Statements of Work
- *Statement of Work (SOW)*
  - Specifies project details, deliverables, timelines, and milestones
  - Provides in-depth project-related information
- *Non-Disclosure Agreement (NDA)*
  - Ensures confidentiality of sensitive information shared during negotiations
  - Commitment to privacy, protecting proprietary data
- *Business Partnership Agreement (BPA) or Joint Venture Agreement (JV)*
  - Goes beyond basic contracts when two entities collaborate
  - Outlines partnership nature, profit-sharing, decision-making, and exit strategies
  - Defines ownership of intellectual property and revenue distribution

Governance and Compliance

Objectives:

- 5.1 - Summarize elements of effective security governance
- 5.4 - Summarize elements of effective security compliance

- **Governance and Compliance**
  - *Governance*
    - Overall management of IT infrastructure, policies, procedures, and operations
    - Framework
      - Aligns with organizational objectives and regulatory requirements
    - Crucial Aspects
      - Risk Management
        - Identify, assess, and manage potential risks
      - Strategic Alignment
        - Ensure IT strategy aligns with business objectives
      - Resource Management
        - Efficient and effective use of IT resources
      - Performance Measurement
        - Mechanisms for measuring and monitoring the performance of IT processes
  - *Compliance*
    - Adherence to laws, regulations, standards, and policies

- Importance
  - Legal Obligations
    - Non-compliance leads to penalties (fines, sanctions)
  - Trust and Reputation
    - Compliance enhances reputation and fosters trust
  - Data Protection
    - Prevents breaches and protects privacy
  - Business Continuity
    - Ensures operation in disasters or disruptions
- Governance Structures
  - Boards, Committees
    - Key elements in organizational structure
  - Government Entities
    - External entities influencing governance
  - Centralized vs Decentralized
    - Explanation of organizational structures
- *Policies*
  - High-level guidelines indicating organizational commitments
  - Topics Covered
    - Acceptable Use Policies
    - Information Security Policies
    - Business Continuity
    - Disaster Recovery
    - Incident Response
    - Change Management
    - Software Development Lifecycle (SDLC)

- *Standards*
  - Specific, mandatory actions or rules adhering to policies
  - Covered Standards
    - Password Standards
    - Access Control Standards
    - Physical Security Standards
    - Encryption Standards
- *Procedures*
  - Step-by-step instructions ensure consistency and compliance
  - Covered Procedures
    - Change Management Procedures
    - Onboarding and Offboarding Procedures
    - Playbooks
- Compliance Coverage
  - Monitoring and Reporting
    - Concepts like due diligence, due care, attestation, and acknowledgment
  - Internal and External Compliance
    - Differentiating factors
  - Automation in Compliance
    - Utilizing automation in the compliance process
- Consequences of Non-compliance
  - Fines, Sanctions
    - Legal penalties
  - Reputational Damage
    - Impact on trust and reputation

        - Loss of License, Contractual Impacts
            - Severe consequences

- **Governance**
    - *Governance*
        - Part of the GRC triad (Governance, Risk, and Compliance)
        - Strategic leadership, structures, and processes ensuring IT aligns with business objectives
        - Involves risk management, resource allocation, and performance measurement
    - Purpose of Governance
        - Establishes a strategic framework aligning with objectives and regulations
        - Defines rules, responsibilities, and practices for achieving goals and managing IT resources
    - Influence on IT Components
        - Shapes guidelines for recommended approaches in handling situations
        - Drives policy development, outlining organizational commitments (e.g., data protection)
        - Impacts standards, defining mandatory rules for policy adherence
        - Ensures procedures align with objectives, providing task-specific guidance
    - Adaptation and Revision
        - Governance must adapt to technological advancements, regulatory changes, and industry culture shifts
        - Monitoring evaluates governance effectiveness and identifies gaps
        - Revision updates governance framework

- **Governance Structures**
  - *Organizational Governance*
    - Complex, multifaceted concept essential for successful organization operation
    - Comprises various components, each with unique functions
  - Governance Structures
    - *Boards*
      - Elected by shareholders to oversee organization management
      - Responsible for setting strategic direction, policies, and major decisions
    - *Committees*
      - Subgroups of boards with specific focuses
      - Allows detailed attention to complex areas
    - Government Entities
      - Play roles in governance, especially for public and regulated organizations
      - Establish laws and regulations for compliance
    - Centralized and Decentralized Structures
      - *Centralized*
        - Decision-making authority at top management levels
        - Ensures consistent decisions and clear authority
        - Slower response to local/departmental needs
      - *Decentralized*
        - Decision-making authority distributed throughout the organization
        - Enables quicker decisions and local responsiveness
        - Potential for inconsistencies

- **Policies**
  - *Acceptable Use Policy (AUP)*
    - Document that outlines the do's and don'ts for users when interacting with an organization's IT systems and resources
    - Defines appropriate and prohibited use of IT systems/resources
    - Aims to protect organizations from legal issues and security threats
  - *Information Security Policies*
    - Cornerstone of an organization's security
    - Outlines how an organization protects its information assets from threats, both internal and external
    - These policies cover a range of areas
      - Data Classification
      - Access Control
      - Encryption
      - Physical Security
    - Ensures confidentiality, integrity, and availability of data
  - *Business Continuity Policy*
    - Ensures operations continue during and after disruptions
    - Focuses on critical operation continuation and quick recovery
    - Includes strategies for power outages, hardware failures, and disasters
  - *Disaster Recovery Policy*
    - Focuses on IT systems and data recovery after disasters
    - Outlines data backup, restoration, hardware/software recovery, and alternative locations
  - *Incident Response Policy*
    - Addresses detection, reporting, assessment, response, and learning from

security incidents

- Specifies incident notification, containment, investigation, and prevention steps
- Minimizes damage and downtime during incidents

- *Software Development Lifecycle (SDLC) Policy*
  - Guides software development stages from requirements to maintenance
  - Includes secure coding practices, code reviews, and testing standards
  - Ensures high-quality, secure software meeting user needs
- *Change Management Policy*
  - Governs handling of IT system/process changes
  - Ensures controlled, coordinated change implementation to minimize disruptions
  - Covers change request, approval, implementation, and review processes

- **Standards**
  - *Standards*
    - Provides a framework for implementing security measures, ensuring that all aspects of an organization's security posture are addressed
  - Password Standards
    - Define password complexity and management
    - Include length, character types, regular changes, and password reuse rules
    - Emphasize password hashing and salting for security
  - Access Control Standards
    - Determine who has access to resources within an organization
    - Include access control models like
      - Discretionary Access Control (DAC)
      - Mandatory Access Control (MAC)
      - Role Based Access Control (RBAC)

        - Enforce principles of least privilege and separation of duties
    - Physical Security Standards
        - Cover physical measures to protect assets and information
        - Include controls like perimeter security, surveillance systems, and access control mechanisms
        - Address environmental controls and secure areas for sensitive information
    - Encryption Standards
        - Ensure data remains secure and unreadable even if accessed without authorization
        - Include encryption algorithms like AES, RSA, and SHA-2
        - Depends on the use case and balance between security and performance

- **Procedures**
    - *Procedures*
        - Systematic sequences of actions or steps taken to achieve a specific outcome in an organization
        - Ensures consistency, efficiency, and compliance with standards
    - *Change Management*
        - Systematic approach to handling organizational changes
        - It aims to implement changes smoothly and successfully with minimal disruption
        - Key Stages
            - Identifying the need for change
            - Assessing impacts
            - Developing a plan
            - Implementation
            - Post-change review

- Onboarding and Offboarding Procedures
  - Onboarding integrates new employees into the organization
    - ensures productivity and engagement
    - Includes orientation, training, and integration activities
  - Offboarding manages the transition when an employee leaves
    - Tasks include property retrieval, access disabling, and exit interviews
- *Playbooks*
  - Detailed guides for specific tasks or processes
  - They provide step-by-step instructions for consistent and efficient execution
  - Used in various situations, from cybersecurity incidents to customer complaints
  - Include resource requirements, steps to be taken, and expected outcomes

- **Governance Considerations**
  - Regulatory Considerations
    - Organizations must comply with various regulations, depending on industry and location
    - Regulations cover areas such as
      - Data Protection
      - Privacy
      - Environmental Standards
      - Labor Laws
    - Non-compliance leads to penalties, sanctions, and reputational damage
  - Legal Considerations
    - Complement regulatory considerations, encompassing contract, intellectual property, and corporate law
    - Employment laws address minimum wage, overtime, safety, discrimination, and

benefits
    - Litigation risks include breach of contract, product liability, and employment disputes
    - Robust legal strategies and resources are needed to manage legal risks
  - Industry Considerations
    - Refer to industry-specific standards, practices, and ethical guidelines
    - Not legally binding but influence customer, partner, and regulator expectations
    - Non-adoption may lead to competitive disadvantages and stakeholder criticism
  - Geographical Considerations
    - Geographical regulations impact organizations at local, regional, national, and global levels
    - Local considerations include city ordinances, zoning laws, and operational restrictions
    - Regional considerations, like CCPA in California, impose state-level regulations
    - National considerations, e.g., ADA in the US, affect businesses across the entire country
    - Global considerations, like GDPR, apply extraterritorially to organizations dealing with EU citizens' data
    - Conflict of laws between jurisdictions is a significant challenge
    - Navigating these differences requires deep legal knowledge and flexibility in governance

- **Compliance**
  - *Compliance*
    - Ensures adherence to laws, regulations, guidelines, and specifications
    - Includes compliance reporting and compliance monitoring

- *Compliance Reporting*
  - Systematic process of collecting and presenting data to demonstrate adherence to compliance requirements
  - Two Types of Compliance Reporting
    - *Internal Compliance Reporting*
      - Ensures adherence to internal policies and procedures
      - Conducted by an internal audit team or compliance department
    - *External Compliance Reporting*
      - Demonstrates compliance to external entities
      - Mandatory, often by law or contract
- *Compliance Monitoring*
  - Regularly reviews and analyzes operations for compliance
  - Includes due diligence and due care, attestation and acknowledgement, and internal and external monitoring
- Due Diligence and Due Care
  - *Due Diligence*
    - Identifying compliance risks through thorough review
  - *Due Care*
    - Mitigating identified risks
- Attestation and Acknowledgement
  - *Attestation*
    - Formal declaration by a responsible party that the organization's processes and controls are compliant
  - *Acknowledgement*
    - Recognition and acceptance of compliance requirements by all relevant parties

- Internal and External Monitoring
  - *Internal Monitoring*
    - Regularly reviewing an organization's operations to ensure compliance with internal policies
  - *External Monitoring*
    - Third-party reviews for compliance with external regulations or standards
- Role of Automation in Compliance
  - Streamlines data collection, improves accuracy, and provides real-time monitoring

- **Non-compliance Consequences**
  - Compliance in IT is essential to avoid severe consequences
  - Consequences of non-compliance include
    - *Fines*
      - Monetary penalties imposed by regulatory bodies
    - *Sanctions*
      - Strict measures by regulatory bodies to enforce compliance
      - Range from restrictions to bans
    - *Reputational Damage*
      - Negative impact on a company's reputation
      - Significant and long-lasting in the age of social media
    - *Loss of License*
      - Loss of the right to operate, relevant in regulated industries
    - *Contractual Impacts*
      - Breach of contracts due to non-compliance with laws and regulations
      - Can lead to legal disputes, financial penalties, or contract termination

- To avoid these consequences, companies should prioritize compliance by
  - Understanding and adhering to relevant laws and regulations
  - Implementing robust cybersecurity measures
  - Regularly reviewing and updating compliance programs

Asset and Change Management

Objectives:

- 1.3 - Explain the importance of change management processes and the impact to security
- 4.1 - Given a scenario, you must be able to apply common security techniques to computing resources
- 4.2 - Explain the security implications of proper hardware, software, and data asset management

- **Asset and Change Management**
  - *Asset Management*
    - Systematic process of developing, operating, maintaining, and selling assets cost-effectively
  - *Change Management*
    - Structured approach to transitioning from a current state to a desired future state
  - *Acquisition and Procurement*
    - Structured process of sourcing, vetting, and obtaining security technologies and services
  - Mobile Asset Deployments
    - Deployment Models
      - BYOD
      - COPE
      - CYOD

- Asset Management
  - Assignment/Accounting and Monitoring/Asset Tracking
    - Clear ownership and classification of assets
    - Rigorous monitoring through inventory checks and MDM solutions
- Asset Disposal and Decommissioning
  - Processes
    - Sanitization, destruction, certification, data retention
    - Minimizes the risk of unauthorized access or data breaches
- Change Management Importance
  - Approval Process
    - Strict approval for every change
    - Consideration of CAB insights, ownership, stakeholder involvement, and impact analysis
- Change Management Processes
  - Best Practices
    - Schedule maintenance windows
    - Thorough backout plans
    - Consistent testing post-implementation
- Technical Implications of Changes
  - Management Aspects
    - Allow lists, deny lists
    - Handling downtime, restarts
    - Managing legacy applications and dependencies
- Documenting Changes
  - Importance
    - Version controlling changes

- Regularly updating diagrams, policies, and procedures
- Updating change requests or trouble tickets post-implementation

- **Acquisition and Procurement**
  - *Acquisition*
    - Process of obtaining goods and services
  - *Procurement*
    - Entire process of sourcing and obtaining those goods and services, including all the processes that lead up to the acquisition
  - Conducting the acquisition and procurement process
    - Understand the different types of purchase options
      - *Company Credit Card*
        - Quick purchase of low-cost items
        - Transaction limits and item restrictions
      - *Individual Purchase*
        - Employee purchases, seeks reimbursement
        - Used in emergencies or when no company credit card is available
      - *Purchase Order*
        - Formal document issued by the purchasing department
        - For larger, more expensive purchases
        - Dictates payment terms (NET 15, NET 30, NET 60)
  - Internal Approval Process
    - Ensures purchase alignment with company goals
    - Validates budget allocation
    - Assesses security and compatibility with existing infrastructure

- Post-Approval Procurement
  - Product compatibility assessment
  - Security checks and configurations
  - User training
  - Integration into the existing workflow

- **Mobile Asset Deployments**
  - Three Main Mobile Device Deployment Models
    - *BYOD (Bring Your Own Device)*
      - Employees use personal devices for work
      - Cost-effective for employers
      - Drawbacks include reduced control over security and device management
    - *COPE (Corporate-Owned, Personally Enabled)*
      - The company provides devices for employees
      - Greater control over security and standards
      - Higher initial investment
      - Employees may have privacy concerns or need to carry two devices
    - *CYOD (Choose Your Own Device)*
      - Employees select devices from a company-approved list
      - Balance between employee choice and organizational control
      - Similar drawbacks to COPE in terms of initial cost and potential privacy concerns
  - Selecting the Right Model
    - Consider the specific needs, budget constraints, and risk appetite of your organization

        - Analyze costs, security, and employee satisfaction
            - BYOD may have hidden costs for security and compatibility
            - COPE offers more control over devices and supports MDM
            - CYOD provides a balance between flexibility and control

- **Asset Management**
    - *Asset Management*
        - Systematic approach to governing and maximizing the value of items an entity is responsible for throughout the asset's life cycle
            - Tangible Assets
                - Office buildings
                - Computers
                - Machinery
            - Intangible Assets
                - Intellectual property
                - Organization's reputation
                - Goodwill
    - Assignment and Accounting of Assets
        - Each asset assigned to a person or group, known as owners
        - Process referred to as the allocation or assignment of ownership
        - Avoids ambiguity, aids troubleshooting, upgrades, and replacements
    - Classification and Categorization
        - Assets should be classified and categorized
        - Classification based on criteria such as function and value
        - Informs maintenance, replacement, or retirement decisions
        - High-value assets may require stringent maintenance schedules

- Low-value assets may be considered for recycling or disposal
- Monitoring and Tracking of Assets
  - Ensures proper accounting and optimal use of assets
    - *Asset Monitoring*
      - Maintaining an inventory with specifications, location, and assigned users
    - *Asset Tracking*
      - Goes beyond monitoring, involving the location, status, and condition of assets using specialized software and tracking technologies
    - *Enumeration*
      - Identifies and counts assets, especially in large organizations or during times of asset procurement or retirement
      - Aids in maintaining an accurate inventory
  - Proactive approach for risk management and resource optimization
- *Mobile Device Management (MDM)*
  - Manages and tracks mobile devices
    - Smartphones
    - Tablets
    - Laptops
    - Wearables
  - Centralizes management, enforces corporate policies, ensures software uniformity, safeguards sensitive data
  - Enables remote lock and wipe of lost devices, remote software updates, and consistent user experiences
  - Reduces risks associated with unsecured or outdated devices

- **Asset Disposal and Decommissioning**
  - *Asset Disposal and Decommissioning*
    - Necessity to manage the disposal of outdated assets
  - *NIST Special Publication 800-88 (Guidelines for Media Sanitization)*
    - Provides guidance on asset disposal and decommissioning
  - *Sanitization*
    - Thorough process to make data inaccessible and irretrievable from storage medium using traditional forensic methods
    - Applies to various storage media
    - Methods include
      - *Overwriting*
        - Replacing the existing data on a storage device with random bits of information to ensure that the original data is obscured
        - Repeated several times to reduce any chance of the original data being recovered
        - Overwriting can use a single pass, 7 passes, or 35 passes
      - *Degaussing*
        - Utilizes a machine called a degausser to produce a strong magnetic field that can disrupt magnetic domains on storage devices like hard drives or tapes
        - Renders data on the storage medium unreadable and irretrievable
        - Permanent erasure of data but makes the device unusable
        - After degaussing, a device can no longer be used to store data
      - *Secure Erase*
        - Deletes data and ensures it can't be recovered

        - Implemented in firmware level of storage devices
        - Built-in erasure routine purges all data blocks
        - Deprecated in favor of cryptographic erase
    - *Cryptographic Erase (CE)*
        - Utilizes encryption technologies for data sanitization
        - Destroys or deletes encryption keys, rendering data unreadable
        - Quick and efficient method of sanitization
        - Supports device repurposing without data leakage
- *Destruction*
    - Goes beyond sanitization, ensures physical device is unusable
    - Recommended methods
        - Shredding
        - Pulverizing
        - Melting
        - Incinerating
    - Used for high-security environments, especially with Secret or Top Secret data
- *Certification*
    - Acts as proof that data or hardware has been securely disposed of
    - Important for organizations with regulatory requirements
    - Creates an audit log of sanitization, disposal, or destruction
- *Data Retention*
    - Strategically deciding what to keep and for how long
    - Data has a lifecycle from creation to disposal
    - Reasons to retain data
        - Regulatory requirements
        - Historical analysis

        - Trend prediction
        - Dispute resolution
    - Retaining everything is not feasible due to costs and security risks
        - The more you store, the more you must secure
    - Clutter and excessive data require additional security measures
  - *Data Protection*
    - All data needs protection from potential data breaches
    - More data requires more extensive security measures
    - Leads to higher costs and resource allocation
    - Excessive data complicates retrieval and analysis

- **Change Management**
  - *Change Management*
    - Orchestrated strategy to transition teams, departments, and organizations from existing state to a more desirable future state
        - Necessary in modern business environments due to constant changes
        - Change is essential but requires
            - Precision
            - Planning
            - Structured approach
        - Ensures changes are properly controlled, planned, and integrated to avoid disruptions
  - Challenges of Change
    - Unplanned or poorly coordinated changes can lead to resistance and confusion
    - Even seemingly simple changes, like software upgrades, can cause issues
    - Existing processes become disrupted by changes, impacting efficiency

- Change Approval and Assessment
  - Changes must be approved and assessed
  - Organizational processes and procedures for change approval
  - Assessment evaluates value and potential disruptions
  - *Change Advisory Board (CAB)*
    - Body of representatives from various parts of an organization that is responsible for evaluation of any proposed changes
    - Evaluates proposed changes before approval, assesses viability, impacts, and alignment with objectives
- *Change Owner*
  - Individual or team responsible for initiating change request
  - Advocates for the change, details reasons, benefits, and challenges
  - Key in presenting the case for the change
- *Stakeholders*
  - Individuals or teams with a vested interest in the proposed change
  - Directly impacted or involved in assessment and implementation
  - These individuals or teams must be
    - Consulted
    - Their feedback considered
    - Their concerns addressed
  - Include technical, business, and end-user stakeholders
- *Impact Analysis*
  - Integral part of the Change Management process
  - Essential before implementing proposed changes
  - Assesses potential fallout, immediate effects, long-term impacts
  - Identifies challenges and prepares for maximizing benefits

- **Change Management Processes**
  - Five Main Steps in Change Management
    - Preparing for the Change
      - Understand the current state and need for transition
      - Assess existing processes and identify inefficiencies and challenges
      - Gather necessary resources, engage stakeholders, and ensure readiness.
    - Creating a Vision for the Change
      - Craft a clear and compelling vision for change
      - Defining the following
        - Desired future state
        - Reasons for the change
        - Success criteria
      - Inspire enthusiasm and buy-in across stakeholders
    - Implementing the Change
      - Put the plan into action, which may involve
        - Training
        - Restructuring,
        - Introducing new tools
      - Maintain continuous communication with stakeholders
      - Address concerns and be open to feedback to reduce resistance
    - Verifying the Change
      - Measure the effectiveness and ensure desired outcomes are achieved
      - It might require the following
        - Surveys
        - Metrics analysis

        - Stakeholder interviews
    - Address discrepancies or issues to refine and optimize the process
- Documenting the Change
    - Maintain historical records of implemented changes
    - Capture lessons learned for future reference
    - Reflect on past initiatives and improve change management practices
- Key Aspects of the Change Management Process
    - *Scheduled Maintenance Window*
        - Designated timeframes for implementing changes
        - Reduces potential disruptions to daily operations
        - Allows flexibility for emergency changes
    - *Backout Plan*
        - Pre-determined strategy to revert systems to their original state in case of issues during change implementation
        - Acts as a safety net for ensuring quick return to normal operations
    - Testing the Results
        - Validates the success of the change by conducting tests on systems and operational processes after implementation
        - Ensures desired outcomes and identifies areas needing further adjustments

    - *Standard Operating Procedures (SOPs)*
        - Detailed step-by-step instructions for specific tasks
        - Ensures consistency, efficiency, and reduces errors in change implementation within the organization

- **Technical Implications of Changes**
  - Technical Implications of Changes
    - Allow Lists and Deny Lists
      - *Allow List*
        - Specifies entities permitted to access a resource
      - *Deny List*
        - Lists entities prevented from accessing a resource
      - Review both lists when proposing changes to prevent unintended access restrictions or grants
      - Essential for maintaining system functionality and security
    - Restricted Activities
      - Certain tasks labeled as 'restricted' due to their impact on system health or security
      - Verify proposed changes for any restricted activities
      - Prevent data breaches and operational disruptions by understanding restrictions
    - Downtime
      - Any change, even minor, carries the risk of causing downtime
      - Estimate potential downtime and assess its negative effects against benefits
      - Schedule changes during maintenance windows to minimize impacts on end users
    - Service and Application Restarts
      - Some changes, like installing security patches, require service or application restarts
      - Restarting critical services can be disruptive, potentially causing data loss

or backlog

- Consider the implications of restarts, especially for key servers

- Legacy Applications
  - Older software or systems still in use due to functionality and user needs
  - Legacy applications are less flexible and more sensitive to changes
  - Minor updates can lead to malfunctions or crashes, so assess their compatibility.
- Dependencies
  - Interconnected systems create dependencies, where changes in one area affect others
  - Mapping dependencies is crucial before implementing changes
  - Prevents cascading effects, outages, or disruptions in various parts of your network

- **Documenting Changes**
  - Documenting changes provides a clear history of the what, when, and why for accountability and future reference
  - *Version Control*
    - Tracks and manages changes in documents, software, and other files
    - Allows multiple users to collaborate and revert to previous versions when needed
    - Ensures changes do not create chaos and helps track project evolution
    - Preserves past iterations and ensures continuity and stability
  - Proper Documentation
    - All accompanying documentation should be updated when implementing a change

- Updates should reflect the implementation of the change, from minor configurations to major network overhauls
- Key elements of proper documentation
  - Updating diagrams to provide a visual representation of system architecture
  - Revising policies and procedures to address issues or improvements
  - Updating change requests and trouble tickets to reflect successful completion
- Proper documentation is critical for clarity and accountability

- Continuous Improvement
  - After implementing a change, evaluate the process and its success
  - Identify issues and revise policies and procedures to prevent recurrence
  - Emphasizes iterative process improvement to ensure smoother future changes
  - Learn from past mistakes for better change management practices
- Importance of Records
  - Change requests and trouble tickets help create a clear timeline of change actions
  - Inform stakeholders and provide a record of change history for future reference
  - Records are essential for communication and accountability in change management

Audits and Assessments

Objective 5.5: Explain types and purposes of audits and assessments

- **Audits and Assessments**
  - *Audits*
    - Systematic evaluations of an organization's information systems, applications, and security controls
    - Types
      - *Internal Audits*
        - Conducted by the organization's own team
      - *External Audits*
        - Performed by third-party entities
    - Purpose
      - Validate security measures
      - Identify vulnerabilities
      - Maintain compliance with regulatory standards
    - Examples
      - Internal Audit Example
        - Review of data protection policies
        - Check policy relevance and compliance
      - External Audit Example
        - Evaluation of e-commerce PCI DSS compliance
        - Assess network security, data encryption, and access controls

- Significance of Audits
  - Identifying Gaps
    - Security policies, procedures, and controls
  - Ensuring Compliance
    - GDPR, HIPAA, PCI DSS

- *Assessments*
  - Detailed analysis to identify vulnerabilities and risks
  - Performed before implementing new systems or significant changes
  - Categories
    - Risk Assessments
    - Vulnerability Assessments
    - Threat Assessments
- *Internal Audits and Assessments*
  - Review processes, controls, and compliance
  - Importance
    - Ensure operational effectiveness and adherence to internal policies
- *External Audits and Assessments*
  - Independent evaluations by external parties
  - Verification Areas
    - Financial statements
    - Compliance
    - Operational practices
- *Penetration Testing*
  - Simulated cyber attacks to identify vulnerabilities
  - Objective
    - Find vulnerabilities exploited by attackers

        - Also known as “Pen Testing” or “Ethical Hacking”
    - *Reconnaissance in Pentesting*
        - Gathering information before a pentest
        - Types
            - Passive
            - Active
        - Environment Consideration
            - Known
            - Partially Known
            - Unknown
    - *Attestation of Findings*
        - Formal, written declaration of audit or assessment results
        - Purpose
            - Confirmation and documentation of outcomes

- **Internal Audits and Assessments**
    - *Internal Audits*
        - Systematic evaluations conducted by an organization's own audit team
        - Assess the effectiveness of internal controls, compliance with regulations, and the integrity of information systems and processes
        - Focus areas may include
            - Data protection
            - Network security
            - Access controls
            - Incident response procedures

- Examples of internal audit focus areas
  - Password policies
  - User access controls
- Process
  - Reviewing policies and procedures
  - Examining access rights
  - Testing effectiveness of controls
  - Findings documented for recommendations and improvements
- Concepts in Internal Audits
  - *Compliance Requirements*
    - Ensuring adherence to established standards, regulations, and laws
    - Compliance is essential for protecting sensitive data and avoiding legal penalties
    - Internal audits may be required for compliance with specific laws or regulations
  - *Audit Committee*
    - A group, often comprising members of a company's board of directors, overseeing audit and compliance activities
    - Responsibilities
      - Reviewing financial reporting
      - Internal controls
      - Internal and external audits
      - Legal and regulatory compliance
    - Addresses issues raised by auditors

- *Internal Assessments*
  - Conducted to identify and evaluate potential risks and vulnerabilities in an organization's information systems
  - Commonly performed before implementing new systems or making significant changes to existing ones
  - *Self-assessments*
    - Internal evaluations assessing compliance with specific standards or regulations
  - Vulnerability assessments, threat modeling exercises, and risk assessments are part of internal assessments
  - Assisted internal assessments may involve dedicated assessment groups
  - Internal Assessment Process
    - *Threat Modeling Exercise*
      - Identifies potential threats to applications (e.g., SQL injection, XSS, DoS attacks)
    - *Vulnerability Assessment*
      - Uses automated scanning tools and manual testing techniques to identify known vulnerabilities and code weaknesses
    - *Risk Assessment*
      - Evaluates the potential impact of the following
        - Identified threats and vulnerabilities
        - Considering likelihood
        - Potential damage
        - Cost of security measures
  - Mitigation Strategies
    - Recommendations to address risks and vulnerabilities

- Code fixes
- Additional security controls
- Architectural changes

- **Performing an Internal Assessment**
  - *Internal Assessment*
    - Proactive evaluation of an organization's security posture
    - Helps to identify and address potential risks and vulnerabilities in information systems
  - Using a Sample Checklist
    - The specific checklists and procedures for an internal assessment may vary based on the following
      - Organization's governance
      - Risk
      - Compliance practices
    - A sample checklist from the Minnesota Counties Intergovernmental Trust (MCIT) is used
    - *MCIT Cybersecurity Self-Assessment*
      - MCIT's Cybersecurity Self-Assessment checklist is designed to help organizations minimize data and cybersecurity-related exposures
      - It assists in identifying areas where data security may need strengthening
      - The checklist comprises yes-or-no questions with sections for comments and action items
      - Action items are assigned to specific individuals or groups responsible for implementing corrective actions

- Collaborative Approach
  - To maximize the checklist's effectiveness, involve a diverse group of participants from across the organization
    - Administration team
    - Information technology staff
    - Cybersecurity professionals
- Overview of the Checklist
  - The checklist is broad and aims to provide a quick overview of the organization's current risk posture
  - Organizations may use different checklists or variations with distinct questions
  - The general format and purpose of self-assessments are consistent across most organizations

- **External Audits and Assessments**
  - *External Audits and Assessments*
    - Essential tools for maintaining a robust security posture and ensuring regulatory compliance
    - Conducted by independent third parties to provide an unbiased perspective on an organization's security
  - *External Audits*
    - Systematic evaluations conducted by independent entities
    - Assess information systems, applications, and security controls
    - Focuses on various areas
      - Data protection
      - Network security
      - Access controls

        - Incident response procedures
    - Objective is to identify gaps in security policies and controls for compliance with regulatory standards such as
        - GDPR
        - HIPAA
        - PCI DSS
  - *External Assessments*
    - Detailed analysis by independent entities to identify vulnerabilities and risks in an organization's security systems
    - Utilize automated scanning tools and manual testing techniques
    - External assessments can take various forms
        - Risk assessments
        - Vulnerability assessments
        - Threat assessments
  - Regulatory Compliance
    - The goal is to ensure organizations comply with relevant laws, policies, and regulations
    - Organizations adopt consolidated and harmonized sets of compliance controls to achieve regulatory compliance, e.g., NIST Cybersecurity Framework
    - Compliance includes adherence to industry-specific rules (e.g., HIPAA, PCI DSS) and more generalized regulations like GDPR
  - *Examinations*
    - Detailed inspections of an organization's security infrastructure conducted externally
    - Cover various areas
        - Network security

            - Data protection
            - Access controls
        - May include testing of the following
            - Key personnel
            - Certifications
            - Standardized assessments
        - Crucial for maintaining a strong security posture and regulatory compliance.
    - Independent Third-Party Audits
        - Provide an unbiased perspective on an organization's security posture
        - Validate security measures and build trust with
            - Customers
            - Stakeholder
            - Regulatory bodies
        - Required by regulations like GDPR and PCI DSS for organizations to undergo regular independent third-party audits

- **Performing an External Assessment**
    - *External Assessment*
        - Part of maintaining a robust security posture and ensuring compliance
        - May vary based on the following
            - Organization's governance
            - Risk
            - Compliance practices
        - Sample checklist used for a HIPAA external assessment from the government of San Bernardino County, California as a demonstration
        - Purpose is to validate compliance with specific regulations and minimize

cybersecurity risks

- Preparing for a HIPAA External Assessment
  - Examiners provide a checklist of questions that organizations must answer
  - Questions are answered as either "yes" or "no"
  - Evidence files, such as documents or links, must be provided to demonstrate compliance
- Sample Checklist
  - Questions cover various aspects like general information, policies, procedures, and employee training
  - Organizations must provide evidence files as proof of compliance
  - External assessments aim to provide a quick overview of the organization's current risk posture

- **Penetration Testing**
  - *Penetration Testing (Pentesting)*
    - Simulated cyber attack to identify exploitable vulnerabilities in a computer system
    - Assesses systems for potential weaknesses that attackers could exploit
    - Various types include
      - Physical
      - Offensive
      - Defensive
      - Integrated

- *Physical Penetration Testing*
  - Evaluates an organization's physical security measures
  - Examples
    - Testing locks
    - Access card
    - Security cameras
  - Identifies vulnerabilities and recommends improvements for enhanced physical security
  - Benefits
    - Improved security awareness
    - Preventing unauthorized access
- *Offensive Penetration Testing*
  - Known as “red teaming”
  - Actively seeks vulnerabilities and attempts to exploit them, like a real cyber attack
  - Helps uncover and report vulnerabilities to improve security
  - Can simulate real-world attacks and gain support for cybersecurity investments
- *Defensive Penetration Testing*
  - Known as “blue teaming”
  - A reactive approach focused on strengthening systems, detecting and responding to attacks
  - Monitors for unusual activity and improves incident response times
  - Enhances detection capabilities and helps improve incident response
- *Integrated Penetration Testing*
  - Known as “purple teaming”
  - Combines elements of offensive and defensive testing

        - Red team conducts offensive attacks, while the blue team detects and responds
        - Encourages collaboration and learning between the red and blue teams
        - Benefits
            - Comprehensive security assessment
            - Promotes collaboration within cybersecurity teams
            - Conducts simulated attacks and responses to improve skills

- **Reconnaissance in Pentesting**
    - *Reconnaissance*
        - Initial phase where an attacker gathers information about the target system
        - Information helps plan the attack and increase its success rate
    - Importance of Reconnaissance
        - Crucial step in penetration testing
        - Identifies potential vulnerabilities in the target system
        - Helps plan the attack to reduce the risk of detection and failure

    - Types of Reconnaissance
        - *Active Reconnaissance*
            - Engaging with the target system directly, such as scanning for open ports using tools like Nmap
        - *Passive Reconnaissance*
            - Gathering information without direct engagement, like using open-source intelligence or WHOIS to collect data
    - Reconnaissance and Environment Types
        - *Known Environment*
            - Penetration testers have detailed information about the target

infrastructure

- Focuses on known assets
- Evaluates vulnerabilities and weaknesses
- Aims to understand exploitability and potential damages
- Resembles an insider threat scenario

- *Partially Known Environment*
  - Testers have limited information, simulating a scenario where an attacker has partial inside knowledge
  - Focus on discovering and navigating the broader environment
- *Unknown Environment*
  - Minimal to no information about the target system
  - Simulates a real-world external attacker aiming to find entry points and vulnerabilities
  - Extensive reconnaissance is essential

- **Performing a Basic PenTest**
  - *Metasploit*
    - Multipurpose computer security and penetration testing framework
    - Has a wide array of powerful tools for conducting penetration tests

- **Attestation of Findings**
  - *Attestation*
    - Involves formal validation or confirmation provided by an entity to assert the accuracy and authenticity of specific information
    - Crucial in internal and external audits to ensure the reliability and integrity of the following

        - Data
        - Systems
        - Processes
    - Attestation of Findings in Penetration Testing
        - Used to prove that a penetration test occurred and validate the findings
        - May be required for compliance or regulatory purposes (e.g., GLBA, HIPAA, Sarbanes-Oxley, PCI DSS)
        - Includes a summary of findings and evidence of the security assessment
        - Evidence helps to prove that identified vulnerabilities and exploits are valid
        - The difference between attestation and the report
            - Attestation includes evidence
            - Report focuses on findings and recommended remediation
        - A letter of attestation may be provided to prove the occurrence of the penetration testing, especially when required by third parties interested in network security
    - Types of Attestation
        - *Software Attestation*
            - Involves validating the integrity of software to ensure it hasn't been tampered with
        - *Hardware Attestation*
            - Validates the integrity of hardware components to confirm they haven't been tampered with
        - *System Attestation*
            - Validates the security posture of a system, often related to compliance with security standards

- Attestation in Audits
  - In internal audits, attestation evaluates organizational compliance, effectiveness of internal controls, and adherence to policies and procedures
  - In external audits, third-party entities provide attestation on financial statements, regulatory compliance, and operational efficiency
  - Attestation builds trust, enhances transparency, ensures accountability, and is essential for stakeholders in making informed decisions

Cyber Resilience and Redundancy

Objective 3.4: Explain the importance of resilience and recovery in security architecture

- **Cyber Resilience and Redundancy**
  - *Cyber Resilience*
    - Ability to deliver outcomes despite adverse cyber events
  - *Redundancy*
    - Having additional systems or processes for continued functionality
  - Significance of Cyber Resilience
    - Swift Recovery
      - Enables organizations to recover swiftly after cyber events
    - Continuous Operations
      - Ensures continuous operations despite attacks or technical failures
  - High Availability
    - Importance
      - Critical for continuous operations
    - Elements
      - Load balancing
      - Clustering
      - Redundancy in power
      - Connections
      - Servers
      - Services
      - Multi-cloud systems

- Data Redundancy
  - Achieved by
    - Redundant storage devices
  - Types
    - RAID configurations
- Capacity Planning
  - Importance
    - Efficient scaling during peak demand
  - Considerations
    - People
    - Technology
    - Infrastructure
- Power Components
  - Generators, UPS, line conditioners, power distribution centers (PDCs)
  - Ensures constant power supply to data centers
- Data Backups
  - Types
    - Onsite
    - Offsite
  - Methods
    - Encryption
    - Snapshots
    - Recovery
    - Replication
    - Journaling

- Business Continuity and Disaster Recovery (BC/DR) Plan
  - Importance
    - Ensures smooth business operations during unforeseen events
- Backup Site Options
  - Hot
  - Cold
  - Warm Sites
  - Geographic Dispersion
  - Virtual Sites
  - Platform Diversity
- Testing Methods
  - Tabletop Exercises
  - Failover Techniques
  - Simulation
  - Parallel Processing
  - Use Cases
    - Support different scenarios within organizations

- **High Availability**
  - High Availability Basics
    - *High Availability*
      - Aims to keep services continuously available by minimizing downtime
      - Achieved through load balancing, clustering, redundancy, and multi-cloud strategies

- Uptime and Availability Standards
  - *Uptime*
    - The time a system remains online, typically expressed as a percentage
  - *Five nines*
    - Refers to 99.999% uptime, allowing only about 5 minutes of downtime per year
  - *Six nines*
    - Refers to 99.9999% uptime, allows just 31 seconds of downtime per year
- *Load Balancing*
  - Distributes workloads across multiple resources
  - Optimizes resource use, throughput, and response time
  - Prevents overloading of any single resource
  - Incoming requests are directed to capable servers
- *Clustering*
  - Uses multiple computers, storage devices, and network connections as a single system
  - Provides high availability, reliability, and scalability
  - Ensures continuity of service even in case of hardware failure
  - Can be combined with load balancing for robust solutions
- *Redundancy*
  - Involves duplicating critical components to increase system reliability
  - Redundancy can be implemented by adding multiple
    - Power supplies
    - Network connections
    - Servers
    - Software services

        - Service providers
    - Prevents single points of failure in systems
    - Examples
        - Redundant power supplies
        - Network connections
        - Backup servers
  - *Multi-Cloud Approach*
    - Distributes data, applications, and services across multiple cloud providers
    - Mitigates the risk of a single point of failure
    - Offers flexibility for cost optimization
    - Aids in avoiding vendor lock-in
    - Requires proper data management, unified threat management, and consistent policy enforcement for security and compliance
  - *Strategic Planning*
    - Design a robust system architecture to achieve high availability
    - Utilize load balancing, clustering, redundancy, and multi-cloud approaches
    - Proactive measures reduce the risk of service disruptions and downtime costs
    - Safeguard organizational continuity and reliability in a competitive environment

- **Data Redundancy**
  - RAID Overview
    - *RAID (Redundant Array of Independent Disks)*
        - Combines multiple physical storage devices into a single logical storage device recognized by the operating system
  - *RAID 0*
    - Provides data striping across multiple disks

        - Used for improved performance but offers no data redundancy
        - Multiple drives increase read and write speeds
        - Suitable for scenarios where performance is essential, and data redundancy is not a concern
    - *RAID 1*
        - Provides redundancy by mirroring data identically on two storage devices
        - Ensures data integrity and availability
        - Suitable for critical applications and maintains a complete copy of data on both devices
        - Only one storage device can fail without data loss or downtime
    - *RAID 5*
        - Utilizes striping with parity across at least three storage devices
        - Offers fault tolerance by distributing data and parity
        - Can continue operations if one storage device fails
        - Data reconstruction is possible but results in slower access speeds
    - *RAID 6*
        - Similar to RAID 5 but includes double parity data
        - Requires at least four storage devices
        - Can withstand the failure of two storage devices without data loss
    - *RAID 10*
        - Combines RAID 1 (mirroring) and RAID 0 (striping)
        - Offers high performance, fault tolerance, and data redundancy
        - Requires an even number of storage devices, with a minimum of four
    - RAID Resilience Categories
        - *Failure-resistant*
            - Resists hardware malfunctions through redundancy (e.g., RAID 1)

        - *Fault-tolerant*
            - Allows continued operation and quick data rebuild in case of failure (e.g., RAID 1, RAID 5, RAID 6, RAID 10)
        - *Disaster-tolerant*
            - Safeguards against catastrophic events by maintaining data in independent zones (e.g., RAID 1, RAID 10)
    - RAIDs are essential for ensuring data redundancy, availability, and performance in enterprise networks
    - The choice of RAID type depends on specific requirements for performance and fault tolerance

- **Capacity Planning**
    - *Capacity Planning*
        - Critical strategic planning effort for organizations
        - Ensures an organization is prepared to meet future demands in a cost-effective manner
    - Four Main Aspects of Capacity Planning
        - People
            - Analyze current personnel skills and capacity
            - Forecast future personnel needs for hiring, training, or downsizing
            - Ensure the right number of people with the right skills for strategic objectives
            - Example
                - Hiring seasonal employees for holiday retail demand
        - Technology
            - Assess current technology resources and their usage

        - Predict future technology demands
        - Consider scalability and potential investments in new technology
        - Example
            - Ensuring an e-commerce platform can handle traffic spikes
    - Infrastructure
        - Plan for physical spaces and utilities to support operations
        - Includes office spaces, data centers, and more
        - Optimize space and power consumption
        - Example
            - Data center capacity planning for server installations

    - Processes
        - Optimize business processes for varying demand levels
        - Streamline workflows, improve efficiency, and consider outsourcing
        - Example
            - Automating employee onboarding to handle high demand

- **Powering Data Centers**
    - Key Terms
        - *Surges*
        - Sudden, small increases in voltage beyond the standard level (e.g., 120V in the US)
        - *Spikes*
        - Short-lived voltage increases, often caused by short circuits, tripped breakers, or lightning

- *Sags*
  - Brief decreases in voltage, usually not severe enough to cause system shutdown
- *Undervoltage Events (Brownouts)*
  - Prolonged reduction in voltage, leading to system shutdown
- *Power Loss Events (Blackouts)*
  - Complete loss of power for a period, potentially causing data loss and damage

- Power Protection Components
  - *Line Conditioners*
    - Stabilize voltage supply and filter out fluctuations
    - Mitigate surges, sags, and undervoltage events
    - Prevent unexpected system behavior and hardware degradation
    - Unsuitable for significant undervoltage events or complete power failures
  - *Uninterruptible Power Supplies (UPS)*
    - Provide emergency power during power source failures
    - Offer line conditioning functions
    - Include battery backup to maintain power during short-duration failures
    - Typically supply 15 to 60 minutes of power during a complete power failure
  - *Generators*
    - Convert mechanical energy into electrical energy for use in an external circuit through the process of electromagnetic induction
    - Backup generators supply power during power grid outages
    - Smaller generators for limited applications (e.g., emergency lighting)
    - Different Types of Generators

        - Portable gas-engine generators
        - Permanently installed generators
        - Battery-inverter generators
    - *Power Distribution Centers (PDC)*
        - Central hub for power reception and distribution
        - Includes circuit protection, monitoring, and load balancing
        - Integrates with UPS and backup generators for seamless transitions during power events
  - Considerations for Data Centers
    - Large data centers use rack-mounted UPS for server protection
    - UPS provides line conditioning and battery backup for 10-15 minutes
    - Power distribution units manage load balancing and line conditioning
    - Backup generators are crucial for extended power outages but require startup time
    - Building data centers with redundancy and protections tailored to use cases and budgets

- **Data Backups**
  - *Data Backup*
    - Creating duplicate copies of digital information to protect against data loss, corruption, or unavailability
    - Safeguards data from accidental deletion or system failures
  - Onsite and Offsite Backups
    - *Onsite Backup*
        - Storing data copies in the same location as the original data

- *Offsite Backup*
  - Storing data copies in a geographically separate location
- Importance
  - Onsite backups are convenient but vulnerable to disasters
  - Offsite backups protect against physical disasters

- Backup Frequency
  - Determining factor of backup frequency is the organization's RPO
    - *Recovery Point Objective (RPO)*
      - Ensures that the backup plan will maintain the amount of data required to keep any data loss under the organization's RPO threshold
  - Considerations
    - Data change rate
    - Resource allocation
    - Organizational needs
- *Encryption*
  - Fundamental safeguard that protects the backup data from unauthorized access and potential breaches
    - *Data-at-rest Encryption*
      - Encrypting data as it is written to storage
    - *Data-in-transit Encryption*
      - Protecting data during transmission
    - Importance
      - Safeguarding backup data from unauthorized access and breaches
- *Snapshots*
  - Point-in-time copies capturing a consistent state

- Records only changes since the previous snapshot, reducing storage requirements
- Use cases
  - Valuable for systems where data consistency is critical, like databases and file servers

- Data Recovery
  - Several key steps in the data recovery process
    - Selection of the right backup
    - Initiating the recovery process
    - Data validation
    - Testing and validation
    - Documentation and reporting
    - Notification
  - Importance
    - Regaining access to data in case of loss or system failure; a well-defined and tested recovery plan is essential
- *Replication*
  - Real-time or near-real-time data copying to maintain data continuity
  - Benefits
    - Ensures seamless data continuity
    - Suitable for high-availability environments
- *Journaling*
  - Maintaining a detailed record of data changes over time
  - Benefits
    - Enables granular data recovery
    - Maintains an audit trail

            - Ensures data integrity and compliance
        - Considerations
            - Data tracking granularity, size, retention policies, and security

- **Continuity of Operations Plan**
    - *Continuity of Operations Plan (COOP)*
        - Ensures an organization's ability to recover from disruptive events or disasters
        - Requires detailed planning and forethought
    - Key Terms
        - *Business Continuity Planning (BC Plan)*
            - Plans and processes for responding to disruptive events
            - Addresses a wide range of threats and disruptive incidents
            - Involves preventative actions and recovery steps
            - Can cover both technical and non-technical disruptions
        - *Disaster Recovery Plan (DRP)*
            - Focuses on plans and processes for disaster response
            - Subset of the BC Plan
            - Focuses on faster recovery after disasters
            - Addresses specific events like hurricanes, fires, or floods
    - Strategies for Business Continuity
        - Consider alternative locations for critical infrastructure
        - Distribute staff across multiple geographic regions
        - Use cloud services to maintain operations during disasters
    - The Role of Senior Management
        - Senior managers are responsible for developing the BC Plan
        - Goals for BC and DR efforts should be set by senior management

        - Appoint a Business Continuity Coordinator to lead the Business Continuity Committee
    - Business Continuity Committee
        - Comprises representatives from various departments (IT, Legal, Security, Communications, etc.)
        - Determines recovery priorities for different events
        - Identifies and prioritizes systems critical for business continuity
    - Defining Scope
        - Senior management decides the plan's scope based on risk appetite and tolerance
        - Can be broken down by business function or geographical area
        - All components must be coherent and compatible for crisis situations

- **Redundant Site Considerations**
    - *Redundant Site*
        - Backup location or facility that can take over essential functions and operations in case the primary site experiences a failure or disruption
    - Types of Continuity Locations
        - *Hot Sites*
            - Up and running continuously, enabling a quick switchover
            - Requires duplicating all infrastructure and data
            - Expensive, but provides instant availability
        - *Warm Sites*
            - Not fully equipped, but fundamentals in place
            - Can be up and running within a few days
            - Cheaper than hot sites but with a slight delay

- *Cold Sites*
  - Fewer facilities than warm sites
  - May be just an empty building, ready in 1-2 months
  - Cost-effective but adds more recovery time
- *Mobile Sites*
  - Can be hot, warm, or cold
  - Utilizes portable units like trailers or tents
  - Offers flexibility and quick deployment (e.g., military DJC2)

- Platform Diversity
  - Critical for effective virtual redundant sites
  - Diversify operating systems, network equipment, and cloud platforms
  - Reduces the risk of a single point of failure
  - Ensures resilience and adaptability in case of disruptions
- Virtual Sites
  - Leveraging cloud-based environments for redundancy
  - *Virtual Hot Site*
    - Fully replicated and instantly accessible in the cloud
  - *Virtual Warm Site*
    - Involves scaling up resources when needed
  - *Virtual Cold Site*
    - Minimizes ongoing costs by activating resources only during disasters
  - Offers scalability, cost-effectiveness, and easy maintenance
- Geographic Dispersion
  - Spreading resources across different locations for higher redundancy
  - Mitigates the risk of localized outages
  - Enhances disaster recovery capabilities

- Considerations for Redundant Site Selection
  - Think about technology stack, people's workspace, and long-term support
  - Determine which type of redundant site suits your organization's needs
  - Ensure continuity of essential functions and services in the event of disruptions

- **Resilience and Recovery Testing**
  - *Resilience Testing*
    - Assess system's ability to withstand and adapt to disruptive events
    - Ensures the system can recover from unforeseen incidents
    - Conducted through tabletop exercises, failover tests, simulations, and parallel processing
    - Helps prepare for events like power loss, natural disasters, ransomware attacks, and data breaches
  - *Recovery Testing*
    - Evaluates the system's capacity to restore normal operation after a disruptive event
    - Involves executing planned recovery actions
    - Performed through failover tests, simulations, and parallel processing
    - Ensures that planned recovery procedures work effectively in a real-world scenario
  - *Tabletop Exercises*
    - Scenario-based discussion among key stakeholders
    - Assess and improve an organization's preparedness and response
    - No deployment of actual resources
    - Identifies gaps and seams in response plans
    - Promotes team-building among stakeholders

        - Low-cost and engaging for participants
    - *Failover Tests*
        - Controlled experiment for transitioning from primary to backup components
        - Ensures uninterrupted functionality during disasters
        - Requires more resources and time
        - Validates the effectiveness of disaster recovery plans
        - Can identify and rectify issues in the failover process
    - *Simulations*
        - Computer-generated representation of a real-world scenario
        - Allows for hands-on response actions in a virtual environment
        - Assesses incident responders and system administrators in real-time
        - Helps evaluate reactions and staff performance
        - Provides feedback for learning and improvement
    - *Parallel Processing*
        - Replicates data and system processes onto a secondary system
        - Runs primary and secondary systems concurrently
        - Tests reliability and stability of the secondary setup
        - Ensures no disruption to day-to-day operations
        - Assesses the system's ability to handle multiple failure scenarios simultaneously
        - Uses of Parallel Processing
            - *Resilience Testing*
                - Tests the ability of the system to handle multiple failure scenarios
            - *Recovery Testing*
                - Tests the efficiency of the system to recover from multiple points of failure

Security Architecture

Objectives:

- 3.1 - Compare and contrast security implications of different architecture models
- 4.1 - Given a scenario, apply common security techniques to computing resources

- **Security Architecture**
    - *Security Architecture*
        - Design, structure, and behavior of an organization's information security environment
    - On-Premise vs. Cloud Deployment
        - On-Premise
            - Traditional local infrastructure setup
        - Cloud
            - Delivery of computing services over the internet
    - Cloud Security Considerations
        - Shared Physical Server Vulnerabilities
        - Inadequate Virtual Environment Security
        - User Access Management
        - Lack of Up-to-date Security Measures
        - Single Point of Failure
        - Weak Authentication and Encryption Practices
        - Unclear Policies and Data Remnants

- Virtualization and Containerization
  - Different virtualization types
  - Containerization benefits and risks
  - Vulnerabilities like vm escape and resource reuse
- *Serverless Computing*
  - Cloud provider manages server allocation
  - Developers focus solely on writing code
- *Microservices Architecture*
  - Collection of small, autonomous services
  - Each performs a specific business process
- *Software-Defined Network (SDN)*
  - Dynamic, programmatically efficient network configuration
  - Improves network performance and monitoring
- *Infrastructure as Code (IaC)*
  - Automation of managing and provisioning technology stack
  - Software-driven setup instead of manual configuration
- Centralized vs. Decentralized Architectures
  - Benefits and risks of centralized and decentralized setups
- *Internet of Things (IoT)*
  - Network of physical devices with sensors and connectivity
  - Enables data exchange among connected objects
- ICS and SCADA
  - *Industrial Control Systems (ICS)*
    - For industrial production
  - *Supervisory Control and Data Acquisition (SCADA)*
    - Subset of ICS

- *Embedded Systems*
  - Dedicated computer system designed for specific functions
  - Part of a complete device system with hardware components

- **On-premise versus the Cloud**
  - *Cloud Computing*
    - Delivery of computing services over the internet, including servers, storage, databases, networking, software, analytics, and intelligence
    - Advantages
      - Faster innovation
      - Flexible resources
      - Economies of scale
  - *Responsibility Matrix*
    - Outlines the division of responsibilities between the cloud service provider and the customer
  - *Third-Party Vendors*
    - Provides specialized services to enhance functionality, security, and efficiency of cloud solutions
  - *Hybrid Solutions*
    - Combined on-premise, private cloud, and public cloud services, allowing workload flexibility
    - Considerations
      - Sensitive data is protected
      - Regulatory requirements are met
      - Systems can communicate with each other
      - The solution is cost-effectiveness

- *On-Premise Solutions*
  - Computing infrastructure physically located on-site at a business
- Key Considerations in Cloud Computing
  - Availability
    - System's ability to be accessed when needed
  - Resilience
    - System's ability to recover from failures
  - Cost
    - Consider both upfront and long-term costs
  - Responsiveness
    - Speed at which the system can adapt to demand
  - Scalability
    - System's ability to handle increased workloads
  - Ease of Deployment
    - Cloud services are easier to set up than on-premise solutions
  - Risk Transference
    - Some risks are transferred to the provider, but customers are responsible for security
  - Ease of Recovery
    - Cloud services offer easy data recovery and backup solutions
  - Patch Availability
    - Providers release patches for vulnerabilities automatically
  - Inability to Patch
    - Compatibility issues or lack of control can hinder patching

        - Power
            - Cloud provider manages infrastructure, including power supply
            - Reduces customer costs and eliminates power management concerns
        - Compute
            - Refers to computational resources, including CPUs, memory, and storage
            - Cloud providers offer various compute options to suit different needs
    - <u>Remember</u>
        - Cloud computing offers flexibility, scalability, and cost-effectiveness
        - On-premise solutions provide control and security but can be expensive and challenging to maintain
        - Hybrid solutions offer flexibility and control but require considerations of security, compliance, interoperability, and cost

- **Cloud Security**
    - Shared Physical Server Vulnerabilities
        - In cloud environments, multiple users share the same physical server
            - Compromised data from one user can potentially impact others on the same server
        - Mitigation
            - Implement strong isolation mechanisms (e.g., hypervisor protection, secure multi-tenancy)
            - Perform regular vulnerability scanning, and patch security gaps
    - Inadequate Virtual Environment Security
        - Virtualization is essential in cloud computing
            - Inadequate security in the virtual environment can lead to unauthorized access and data breaches

- Mitigation
  - Use secure VM templates
  - Regularly update and patch VMs
  - Monitor for unusual activities
  - Employ network segmentation to isolate VMs
- User Access Management
  - Weak user access management can result in unauthorized access to sensitive data and systems
  - Mitigation
    - Enforce strong password policies
    - Implement multi-factor authentication
    - Limit user permissions (Principle of Least Privilege)
    - Monitor user activities for suspicious behavior
- Lack of Up-to-date Security Measures
  - Cloud environments are dynamic and require up-to-date security measures
    - Failure to update can leave systems vulnerable to new threats
  - Mitigation
    - Regularly update and patch software and systems
    - Review and update security policies
    - Stay informed about the latest threats and best practices
- Single Point of Failure
  - Cloud services relying on specific resources or processes can lead to system-wide outages if they fail
  - Mitigation
    - Implement redundancy and failover procedures
    - Use multiple servers, data centers, or cloud providers

        - Regularly test failover procedures
    - Weak Authentication and Encryption Practices
        - Weak authentication and encryption can expose cloud systems and data
        - Mitigation
            - Use multi-factor authentication
            - Strong encryption algorithms
            - Secure key management practices
    - Unclear Policies
        - Unclear security policies can lead to confusion and inconsistencies in implementing security measures
        - Mitigation
            - Develop clear, comprehensive security policies covering data handling, access control, incident response, and more
            - Regularly review and update policies and provide effective communication and training
    - Data Remnants
        - *Data Remnants*
            - Residual data left behind after deletion or erasure processes
            - In a cloud environment, data may not be completely removed, posing a security risk
        - Mitigation
            - Implement secure data deletion procedures
            - Use secure deletion methods
            - Manage backups securely
            - Verify data removal after deletion
    - <u>Remember</u> that cloud security is a shared responsibility

- **Virtualization and Containerization**
  - *Virtualization*
    - Emulates servers, each with its own OS within a virtual machine
  - *Containerization*
    - Lightweight alternative, encapsulating apps with their OS environment
    - Key Benefits
      - Efficiency and Speed
      - Portability
      - Scalability
      - Isolation
      - Consistency
  - Hypervisors
    - Two Types of Hypervisors
      - *Type 1 (Bare Metal)*
        - Runs directly on hardware (e.g., Hyper-V, XenServer, ESXi)
      - *Type 2 (Hosted)*
        - Operates within a standard OS (e.g., VirtualBox, VMware)
  - Virtualization Vulnerabilities
    - *Virtual Machine (VM) Escape*
      - Attackers break out of isolated VMs to access the hypervisor
    - *Privilege Elevation*
      - Unauthorized elevation to higher-level users
    - *Live VM Migration*
      - Attacker captures unencrypted data between servers

        - *Resource Reuse*
            - Improper clearing of resources may expose sensitive data
    - Containerization Technologies
        - Docker, Kubernetes, Red Hat OpenShift are popular containerization platforms
        - Revolutionized application deployment in cloud environments
    - Securing Virtual Machines
        - Regularly update OS, applications, and apply security patches
        - Install antivirus solutions and software firewalls
        - Use strong passwords and implement security policies
        - Secure the hypervisor with manufacturer-released patches
        - Limit VM connections to physical machines and isolate infected VMs
        - Distribute VMs among multiple servers to prevent resource exhaustion
        - Monitor VMs to prevent "Virtualization Sprawl"
        - Enable encryption of VM files for data safety and confidentiality

- **Serverless**
    - What is Serverless?
        - Serverless computing doesn't mean no servers; it shifts server management away from developers
        - Relies on cloud service providers to handle server management, databases, and some application logic
        - *Functions as a Service (FaaS) Model*
            - Developers write and deploy individual functions triggered by events
    - Benefits of Serverless
        - Reduced operational costs
            - Pay only for compute time used, no charges when code is idle

        - Automatic scaling
            - Cloud provider scales resources based on workload, ensuring optimal capacity
        - Focus on core product
            - Developers can concentrate on application functionality, not server management
        - Faster time to market
            - Reduced infrastructure concerns speed up application development
    - Challenges and Risks
        - Vendor Lock-in
            - Reliance on proprietary interfaces limits flexibility and may increase costs
        - Immaturity of best practices
            - Serverless is a relatively new field, and best practices are still evolving
    - Not a one-size-fits-all solution
        - Consider the specific needs and requirements of your application; serverless introduces challenges like Vendor Lock-in and service provider dependencies

- **Microservices**
    - *Microservices*
        - Architectural style for breaking down large applications into small, independent services
        - Each microservice runs a unique process and communicates through a well-defined, lightweight mechanism
        - Contrasts with traditional monolithic architecture, where all components are interconnected
            - Each service in the microservice architecture is self-contained and able to

run independently

- Advantages of Microservices
  - Scalability
    - Services can be scaled independently based on demand
  - Flexibility
    - Microservices can use different technologies and be managed by different teams
  - Resilience
    - Isolation reduces the risk of system-wide failures
  - Faster Deployments and Updates
    - Independent deployment and updates allow for agility and reduced deployment risk
- Challenges of Microservices
  - Complexity
    - Managing multiple services involves inter-service communication, data consistency, and distributed system testing
  - Data Management
    - Each microservice can have its own database, leading to data consistency challenges
  - Network Latency
    - Increased inter-service communication can result in network latency and slower response times
  - Security
    - The distributed nature of microservices increases the attack surface, requiring robust security measures

- **Network Infrastructure**
  - *Network Infrastructure*
    - Backbone of modern organizations
    - Comprises hardware, software, services, and facilities for network support and management
  - *Physical Separation*
    - Security measures to protect sensitive information
    - Often referred to as "Air Gapping"
    - Isolates a system by physically disconnecting it from all networks
    - Physical separation is one of the most secure methods of security, but it is still vulnerable to sophisticated attacks
  - *Logical Separation*
    - Establishes boundaries within a network to restrict access to certain areas
    - Implemented using firewalls, VLANs, and network devices
  - Comparison
    - Physical Separation (Air-Gapping)
      - High security, complete isolation
    - Logical Separation
      - More flexible, easier to implement
      - Less secure if not configured properly

- **Software-defined Network (SDN)**
  - *Software-Defined Network (SDN)*
    - Revolutionary approach to network management
    - Enables dynamic, programmatically efficient network configuration
    - Improves network performance and monitoring

        - Reduces complexity in static and inflexible network architectures
        - Provides a centralized view of the entire network
    - *SDN Architecture*
        - Decouples network control and forwarding functions
        - Three Distinct Planes
            - *Data Plane (Forwarding Plane)*
                - Responsible for handling data packets
                - Makes decisions based on protocols like IP and Ethernet
                - Concerned with sending and receiving data
            - *Control Plane*
                - Centralized decision-maker in SDN
                - Dictates traffic flow across the entire network
                - Replaces traditional, distributed router control planes
                - Increases network manageability and flexibility
            - *Application Plane*
                - Hosts all network applications that interact with the SDN controller
                - Applications instruct the controller on network management
                - Controller manipulates the network based on these instructions

- **Infrastructure as Code (IaC)**
    - *Infrastructure as Code (IaC)*
        - Modern approach to IT infrastructure management
        - Automates provisioning and management through code
        - Used in DevOps and with cloud computing

- IaC Method
  - Developers and ops teams manage infrastructure through code
  - Code files are versioned, tested, and audited
  - High-level languages like YAML, JSON, or domain-specific languages (e.g., HCL) used
  - Idempotence ensures identical environments
    - *Idempotence*
      - Operation consistently produces the same results
      - Crucial for consistency and reliability in multiple environments
- Benefits of IaC
  - Speed and Efficiency
  - Consistency and Standardization
  - Scalability
  - Cost Savings
  - Auditability and Compliance
- Challenges
  - Learning Curve
    - New skills and mindset required
    - Teams learn to write, test, and maintain infrastructure code
  - Complexity
    - Infrastructure code can become complex
    - Mitigated with modularization and documentation
  - Security Risks
    - Sensitive data exposure in code files
    - Insecure configurations may be introduced

- **Centralized vs Decentralized Architectures**
  - *Centralized Architecture*
    - All computing functions managed from a single location or authority
    - Components
      - Central Server
      - Mainframe
      - Data Center
    - Data and applications stored in one place, accessed via a network
    - Benefits
      - Efficiency and Control
        - High resource control and efficient resource allocation
      - Consistency
        - Ensures uniform and accurate data across the organization
      - Cost-effective
        - Reduced maintenance and infrastructure costs
    - Risks
      - Single Point of Failure
        - Server failure can disrupt the entire network
      - Scalability Issues
        - Struggles to handle growth, leading to performance problems
      - Security Risks
        - Attractive targets for cybercriminals; compromised server risks data and app security
  - *Decentralized Architecture*
    - Computing functions distributed across multiple systems or locations

- No single point of control; each node operates independently
- Benefits
  - Resilience
    - Can continue functioning despite individual node failures
  - Scalability
    - Easily scales with organization growth by adding new nodes
  - Flexibility
    - Supports remote work and distributed teams
- Risks
  - Security Risks
    - Vulnerable to security threats, especially in remote work scenarios
  - Management Challenges
    - Complex management, coordinating multiple nodes
  - Data Inconsistency
    - Potential issues with data consistency and synchronization
- Considerations for Choosing Architecture
  - Choice depends on the organization's specific needs and context
  - Centralized systems for
    - Data accuracy and resource management priorities
  - Decentralized systems for
    - Resilience, flexibility, and rapid scaling needs

- **Internet of Things (IoT)**
  - *Internet of Things (IoT)*
    - Network of physical devices with sensors, software, and connectivity
    - Enables data exchange among connected objects

- *Hub/Control System*
  - Central component connecting IoT devices
  - Collects, processes, analyzes data, and sends commands
  - Can be a physical device or software platform
- *Smart Devices*
  - Everyday objects enhanced with computing and internet capabilities
  - Sense environment, process data, and perform tasks autonomously
- *Wearables*
  - Subset of smart devices worn on the body
  - Monitor health, provide real-time information, and offer hands-free interface
- *Sensors*
  - Detect changes in environment, convert into data
  - Measure various parameters (temperature, motion, etc.)
  - Enable interaction and autonomous decisions in smart devices
- IoT Risks
  - Weak Default Settings
    - Common security risk
    - Default usernames/passwords are easy targets for hackers
    - Changing defaults upon installation is essential
  - Poorly Configured Network Services
    - Devices may have vulnerabilities due to open ports, unencrypted communications
    - Unnecessary services can increase attack surface
    - Keeping IoT devices on a separate network is recommended

- **ICS and SCADA**
  - *Industrial Control Systems (ICS)*
    - Systems used to monitor and control industrial processes, found in various industries like electrical, water, oil, gas, and data
    - *Distributed Control Systems (DCS)*
      - Used in control production systems within a single location
    - *Programmable Logic Controllers (PLCs)*
      - Used to control specific processes such as assembly lines and factories
  - *Supervisory Control and Data Acquisition (SCADA) Systems*
    - Type of ICS designed for monitoring and controlling geographically dispersed industrial processes
    - Common in industries like
      - Electric power generation, transmission, and distribution systems
      - Water treatment and distribution systems
      - Oil and gas pipeline monitoring and control systems
  - Risks and Vulnerabilities
    - Unauthorized Access
      - Unauthorized individuals can manipulate system operations without proper protection
    - Malware Attacks
      - Vulnerable to disruptive malware attacks
    - Lack of Updates
      - Running outdated software with unpatched vulnerabilities
    - Physical Threats
      - Susceptible to damage to hardware or infrastructure

- Securing ICS and SCADA Systems
  - Implement Strong Access Controls
    - Strong passwords
    - Two-factor authentication
    - Limited access to authorized personnel only
  - Regularly Update and Patch Systems
    - Keep systems updated to protect against known vulnerabilities
  - Use Firewall and Intrusion Detection Systems
    - Detect and prevent unauthorized access
  - Conduct Regular Security Audits
    - Identify and address potential vulnerabilities through routine assessments
  - Employee Training
    - Train employees on security awareness and response to potential threats

- **Embedded Systems**
  - *Embedded Systems*
    - Specialized computing components designed for dedicated functions within larger devices
    - They integrate hardware and mechanical elements and are essential for various daily-use devices
  - *Real-Time Operating System (RTOS)*
    - Designed for real-time applications that process data without significant delays
    - Critical for time-sensitive applications like flight navigation and medical equipment

- Risks and Vulnerabilities in Embedded Systems
  - Hardware Failure
    - Prone to failure in harsh environments
  - Software Bugs
    - Can cause system malfunctions and safety risks
  - Security Vulnerabilities
    - Vulnerable to cyber-attacks and unauthorized access
  - Outdated Systems
    - Aging software and hardware can be more susceptible to attacks
- Key Security Strategies for Embedded Systems
  - *Network Segmentation*
    - Divide the network into segments to limit potential damage in case of a breach
  - *Wrappers (e.g., IPSec)*
    - Protect data during transfer by hiding data interception points
  - *Firmware Code Control*
    - Manage low-level software to maintain system integrity
  - Challenges in Patching
    - Updates face operational constraints; OTA updates demand meticulous planning and security measures
      - *Over-the-Air (OTA) Updates*
        - Patches are delivered and installed remotely

Security Infrastructure

Objectives:

- 3.2 - Given a scenario, you must be able to apply security principles to secure enterprise architecture
- 4.5 - Given a scenario, you must be able to modify enterprise capabilities to enhance security

- **Security Infrastructure**
    - *Security Infrastructure*
        - Encompasses hardware, software, networks, data, and policies working cohesively for information asset safeguarding
    - Firewalls
        - Types
            - Web Application
            - Unified Threat Management
            - Next-generation
    - Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
        - Mechanisms
            - Identifying trends
            - Showcasing signatures
    - *Network Appliances*
        - *Specialized hardware or software for specific networking functions*
        - Functions
            - Load Balancing
            - Proxying

            - Monitoring
            - Security Enforcement
    - *Port Security*
        - Restricting and controlling network access
        - *Basis*
            - Media Access Control (MAC) addresses
        - *Concepts*
            - 802.1x and EAP
    - Securing Network Communications
        - Technologies
            - VPNs
            - IPSec
            - TLS
        - Objective
            - Create a secure backbone for communication
    - Software-Defined Wide Area Networks (SD-WAN) and Secure Access Service Edge (SASE)
        - *SD-WAN*
            - Optimize WAN connections with software-defined principles
        - *SASE*
            - Cloud-based service integrating security and wide area networking
    - Infrastructure Considerations
        - Aspects
            - Device placement, security zones, screen subnets, attack surfaces
        - Connectivity
            - Concerns and considerations

        - Device Attributes
            - Active vs. passive, inline vs. taps or monitors
        - Failure Mode Options
            - Fail-open or fail-closed for security devices
    - Selection of Infrastructure Controls
        - Choosing controls aligned with network needs
        - *Tailoring*
            - Ensuring robust security architecture

- **Ports and Protocols**
    - *Ports*
        - Logical communication endpoints on a computer or server
        - Classified as either
            - *Inbound*
                - Listening for connections
            - *Outbound*
                - Used to connect to a server
        - Example
            - SSH connection with an inbound port 22 and an outbound port on the client
    - Port Classification
        - *Well-Known Ports (0-1023)*
            - Assigned by IANA, commonly-used protocols
        - *Registered Ports (1024-49151)*
            - Vendor-specific, registered with IANA

- *Dynamic and Private Ports (49152-65535)*
    - Temporary outbound connections
- *Protocols*
    - Rules governing device communication and data exchange
    - Example
        - HTTPS (port 443) uses the HTTPS protocol for secure web communication
- Memorization Tips
    - Memorize for each port
        - Port number
        - Default protocol
        - Support for TCP or UDP
        - Basic description of the port or protocol
- List of Ports and Protocols
    - Port 21: FTP (File Transfer Protocol) - TCP
    - Port 22: SSH, SCP, SFTP - TCP
    - Port 23: Telnet - TCP
    - Port 25: SMTP (Simple Mail Transfer Protocol) - TCP
    - Port 53: DNS (Domain Name System) - TCP/UDP
    - Port 69: TFTP (Trivial File Transfer Protocol) - UDP
    - Port 80: HTTP (Hypertext Transfer Protocol) - TCP
    - Port 88: Kerberos - UDP
    - Port 110: POP3 (Post Office Protocol) - TCP
    - Port 119: NNTP (Network News Transfer Protocol) - TCP
    - Port 135: RPC (Remote Procedure Call) - TCP/UDP
    - Ports 137, 138, 139: NetBIOS - TCP/UDP
    - Port 143: IMAP (Internet Message Access Protocol) - TCP

- Port 161: SNMP (Simple Network Management Protocol) - UDP
- Port 162: SNMPTrap - UDP
- Port 389: LDAP (Lightweight Directory Access Protocol) - TCP
- Port 443: HTTPS (HTTP Secure) - TCP
- Port 445: SMB (Server Message Block) - TCP
- Ports 465, 587: SMTPS (SMTP Secure) - TCP
- Port 514: Syslog - UDP
- Port 636: LDAPS (LDAP Secure) - TCP
- Port 993: IMAPS (IMAP over SSL/TLS) - TCP
- Port 995: POP3S (POP3 over SSL/TLS) - TCP
- Port 1433: Microsoft SQL - TCP
- Ports 1645, 1646: RADIUS (Remote Authentication) - TCP
- Ports 1812, 1813: RADIUS UDP - UDP
- Port 3389: RDP (Remote Desktop Protocol) - TCP
- Port 6514: Syslog TLS - TCP

- <u>Study Tips</u>
  - Create flashcards with protocol, port, and connection details
  - Regularly test yourself to memorize ports and protocols
  - Understanding these is crucial for success in exams related to cybersecurity

- **Firewalls**
  - *Firewall*
    - A network security device or software that monitors and controls network traffic based on security rules
    - Protects networks from unauthorized access and potential threats

- *Screened Subnet (Dual-homed Host)*
  - Acts as a security barrier between external untrusted networks and internal trusted networks using a protected host with security measures like a packet-filtering firewall
- Types of Firewalls
  - *Packet Filtering Firewalls*
    - Inspect packet headers for IP addresses and port numbers
    - Limited in inspection, operates at Layer 4 (Transport Layer)
  - *Stateful Firewalls*
    - Track connections and requests, allowing return traffic for outbound requests
    - Operates at Layer 4, with improved awareness of connection state
  - *Proxy Firewalls*
    - Make connections on behalf of endpoints, enhancing security
    - Two Types of Proxy Firewalls
      - Circuit level (Layer 5)
      - Application level (Layer 7)
  - *Kernel Proxy Firewalls*
    - Minimal impact on network performance, full inspection of packets at every layer
    - Placed close to the system they protect
- Firewall Evolutions
  - *Next Generation Firewall (NGFW)*
    - *Application-aware*
      - distinguish between different types of traffic
    - Conduct deep packet inspection and use signature-based intrusion

protection

- Operate fast within minimal network performance impact
- Offer full-stack traffic visibility
- Can integrate with other security products
    - Can be a problem if organizations become reliant on a single vendor due to firewall configurations tailored to one product line

- *Unified Threat Management (UTM) Firewall*
    - Combines multiple security functions in a single device
    - Functions include firewall, intrusion prevention, antivirus, and more
    - Reduces the number of devices
    - Are a single point of failure
    - UTMs use separate individual engine
        - NGFW uses a single engine
- *Web Application Firewall (WAF)*
    - Focuses on inspecting HTTP traffic
    - Prevents common web application attacks like cross-site scripting and SQL injections
    - Can be placed
        - In-line (live attack prevention)
            - Device sits between the network firewall and the web servers
        - Out of band (detection)
            - Device receives a mirrored copy of web server traffic

- Layer based Firewalls
    - *Layer 4 Firewall*
        - Operates at the transport layer

            - Filters traffic based on port numbers and protocol data
        - *Layer 7 Firewall*
            - Operates at the application layer
            - Inspects, filters, and controls traffic based on content and data characteristics

- **Configuring Firewalls**
    - Firewalls and Access Control Lists (ACLs)
        - *Firewalls*
            - Dedicated devices for using Access Control Lists (ACLs) to protect networks
        - *Access Control Lists (ACLs)*
            - Essential for securing networks from unwanted traffic
            - Consist of permit and deny statements, often based on port numbers
            - Rule sets placed on firewalls, routers, and network infrastructure devices
            - Control the flow of traffic into and out of networks
            - May define quality of service levels inside networks but are primarily used for network security in firewalls
    - Configuring ACLs
        - A web-based interface or a text-based command line interface can be used
        - The order of ACL rules specifies the order of actions taken on traffic (top-down)
        - The first matching rule is executed, and no other ACLs are checked
        - Place the most specific rules at the top and generic rules at the bottom
        - Some devices support implied deny functions, while others require a "deny all" rule at the end
        - Actions taken by network devices should be logged, including deny actions

- ACL Rules
  - Made up of some key pieces of information including
    - Type of traffic
    - Source of traffic
    - Destination of traffic
    - Action to be taken against the traffic
- Firewall Types
  - *Hardware-Based Firewall*
    - A dedicated network security device that filters and controls network traffic at the hardware level
    - Commonly used to protect an entire network or subnet by implementing ACLs and rules
  - *Software-Based Firewall*
    - A firewall that runs as a software application on individual devices, such as workstations
    - Utilizes ACLs and rules to manage incoming and outgoing traffic, providing security at the software level on a per-device basis
- Key Takeaway
  - Firewalls use ACLs to control network traffic, ensuring security by specifying permitted and denied actions
  - Proper ACL configuration and rule order are crucial for effective network protection

- **IDS and IPS**
  - Key difference
    - IDS - Logs and alerts
    - IPS - Logs, alerts, and takes action
  - *Intrusion Detection Systems (IDS)*
    - Logs or alerts that it found something suspicious or malicious
    - Three Types of Intrusion Detection Systems (IDS)
      - *Network-based IDS (NIDS)*
        - Monitors the traffic coming in and out of a network
      - *Host-based IDS (HIDS)*
        - Looks at suspicious network traffic going to or from a single or endpoint
      - *Wireless IDS (WIDS)*
        - Detects attempts to cause a denial of a service on a wireless network
    - Intrusion detection systems operate either using signature-based or anomaly-based detection algorithms
      - *Signature-based IDS*
        - Analyzes traffic based on defined signatures and can only recognize attacks based on previously identified attacks in its database
          - *Pattern-matching*
            - Specific pattern of steps
            - NIDS, WIDS
          - *Stateful-matching*
            - Known system baseline

- HIDS
- *Anomaly-based IDS*
  - Analyzes traffic and compares it to a normal baseline of traffic to determine whether a threat is occurring
  - Five Types of Anomaly-based Detection Systems
    - Statistical
    - Protocol
    - Traffic
    - Rule or Heuristic
    - Application-based
- *Intrusion Prevention Systems (IPS)*
  - Logs, alerts, and takes action when it finds something suspicious or malicious
  - Scans traffic to look for malicious activity and takes action to stop it

- **Network Appliances**
  - *Network Appliance*
    - A dedicated hardware device with pre-installed software for specific networking services
  - Different Types of Network Appliances
    - *Load Balancers*
      - Distribute network/application traffic across multiple servers
      - Enhance server efficiency and prevent overload
      - Ensure redundancy and reliability
      - Perform continuous health checks
      - Application Delivery Controllers (ADCs) offer advanced functionality
      - Essential for high-demand environments and high-traffic websites

- *Proxy Servers*
  - Act as intermediaries between clients and servers
  - Provide content caching, requests filtering, and login management
  - Enhance request speed and reduce bandwidth usage
  - Add a security layer and enforce network utilization policies
  - Protect against DDoS attacks
  - Facilitate load balancing and user authentication
  - Handle data encryption and ensure compliance with data sovereignty laws
- *Sensors*
  - Monitor, detect, and analyze network traffic and data flow
  - Identify unusual activities, security breaches, and performance issues
  - Provide real-time insights for proactive network management
  - Aid in performance monitoring and alerting
  - Act as the first line of defense against cyber threats
- *Jump Servers/Jump Box*
  - Secure gateways for system administrators to access devices in different security zones
  - Control access and reduce the attack surface area
  - Offer protection against downtime and data breaches
  - Simplify logging and auditing
  - Speed up incident response during cyber-attacks
  - Streamline system management and maintenance
  - Host essential tools and scripts
  - Monitor system health for performance and security

- **Port Security**
  - *Port Security*
    - A network switch feature that restricts device access to specific ports based on MAC addresses
    - Enhances network security by preventing unauthorized devices from connecting
  - *Network Switches*
    - Networking devices that operate at Layer 2 of the OSI model
    - Use MAC addresses for traffic switching decisions through transparent bridging
    - Efficiently prevent collisions, operate in full duplex mode
    - Remember connected devices based on MAC addresses
    - Broadcast traffic only to intended receivers, increasing security
  - *CAM Table (Content Addressable Memory)*
    - Stores MAC addresses associated with switch ports
    - Vulnerable to MAC flooding attacks, which can cause the switch to fail open
  - Port Security Implementation
    - Associate specific MAC addresses with interfaces
    - Prevent unauthorized devices from connecting
    - Can use Sticky MACs for easier setup
    - Susceptible to MAC spoofing attacks
  - *802.1x Authentication*
    - Provides port-based authentication for wired and wireless networks
    - Requires three roles
      - Supplicant
      - Authenticator
      - Authentication server
    - Utilizes RADIUS or TACACS+ for actual authentication