SECURITY+ SYO-701 NOTES

Your Trusted Companion for Security+ Success

Yogesh Rathod

Table of Contents

Chapter 1 – Today's Security Professional

Cybersecurity Objectives

CIA Triad

Confidentiality

- Certain information should be only known to certain people.
- Includes Encryption
- Includes access controls.
- May have two factor authentication for reconfirmation to share the resource.

Integrity

- Data is stored and transferred as intended.
- Includes ***hashing*** which maps data of an arbitrary length to the fixed length.
- Includes digital signatures.
- Certificates
- Non-repudiation

Availability

- Systems and networks must be up and running.
- Fault tolerant systems
- To make available Managed and updated by Patching the systems.

DAD Triad

Disclosure exposes sensitive information, violating confidentiality, through data exfiltration by attackers, accidental misconfigurations, or lost devices.

Alteration modifies data without authorization, breaching integrity, through attacks, natural events, or accidental user errors.

Denial disrupts access, violating availability, via DDoS attacks, server failures, or natural disasters.

AAA framework

Identification

- This is who you claim to be.

Authentication

- Prove you are who you say you are.
- Password and other authentication factors.

Authorization

- Based on your identification and authentication, what access do you have?

Accounting

- Resources used: Login time, data sent and received, logout time.

Breach Impact

Financial Risk: the risk of monetary damage to the organization as the result of a data breach.

Reputational Risk: when the negative publicity surrounding a security breach causes the loss of goodwill among customers, employees, suppliers, and other stakeholders.

Strategic Risks: Strategic risk is the risk that an organization will become less effective in meeting its major goals and objectives because of the breach.

Operational Risk: Operational risk is risk to the organization's ability to carry out its day-to-day functions.

Compliance Risk: Compliance risk occurs when a security breach causes an organization to run afoul of legal or regulatory requirements.

Implementing Security Controls

Gap Analysis

- Gap Analysis simply means "***where***" you are right now and where you want to be.
- The "***gap***" between the two.
- This can take weeks or months and may require extensive research.

Gap analysis includes

- Evaluate people and processes.
- Working towards the baseline.
- Determine the end goal.
- Evaluate existing systems and their weaknesses.
- Final comparison
  - Detailed baseline objectives.
  - A clear view of the current state.
- Need a path to get from the current security to the goal.
- Time to create the gap analysis report.

Zero Trust

- Zero trust is a holistic approach to network security.
  - Covers every device, every process, and every person.
- Everything must be verified.
  - Nothing is inherently trusted.
  - Multifactor authentication, encryption, system permissions, additional firewalls, monitoring, and analytics, etc.

Planes of operation

- Split the network into functional planes.
  - Applies to physical, virtual and cloud components.

Data plane

- Process the frames, packets, and network data.
- Processing, forwarding, trunking, encrypting, NAT.

Control plane

- Manages the actions of the data plane.
- Defines policy and rules.
- Determines how packets should be forwarded.
- Routing tables, session tables, NAT tables.

Controlling Trust

Adaptive Identity

- Consider the source and the requested resources.
- Multiple risk indicators – relationship to the organization, physical location, type of connection, IP address, etc.
- Make the authentication strong, if needed.

Threat scope reduction

- Decrease the number of possible entry points.

Policy-driven access control

- Combine the adaptive identity with a predefined set of rules.

Security Zones

- Security is more than a one-to-one relationship.
  - Broad categorizations provide a security-related foundation.
- Where are you coming from and where are you going?
  - Trusted, untrusted.
  - Internal network, external network
  - VPN1, VPN5
  - Marketing, IT, Accounting, Human Resources
- Using the zones may be enough by itself to deny access.

Security Control Categories

Technical controls safeguard confidentiality, integrity, and availability in the digital domain through tools like firewalls, access control lists, intrusion prevention systems, and encryption.
Operational controls involve processes ensuring secure technology management, such as user access reviews, log monitoring, and vulnerability assessments.
Managerial controls are procedural methods addressing risk management, including risk assessments, security planning, and integrating security into change management, service acquisition, and project management.
Physical controls enhance security in the physical realm using measures like fences, locks, perimeter lighting, fire suppression systems, and burglar alarms.

Data Protection

Three types of data states are:

Data at rest is stored on media like hard drives or cloud storage, vulnerable to theft by insiders or attackers.
Data in transit moves over networks and risks eavesdropping on untrusted connections.
Data in use resides in memory during processing and can be stolen if attackers control the system.

Data Loss Prevention

Data Loss Prevention (DLP) systems enforce policies to prevent data theft, scanning for sensitive data, monitoring traffic, and blocking unauthorized transmissions while alerting administrators.

Agent-based DLP: Uses installed software to detect and secure sensitive data on systems, monitor configurations, and block actions like USB use.
Agentless DLP: Monitors outbound network traffic to block unencrypted sensitive data and can apply encryption, especially for emails.

Mechanisms:

- Pattern Matching: Identifies sensitive data formats or keywords.
- Watermarking: Tracks tagged documents to prevent unencrypted sharing, also used in DRM solutions.

Data Minimization

Data minimization reduces risk by limiting sensitive information, primarily through data destruction or transforming data to deidentify individuals.
Deidentification: Removes links to individuals, reducing sensitivity.
Obfuscation Techniques:
Hashing: Converts data to hash values using strong functions but is vulnerable to rainbow table attacks.
Tokenization: Replaces sensitive values with unique identifiers using secure lookup tables.
Masking: Redacts data by replacing parts with blank characters (e.g., masking credit card numbers).

Chapter 2 – Cybersecurity Threat Landscape

Threat Actors

Nation States

- It might be an external entity like govt or national security.
- Many possible motivations like disruption, war, revenge.
- Constant attacks due to massive resources.
- Can perform high sophistication level attacks due to military control, utilities, financial control.

Unskilled Attackers

- Attacker does not know what's really happening.
- Also called ***script kiddies***
- Not very sophisticated

Hacktivist

- A hacker with a purpose.
- Motivated by ***philosophy***, revenge, disruption, etc.
- Often an external entity.
- Can be very sophisticated.
- Can perform specific hacks like DOS, website defacing, private document disclosure.
- Funding maybe limited.
- Example: "Anonymous" hacktivist group.

Insider threat

- Has extensive resources
- Motivated by revenge, financial gain.
- Medium level of sophistication
- The insider knows what to hit and can direct the attacks to vulnerable systems.

Organized crimes

- Professional criminals
- Motivated by money.
- Very sophisticated
- One person hacks, one person manages the exploits, another person sells the data, another handles customer support.
- Lots of capital to fund hacking efforts.
- Example: Russian Mafia

Shadow IT

- Working around the internal IT organization
- Builds their own infrastructure.
- Limited by company's budget
- Medium sophistication
- May not have IT training knowledge.

Motivations of an attacker

Attackers may be motivated by many different drivers. Common motivations for attack include:

- Data Exfiltration
- Espionage
- Service disruption
- Blackmail
- Financial gain
- Philosophical or political beliefs
- Revenge
- Disruption and chaos
- War

Threat actor	Location	Resources	Sophistication	Possible motivations
Nation state	External	Extensive	Very high	Data exfiltration, philosophical, revenge, disruption, war
Unskilled	External	Limited	Very low	Disruption, data exfiltration, philosophical beliefs
Hacktivist	External	Some funding	Can be high	Philosophical beliefs, revenge, disruption/chaos
Insider threat	Internal	Many resources	Medium	Revenge, financial gain
Organized crime	External	Often extensive	Very high	Financial
Shadow IT	Internal	Many resources	Limited	Philosophical beliefs, revenge

Figure 1 - Threat Actors (Reference: Professor Messer)

Threat Vectors (Entry point for attackers)

Message-based Threat Vectors

- Email Phishing
- Text/SMS Phishing
- Voice Phishing (Vishing)

Wired Networks

- Don’t need to gain physical access to the network
- Bluetooth
- Unsecure interfaces – No 802.1X

Wireless

- Outdated security protocols.
- Open or rogue wireless networks.

Systems
- Open ports and services
- Usage of legacy and outdated applications
- Unpatched software

Files and Images
- Embedding malicious payload in a file
- Sent by email, stored in a server

Removable Devices
- USB sticks to spread malware

Cloud
- Improper access controls
- Accidentally published API keys
- Security Flaws

Supply Chain
- Provides an indirect mechanism to attack the organization.
- If there is flaw in third party service used by a firm, it may be an entry point to the firm using that service.

Default credentials:
- Most devices have default usernames and passwords for admins too.

Assessing Threat Intelligence
Regardless of the source of your threat intelligence information, you need to assess it. Common factors are:
Is it timely? A feed that is operating on delay can cause you to miss a threat.
Is the information accurate? Can you rely on what it says
Is the information relevant? What if it describes the wrong platform, software, or reason for the organization to be targeted?

Threat Management and Exchange

STIX (Structured Threat Information Expression) A standardized language for sharing and analyzing cyber threat intelligence.

AIS (Automated Indicator Sharing) US government initiative for real-time sharing of cyber threat indicators.

TAXII (Trusted Automated Exchange of Intelligence Information) A protocol for securely sharing cyber threat intelligence using STIX.

Chapter 3 – Malicious Code

Types of Malwares

Ransomware: Ransomware is malware that takes over a computer and then demands a ransom.

Trojan: Trojans, or Trojan horses, are a type of malware that is typically disguised as legitimate software. They are called Trojan horses because they rely on unsuspecting individuals running them, thus providing attackers with a path into a system.

Worms: Unlike Trojans that require user interaction, ***worms spread themselves***. Worms also self-install, rather than requiring users to click on them, making them quite dangerous. (example: Stuxnet – Nationwide Worm attack)

Spyware: Spyware is malware that is designed to obtain information about an individual, organization, or system. Many spyware packages track users' browsing habits, installed software, or similar information and report it back to central servers.

Bloatware: unwanted applications installed on systems by manufacturers. It is not usually intentionally malicious.

Virus: Computer viruses are malicious programs that self-copy and self-replicate once they are activated. They can't spread themselves; they need some interaction or medium. Virus has ***trigger*** and ***payload*.**

Keyloggers: Keyloggers are programs that capture keystrokes from a keyboard, although keylogger applications may also capture other input such as mouse movement, touchscreen inputs, or credit card swipes from attached devices

Logic Bombs: They are not independent malicious programs, rather they are **functions or code** placed inside other programs that will activate when set conditions are met.

Rootkits: Rootkits are malware that is specifically designed to allow attackers to access a system through a backdoor. Once a rootkit is discovered, removal can be challenging. Common IoCs for rootkits include:

1. File hashes and signatures
2. Command and control domains, IP addresses, and systems
3. Behavior-based identification like the creation of services, executables, configuration changes, file access, and command invocation.
4. Opening ports or creation of reverse proxy tunnels.

Bots: Bots connect to command and control (C&C) systems, allowing them to be updated, controlled, and managed remotely.

Chapter 4 – Social Engineering and Password Attacks

Social Engineering Techniques

Phishing
Fraudulent attempts to acquire sensitive information, often via email, but also through methods like **smishing** (SMS) and **vishing** (phone calls).
Spear Phishing: Targets specific individuals or groups, while **whaling** focuses on high-level executives like CEOs and CFOs.

Vishing
Vishing is phishing accomplished via voice or voicemail messages. Common vishing scams include requests to help a relative or friend in another country, leading to wire fraud; various tax scams, particularly during tax season in the United States; threats of law enforcement action; and requests for a staff member to perform a task for a senior executive.

Smishing
Smishing relies on text messages as part of the phishing scam. Smishing scams frequently attempt to get users to click on a link in a text message. Smishing attacks rely on similar **pretexts** to build trust or urgency.

Misinformation and Disinformation

It can be a bit confusing distinguishing between misinformation and disinformation.
Misinformation = Incorrect Information
Disinformation = Inaccurate/incorrect or outright false information that was intentionally provided to serve an individual or organization's goals.

Impersonation
Pretending to be someone else, or impersonation, is a key tool in a social engineer's toolkit. Identity fraud, or identity theft, is the use of someone else's identity. identity fraud may be used as part of penetration tests or other security efforts as well.

Business Email Compromises (BEC)
Business email compromise, often called BEC, relies on using apparently legitimate email addresses to conduct scams and other attacks.
- Using compromised accounts.
- Sending spoofed emails.
- Using common fake but similar domain techniques.
- Using malware or other tools.

Pretexting
Pretexting is the process of using a made-up scenario to justify why you are approaching an individual.

Watering Hole Attacks

Watering hole attacks use websites that targets frequent to attack them. These frequently visited sites act like a watering hole for animals and allow the attackers to stage an attack, knowing that the victims will visit the site.

Watching the watering hole

- Configure defense-in-depth for understanding how the attack took place.
- Use IPS and firewalls to stop the network traffic before things get bad.

Brand Impersonation

Intended to appear to be from a legitimate brand, relying on name recognition and even using email templates used by the brand itself.

Typosquatting

Typosquatters use misspelled and slightly off but like the legitimate site URLs to conduct typosquatting attacks. A ***related form*** of attack is known as ***pharming***. Unlike typosquatting, pharming relies either on changing a system's hosts file (which is the first reference a system checks when looking up DNS entries), or on active malware on the system that changes the system's DNS servers.

Password Attacks

Brute-force attack

- which iterate through passwords until they find one that works.

Password Spraying

- attacks are a form of brute-force attack that attempts to use a single password or small set of passwords against many accounts.

Dictionary Attacks

- form of brute-force attack that uses a list of words for their attempts.
- Examples: JTR (John the Ripper)

Rainbow Table Attack

- A rainbow table attack uses precomputed hash values stored in a table to crack hashed passwords quickly by matching them with the table entries.
- It exploits weak password hashing ***without salts***, making hash collisions easier to find.
- To prevent this, websites use ***salts***—random values added to each password before hashing, which makes rainbow tables ineffective by requiring a different table for each unique salt.

Downgrade attack

- A downgrade attack is sometimes used against secure communications such as TLS to get the user or system to inadvertently shift to less secure cryptographic modes.

Birthday Attack

- Based on birthday theorem (probability).
- In cryptography, a birthday attack is used to find two different inputs that produce the same hash (called a **collision**). Since finding a match is easier than calculating an exact value, the attacker can potentially break hash functions faster by focusing on collisions.

Frequency Analysis

- Involves looking at the blocks of an encrypted message to determine if any common patterns exist.
- In the English language, the letters 'e' and 't' and words like *'**the, and, that, it, and is**'* are very common. Single letters that stand alone in a sentence are usually limited to A and I.

Known plain text

- This method relies on having a pair of plain text to start with.
- Not efficient now.

Chosen plain text

- Here, the attacker obtains the ciphertexts corresponding to a set of plain texts of their own choosing.
- This allows the attacker to attempt to derive the key used and thus decrypt other messages encrypted with that key.

Related Key Attack:

- This is like a chosen plain-text attack, except the attacker can obtain ciphertexts encrypted under two different keys.
- This is a useful attack if you can obtain the plain-text and matching ciphertext.

Chapter 5 – Security Assessment & Testing

Vulnerability Scanning Tools

Infrastructure Vulnerability Scanning

Network vulnerability scanners probe connected devices for known vulnerabilities by identifying device types and configurations, then running targeted tests. Common tools include:

- ***Nessus***: One of the earliest and most respected scanners.
- ***Qualys***: A SaaS-based scanner for both on-premises and cloud environments.
- ***Nexpose***: A commercial scanner similar to Nessus and Qualys.
- ***OpenVAS***: A free, open-source alternative.

Web Application Scanning

Specialized tools used to examine the security of web applications. These tools test for web specific vulnerabilities, such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF) vulnerabilities.

Understanding CVSS Score:

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

The first section, "CVSS:3.0", simply informs the reader (human or system) that the vector was composed using CVSS version 3. The next eight sections correspond to each of the eight CVSS metrics.
Attack Vector: Network
***Attack Complexity*:** Low
***Privileges Required*:** None
***User Interaction*:** None
***Scope*:** Unchanged
Confidentiality: High
***Integrity*:** None
***Availability*:** None

Calculating Impact Sub-score (ISS)

ISS = 1 – [(1 - Confidentiality) * (1 – Integrity) * (1 – Availability)]

Calculating Impact Score

If the scope is unchanged,

- Impact =6.42 * ISS

If the scope is changed,

- Impact = 7.52 * (ISS – 0.029) – 3.25 * (ISS – 0.02)^{15}

Calculating Exploitability Score

Exploitability = 8.22 * Attack Vector * Attack Complexity * Privilege Required * User Interaction

Calculating Base Score

- If the impact is 0, the base score is 0.
- If the scope metric is Unchanged, ***base score = impact + exploitability.***
- If the scope metric is Changed, ***base score = (impact + exploitability) * 1.08***
- The highest possible base score is 10. If the calculated value is greater than 10, set the base score to 10.

CVSS score Rating

0.0 None
0.1–3.9 Low
4.0–6.9 Medium
7.0–8.9 High
9.0–10.0 Critical

Confirmation of Scan Results

False positive: A vulnerability is identified but doesn't really exist.
False negative: A vulnerability exists, but it isn't detected.
True Positive*:* A vulnerability exists, and it is correctly identified.
True Negative*:* No vulnerability exists, and the system correctly reports its absence.

Penetration Testing

There are four major categories of penetration testing:

Physical Penetration Testing: Assesses vulnerabilities in physical security, such as access control and surveillance.

Offensive Penetration Testing: Simulates real-world cyberattacks to exploit vulnerabilities in networks, systems, and applications.

Defensive Penetration Testing: Evaluates an organization's ability to detect and defend against cyberattacks.

Integrated Penetration Testing: Combines offensive and defensive testing for a comprehensive security assessment.

Chapter 6 – Application Security

SDLC (Software Development Lifecycle)

- **Planning**: Define project goals, scope, and feasibility.
- **Requirements**: Gather and document functional and non-functional requirements.
- **Design**: Architect the system's structure, components, and interfaces.
- **Implementation**: Develop and code the application based on design.
- **Testing**: Identify and fix defects through various tests to ensure quality.
- **Deployment**: Release the software to a production environment for users.
- **Maintenance**: Monitor, update, and fix issues after release.

Code Deployment Environments

1. Development Environment
2. Test Environment
3. Staging Environment
4. Production Environment

Software Security Testing - Analyzing and Testing Code

Static Code Analysis

- Done by reviewing code
- Static analysis does not run the program.
- Can be done manually or by using automated tools.

Dynamic Code Analysis

- It relies on the execution of the code while providing it with input to test the software.

Fuzzing

- Sending ***invalid or random data*** to test the application's ability to handle exception unexpected data.
- Typically done through automated tools due to high volume of data.
- Useful for data validation, logic issues and sometimes memory leak issues.

Interactive Testing

- Combines static and dynamic testing, analyzing source code while testers interact with the application.

Chapter 7 – Cryptography and the PKI

A ***cipher*** is a method used to scramble or obfuscate characters to hide their value.

Two types of Ciphers:

Substitution: Replaces characters.
- ***Stream ciphers*** which operate on ***one character*** or bit of a message.
  - Ceaser Cipher
  - ROT13 (rotates every letter 13 places in the alphabet)
  - Polyalphabetic ciphers: Vigenère cipher.

Transposition: Rearranges characters**.**
- ***Block ciphers*** which operate on ***blocks*** or ***chunks*****.**
- Example: In a columnar transposition cipher, the plaintext is written into a grid, and the letters are read out in a different order, such as by column instead of row.

Steganography
- Steganography is the art of using cryptographic techniques to embed secret messages within another file.
- It can be used to hide images, text, audio, video, and many other forms of digital content.

Goals of Cryptography

Confidentiality
When developing a cryptographic system for the purpose of providing confidentiality, you must think about three types of data:

Data at rest, or stored data: which resides in a permanent location awaiting access. Examples of data at rest include data stored on hard drives, backup tapes, cloud storage services, USB devices, and other storage media.

Data in transit, or data in transport/communication: data being transmitted across a network between two systems. Data in transit might be traveling on a corporate network, a wireless network, or the public Internet. The most common way to protect network communications using sensitive data is with the Transport Layer Security (TLS) protocol.

Data in use is data that is stored in the active memory of a computer system where it may be accessed by a process running on that system.

Encrypting Data at Rest:

Encrypting Data in Disk:

Full Disk Encryption (FDE):

- All data on hard drive is encrypted including OS and OS files.
- In case of loss and theft, FDE can prevent unauthorized access.
- Can be implemented at a hardware level using ***SED (self-encrypting drive).***

Self-encrypting Drives:

- Implement encryption capabilities in their hardware and firmware.
- Form of Full Disk Encryption.
- Systems having SED require a key to boot the system using a key which may be entered manually or provided by a hardware token or device.

Partition Encryption:

- Targets specific partition of the drive instead of entire disk.
- Useful when dealing with dual-boot systems or when segregating sensitive data.

Volume Encryption (sometimes called File-level encryption):

- Encrypting a set "volume" on a storage device, which could contain several folders and files.
- Useful when you want to encrypt a large amount of data at once but don't need to encrypt an entire disk or partition.
- File and folder level encryption focuses on individual files.

Encrypting Data in Database:

Database Level

- ***Transparent Data Encryption (TDE),*** which encrypts the entire database.
    - ***Column-level Encryption (CLE),*** which allows for specific columns within tables to be encrypted.
    - ***Record Level*****:** Provides granular and precise control over the data.

Integrity

Integrity ensures that data is not altered without authorization. If integrity mechanisms are in place, the recipient of a message can be certain that the message received is identical to the message that was sent.
Message integrity is enforced using encrypted message digests, known as ***digital signatures****.*

Authentication

Authentication verifies the claimed identity of system users and is a major function of cryptosystems.

Non-repudiation

Non-repudiation provides assurance to the recipient that the message was originated by the sender and not someone masquerading as the sender. It is only offered by ***public key or asymmetric cryptography.***

Comparison on Encrypting Algorithms

DES (Data Encryption Standard) An outdated ***symmetric*** algorithm with known vulnerabilities due to its short key length (56 bits).

3DES A more secure version of DES that applies the algorithm three times but is slower and less efficient than modern alternatives.

AES (Advanced Encryption Standard) The current standard for ***symmetric*** encryption, offering strong security (key sizes of 128, 192, or 256 bits) and high efficiency.

RSA An ***asymmetric*** encryption algorithm used for secure data transmission, relying on key pairs and not suitable as a symmetric encryption method.

Digital Signatures

1. Digitally signed messages assure the recipient that the message truly came from the claimed sender. They enforce non-repudiation.
2. Digitally signed messages assure the recipient that the message was not altered while in transit between the sender and recipient.

HMAC

The Hash-Based Message Authentication Code (HMAC) algorithm implements a partial digital signature. It **guarantees the integrity** of a message during transmission, but it **does not** provide for **non-repudiation**.

Symmetric Encryption

- A single, shared key.
- Symmetric key cryptography can also be called ***secret key cryptography*** and ***private key cryptography*.**
- Encrypt and decrypt using the same key.
- Key is Also known as shared secret.
- Doesn’t scale very well.
- Very fast to use.
- The total number of keys required to completely connect n parties using symmetric cryptography is given by the following formula:
- ***Number of Keys = n(n–1) / 2***

Creation and Distribution on Symmetric Keys

- Offline Distribution
- Public Key Encryption
- Diffie-Hillman

Storage and Destruction of Symmetric Keys

- Never store an encryption key on the same system where encrypted data resides. This just makes it easier for the attacker!
- For sensitive keys, consider providing two different individuals with half of the key.

Asymmetric Encryption:

- Public key algorithm.
- Includes Private/public key.
- The **private key** is the only key that can ***decrypt data*** which is ***encrypted*** by ***public key.***
- ***No additional keys*** are needed for secure communication as users can use each other's public keys to encrypt messages.

Types of Hashing Algorithms

- ***SHA (Secure Hashing Algorithm)***
- ***SHA2:***
  - ***SHA-2,*** which has four variants:
  - ***SHA-256*** produces a 256-bit message digest using a 512-bit block size.
  - ***SHA-224*** uses a truncated version of the SHA-256 hash to produce a 224-bit message digest using a 512-bit block size.
  - ***SHA-512*** produces a 512-bit message digest using a 1,024-bit block size.
  - ***SHA-384*** uses a truncated version of the SHA-512 hash to produce a 384-bit digest using a 1,024-bit block size.
- ***MD5***
  - It is not used as it is prone to collision attacks.

Strengths of Asymmetric Encryption:

- The addition of new users requires the generation of only one public-private key pair.
- Users can be removed far more easily from asymmetric systems.
- Key regeneration is required only when a user's private key is compromised.
- Key exchange is a simple process.
- No preexisting communication link needs to exist.

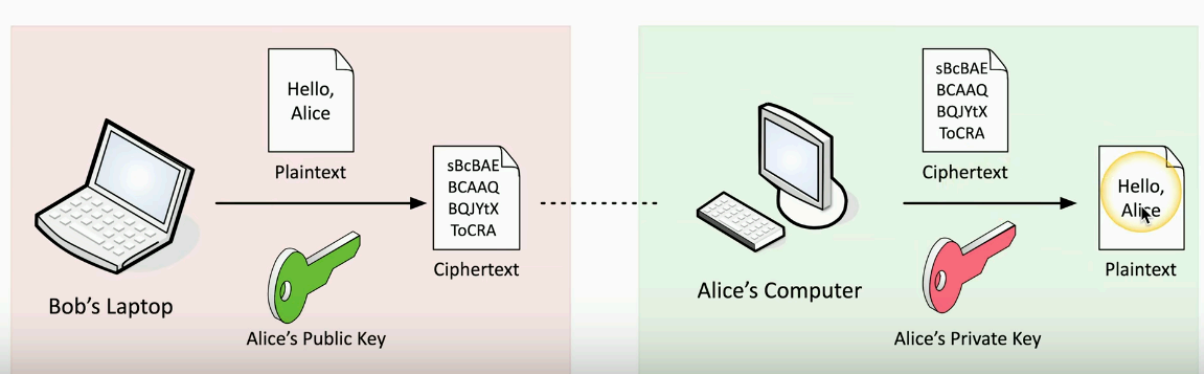

Figure 2 - Demonstration of asymmetric encryption/decryption

Key escrow

- Key escrow systems address this situation by having a third party store a protected copy of the key for use in an emergency.
- Someone else holds your decryption key.

Public Key Infrastructure (PKI)

PKI is a hierarchical system that facilitates the creation, management, storage, distribution, and revocation of digital certificates, ensuring secure communications and identity verification in digital environments.

Certificates

- Digital certificates provide communicating parties with assurance that people that they are communicating with are who they claim to be.
- Certificates that conform to X.509 contain the following attributes:
  - Version of X.509 to which the certificate conforms.
  - Serial number.
  - Signature algorithm identifier (specifies the technique used by the certificate authority to digitally sign the contents of the certificate).
  - Issuer name (identification of the certificate authority that issued the certificate)
  - Validity period (specifies the dates and times—a starting date and time and an expiration date and time—during which the certificate is valid).
  - Subject's Common Name (CN) that clearly describes the certificate owner (e.g., example.com).
  - Subject's Public Key

Certificate Authorities (CA)

- PKI relies on a hierarchy of trust relationships. If you configure your browser to trust a CA, it will automatically trust all the digital certificates issued by that CA.
- Browser developers preconfigure browsers to trust the major CAs to avoid placing this burden on users.
- ***Registration authorities (RAs)*** assist CAs with the burden of verifying users' identities prior to issuing digital certificates.
- In the CA trust model, the use of a series of intermediate CAs is known as ***certificate chaining.***

Root CA

- The ***Root CA*** is the highest authority in a PKI hierarchy, responsible for issuing and signing certificates for intermediate CAs.
- It is typically kept offline to enhance security and prevent unauthorized access.

Intermediate CA

1. The ***Intermediate CA*** serves as a bridge between the Root CA and end-user certificates, issuing and signing certificates to lower-level CAs or directly to users. This structure reduces the risk associated with exposing the Root CA.

Registration Authority (RA)

- The ***RA*** verifies the identity of entities requesting digital certificates and forwards legitimate requests to the CA for issuance. It acts as a mediator but does not issue certificates itself.
- ***Can revoke certificates.***

Internal CA

- An ***Internal CA*** is managed within an organization to issue certificates for internal use, such as applications and devices.
- ***Can revoke certificates.***

Wildcard Certificate A type of digital certificate that can be used to secure multiple subdomains within a primary domain.

Subject Alternative Name (SAN) certificate allows to secure multiple domain names or subdomains with a single certificate

Certificate Generation and Destruction

Enrolment

- Proving your identity to a CA in some manner is called ***enrolment***.
- After proving identity, give your public key to CA in form of CSR (Certificate Signing Request).
- The CA next creates an X.509 digital certificate containing your identifying information and a copy of your public key.
- Then CA digitally signs the certificate with its private key.

Certificate authorities issue different types of certificates depending on the level of identity verification that they perform.

- The simplest, and most common, certificates are ***Domain Validation (DV)*** certificates, where the CA simply verifies that the certificate subject has control of the domain name.
- ***Extended Validation (EV)*** certificates provide a higher level of assurance.

Verification

- When you receive a digital certificate from someone, you verify the certificate by checking the CA's digital signature using the CA's public key.
- Next, you must check and ensure that the certificate was not revoked using a ***certificate revocation list (CRL)*** *or the* ***Online Certificate Status Protocol (OCSP).***

Revocation

- Occasionally, a certificate authority needs to revoke a certificate. This might occur for one of the following reasons:
- The certificate was compromised (for example, the certificate owner accidentally gave away the private key).
- The certificate was erroneously issued (for example, the CA mistakenly issued a certificate without proper verification).

- The details of the certificate changed (for example, the subject's name changed).
- The security association changed (for example, the subject is no longer employed by the organization sponsoring the certificate).

Techniques to verify the Authenticity of certificates

Certificate Revocation Lists Certificate revocation lists (CRLs) require clients to download a list of revoked certificates, which may be less efficient.

Online Certificate Status Protocol (OCSP) requires real-time communication with a remote server to check the certificate status.

Certificate Stapling allows clients to quickly verify the status of digital certificates without contacting a remote server.

Certificate Formats

Standard	***Format***	***File Extensions***
Distinguished Encoding Rules (DER)	Binary	.der, .crt, .cer
Privacy Enhanced Mail (PEM)	Text	.pem, .crt
Personal Information Exchange (Commonly used in Windows)	Binary	.pfx, .p12

Hashing, Salting and Key Stretching

Key stretching

- ***Key stretching*** is a technique used to make weak passwords stronger by applying a hash function multiple time.
- This process increases the time it takes for an attacker to crack the password using brute force or dictionary attacks.
- By repeatedly hashing the password (along with a ***salt***), key stretching slows down the process of generating potential passwords, making it much harder for attackers to guess or compute the original password, even with advanced tools.
- Key stretching tools: PBKDF2, bcrypt, and Argon2.

Hashing

There are five basic requirements for a cryptographic hash function:

1. They accept an input of any length.
2. They produce an output of a fixed length, regardless of the length of the input.
3. The hash value is relatively easy to compute.
4. The hash function is one-way (meaning that it is extremely hard to determine the input when provided with the output).

5. A secure hash function is collision free (meaning that it is extremely hard to find two messages that produce the same hash value).

Rainbow table

Rainbow table attack is a hacking method used to crack hashed passwords by precomputing and storing a huge list of hash values and their matching original passwords. Instead of brute-forcing every possible password, the attacker quickly looks up the hash in this pre-made table to find a match.

Chapter - 8 Identity and Access Management

Authentication and Authorization Technologies

Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol designed to provide more security than earlier protocols like PAP.

MSCHAP, or Microsoft Challenge Handshake Authentication Protocol, is used for authenticating users in point-to-point connections, such as VPNs, dial-up networking, and wireless networks. Commonly found in Microsoft environments. ***Less secure*** than PEAP.

The *Extensible Authentication Protocol (EAP)* is an authentication framework that is commonly used for wireless networks.

LEAP (Lightweight Extensible Authentication Protocol) is the older version and has vulnerabilities.

PEAP (Protected EAP) authenticates servers using certificates and wraps EAP using tunnels. ***More secure*** than LEAP.

Protocols based on security (lowest to highest): MSCHAP < LEAP < EAP < PEAP

IEEE 802.1X
- Port-based Network Access Control (NAC)
- You don't get access to the network until you authenticate.
- EAP integrates with 802.1X

Remote Authentication Dial-In User Service (RADIUS) is one of the most common ***authentication, authorization, and accounting (AAA)*** systems for network devices, wireless networks, and other services. RADIUS can operate via TCP or UDP and operates in a client-server model.
RADIUS sends passwords that are obfuscated by a shared secret and MD5 hash, meaning that its password security is not very strong.

Supplicant – the client
Authenticator – The device that provides access.
Authentication Server – Validates the clients' credentials

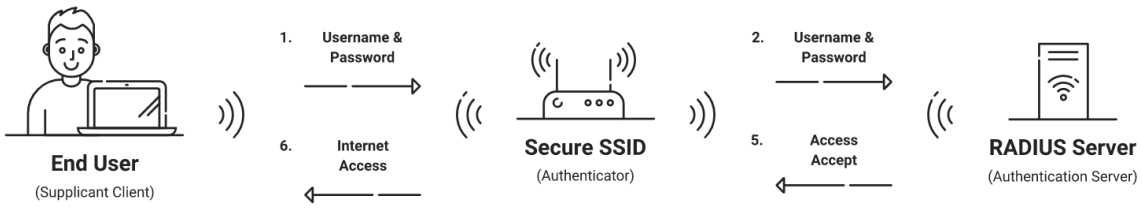

Figure 3 – Authentication through RADIUS

Terminal Access Controller Access Control System Plus (TACACS+) is a ***Cisco-designed*** extension to TACACS, which TCP traffic to provide authentication, authorization, and accounting services.

Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network like the Internet.

- When a client wants to use Kerberos to access a service, the client requests an authentication ticket, or ***ticket-granting ticket (TGT)***.
- An authentication server checks the client's credentials and responds with the TGT, which is encrypted using the secret key of the ticket-granting service (TGS).

Provisioning and Deprovisioning Accounts

Privileged Access Management

Privileged access management (PAM) tools can be used to handle the administrative and privileged accounts. Uses the concept of least privilege. Offers more granular and detailed control.

Just in Time (JIT) are permissions that are granted only when needed and revoked when needed.
Password Vaulting is used to access privileged accounts without needing the password.
Ephemeral accounts are temporary accounts with limited lifespans.

Chapter – 9 Resilience and Physical Security

Common elements in Design of Redundancy include:

One of the most common ways to build ***resilience*** is through ***redundancy***—in other words, having more than one of a system, service, device, or other component.

Geographic dispersion of systems ensures that a single disaster, attack, or failure cannot disable or destroy them.

Separation of servers and other devices in datacentres is also commonly used to avoid a single rack being a point of failure.

Use of *multiple network paths* (multipath) solutions ensures that a severed cable or failed device will not cause a loss of connectivity.

Load balancing, which makes multiple systems or services appear to be a single resource, allowing both redundancy and increased ability to handle loads by distributing them to more than one system.

Clustering describes groups of computers connected to perform the same task.

Platform diversity, or diversity of technologies and vendors, is another way to build resilience into an infrastructure. Using different vendors, cryptographic solutions, platforms, and controls can make it more difficult for a single attack or failure to have system- or organization-wide impacts.

Availability
Load balancing, which makes multiple systems or services appear to be a single resource, allowing both redundancy and increased ability to handle loads by distributing them to more than one system.

Clustering describes groups of computers connected to perform the same task.

Protection of power, using *uninterruptible power supply (UPS)* systems that provide battery or other backup power options for short periods of time.

Generator systems that are used to provide power for longer outages; and design elements, such as dual-supply or multi-supply hardware, ensures that a power supply failure won't disable a server.

Managed power distribution units (PDUs) are also used to provide intelligent power management and remote control.

Platform diversity or diversity of technologies and vendors.

RAID - Redundant Arrays of Inexpensive Disks:

RAID is a common solution that uses multiple disks with data either striped (spread across disks) or mirrored (completely duplicated), and technology to ensure that data is not corrupted or lost (parity).

1. ***RAID 0****:* Data is striped across multiple disks for high performance but offers no redundancy.
2. ***RAID 1****:* Data is mirrored across two disks, providing redundancy but with reduced storage efficiency.
3. ***RAID 5****:* Data is striped with parity across **3+ disks**, offering redundancy and efficient use of space.
4. ***RAID 6****:* Similar to RAID 5, but with double parity, allowing for two disk failures.
5. ***RAID 10 (1+0)****:* Combines mirroring and striping, offering high performance and redundancy by mirroring data across striped sets

Recovery Processes involve restoring data and systems after a failure, focusing on ensuring data integrity and minimal downtime; factors impacting recovery include the backup frequency, system architecture, and the extent of the failure.

Replication involves creating and maintaining copies of data in real-time or near-real-time across different locations for redundancy, often used in high-availability systems.

Journaling captures changes to data as they occur, allowing for point-in-time recovery, typically used in database systems to ensure data consistency during transactions.

Availability Solutions

Vertical scalability requires a larger or more powerful system or device. Vertical scalability can help when all tasks or functions need to be handled on the same system or infrastructure. Vertical scalability can be very expensive to increase, particularly if the event that drives the need to scale is not ongoing or frequent. There are, however, times when vertical scalability is required, such as for every large memory footprint application that cannot be run on smaller, less capable systems.

Horizontal scaling uses smaller systems or devices but adds more of them. When designed and managed correctly, a horizontally scaled system can take advantage of the ability to transparently add and remove more resources, allowing it to adjust as needs grow or shrink. This approach also provides opportunities for transparent upgrades, patching, and even incident response.

Site Resilience

Three major types of disaster recovery sites are used for site resilience:

Hot Sites are fully equipped with infrastructure and data for immediate operational capability, often running full-time to balance traffic and ensure staff readiness during emergencies.
Warm Sites have some systems and configurations in place but ***lack live data***, balancing cost and capability for quicker restoration compared to cold sites, although they incur higher maintenance costs.
Cold Sites offer only space, power, and network connectivity, requiring organizations to bring in or acquire systems and data in a disaster, making them the ***least expensive*** option but potentially challenging during emergencies.

Capacity Planning

People Capacity Planning ensures sufficient staffing with necessary skills for scaling and disaster recovery, often achieved through global staffing or third-party support like consultants and cloud services.

Technology Capacity Planning involves assessing the scalability of deployed technologies, such as web servers, load balancers, or storage devices, focusing on performance under increased load.

Infrastructure Capacity Planning addresses the scalability of underlying systems like networks, storage, and connectivity to support changing demands or disaster recovery efforts.

Testing Resilience and Recovery Controls and Designs

Once you've implemented resilience and recovery controls, it is important to test and validate them. Four common methods of doing this are:

Tabletop Exercises use discussions among assigned personnel to validate disaster plans, identifying gaps with minimal disruption but ***lacking real-world accuracy***.

Simulation Exercises involve practice ***drills*** where staff simulate their roles in a disaster, minimizing disruptions but requiring clear communication that it's not a real event.

Parallel Processing Exercises test backup systems or sites by moving processing to them, with ***some risk of disruption*** if systems are not fully separated.

Failover Exercises fully test switching to alternate sites or systems, offering the most realistic scenario but with the ***highest risk*** of disruption.

Physical Security Controls

Barricades/bollards

- Prevent access.
- Channel people through a specific access point.
- Identify safety concerns and prevents injuries.
- Can be used to an extreme

Access control vestibules

- All doors are normally unlocked.
  - Opening one door causes others to lock.
- All doors are normally locked.
  - Unlocking one door prevents others from being unlocked.
- One door open / other locked.
  - When one door is open, other cannot be unlocked.
- One at a time, controlled groups
  - Managed control through the area. (Might include identification by security)

Fencing

- Build a perimeter.
- May be a transparent fence or opaque.
- Must be robust.
- Could Prevent climbing.

Video Surveillance

- CCTV
- Can have motion detection, object detection which can detect a license plate or person's face.

Guards and access badges

- Security guard
  - Physical protection at the reception area of a facility.
  - Validates identification of existing employees.
- Access badge
  - Picture, name, other details**.**
  - Must be always worn.
  - Electronically logged.

Lighting

- More light means more security.
  - Attackers avoid the light.
  - Easier to see when lit.
  - Non-IR cameras can see better.

Sensors

- Infrared
  - Detects infrared radiation in both light and dark.

- Common in motion detectors and cheap.

Pressure

- Detects a change in force.
- Floor and window sensors.

Microwave

- Detects movement across large areas.

Ultrasonic

- Sends ultrasonic signals, receive reflected sound waves.
- Detects motion, collision detection, etc.

Chapter 10 – Cloud and Virtualization Security

Cloud Standards and Guidelines

NIST SP 500-292, offers a high-level taxonomy for cloud services.

The *Cloud Security Alliance (CSA)* is an industry organization focused on developing and promoting best practices in cloud security. They developed the ***Cloud Controls Matrix (CCM)*** as a reference document designed to help organizations understand the appropriate use of cloud security controls and map those controls to various regulatory standards.

Virtualization

Hypervisors

The primary responsibility of the hypervisor is ***enforcing isolation*** between virtual machines. ***Prevents VM-escape attacks.*** Isolation ensures that virtual machines do not interfere with each other's operations.
Two types of hypervisors:

Type I hypervisors, also known as bare-metal hypervisors, operate directly on top of the underlying hardware. Highly efficient and most common in datacenter virtualization.

Type II hypervisors run as an application on top of an existing operating system. Commonly used when virtualization is done in personal computers.

Containerization

- Containers provide ***application-level virtualization*** but must be protected like VMs.
    - Instead of creating complex virtual machines that require their own operating systems, containers package applications and allow them to be treated as units of virtualization that become portable across operating systems and hardware platforms.

Cloud Security

Cloud Access Security Brokers (CASBs)

- Cloud access security brokers (CASBs) are software tools that serve as intermediaries between cloud service users and cloud service providers.
- This positioning allows them to monitor user activity and enforce policy requirements.

CASB are of two types:

- ***Inline CASB***
  - Inline CASB solutions physically or logically reside in the connection path between the user and the service.
  - This approach requires configuration of the network and/or endpoint devices.
- ***API-based CASB***
  - API-based CASB solutions do not interact directly with the user but rather **interact directly with the cloud provider** through the provider's API.
  - it also does not allow the CASB to block requests that violate policy.

Chapter 11 – Endpoint Security

Hardware & firmware vulnerabilities

Vendors use several terms to describe their sales and support life cycles. Common terms and definitions include the following:

End of sales is the ***last date*** at which a specific model or device will be sold, although devices often remain in the supply chain through resellers for a period.

End of life While the equipment or device is ***no longer sold***, it ***remains supported***. End of-life equipment should typically be on a path to retirement, but it has some usable lifespan left.

End of support is the last date on which the vendor will provide support and/or updates.

Legacy This term is less well defined but typically is used to describe hardware, software, or devices that are ***unsupported***.

Protecting Endpoints

Preserving Boot Integrity

Keeping an endpoint secure while it is running starts as it boots up. If untrusted or malicious components are inserted into the boot process, the system cannot be trusted.

Modern ***Unified Extensible Firmware Interface (UEFI)*** firmware has replaced the traditional ***Basic Input/Output System [BIOS].***

A Trusted Platform Module (TPM) is a hardware chip that securely stores cryptographic keys, certificates, and passwords, providing enhanced security for devices. It's essential in applications like secure boot, disk encryption, and authentication, ensuring system integrity and protecting sensitive data against unauthorized access.

Similar techniques are used for Apple's Secure Enclave, a dedicated secure element that is built into Apple's System on Chip (SoC) modules which is separated from the main processor. This isolation keeps keys safe during their entire use and protects sensitive data.

Hardware security modules (HSM) are typically ***external devices*** or plug-in cards used to ***create, store, and manage digital keys*** for cryptographic functions and authentication, as well as to offload cryptographic processing.

- Cloud providers like Amazon and Microsoft offer cloud-based HSMs.

*** TPM – used for System Security*
HSM – Used to create, store and manage security keys.
KMS – Used to manage secrets

Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR)

EDR tools combine monitoring capabilities on endpoint devices and systems using a client or software agent with network monitoring and log analysis capabilities to collect, correlate, and analyse events.

XDR (Extended Detection and Response) is like EDR but has a broader perspective considering not only endpoints but the full breadth of an organization's technology stack, including cloud services, security services and platforms, email, and similar components.

Data Loss Prevention

Key elements of DLP systems include the ability to classify data so that organizations know which data should be protected; data labelling or tagging functions, to support classification and management practices; policy management and enforcement functions used to manage data to the standards set by the organization; and monitoring and reporting capabilities, to quickly notify administrators or security practitioners about issues or potential problems

Network Defense

- ***Host-based Firewalls***
- ***Host-based Intrusion Prevention System (HIPS)*** – can take actions to mitigate a risk
- ***Host-based Intrusion Detection System (HIDS)*** – can only report and send alerts

OS Hardening

Security-Enhanced Linux (SELinux)

- Security patches for linux kernel.
- Adds mandatory access control to Linux.
- Linux traditionally uses DAC.
- Limits application access which will limit the scope of any potential breach.

Configuration, Standards, and Schemas

Three phases of baseline cycles are:

Establishing a baseline, which is most often done using an existing industry standard like the CIS benchmarks with modifications and adjustments made to fit the organization's needs.

Deploying the security baseline using central management tools or even manually depending on the scope, scale, and capabilities of the organization.

Maintaining the baseline by using central management tools and enforcement capabilities as well as adjusting the organization's baseline if required by functional needs or other changes.

Securing Embedded and Specialized Systems

Embedded systems are computer systems that are built into other devices.

Real-time Operating System (RTOS)

- An OS with a deterministic processing schedule.
- No time to wait for other processes. Consider it as a highest priority.
- Examples are Industrial equipment, automobiles, military environments.
- They are extremely sensitive to security issues.
- Need to always be available.

SCADA and ICS

Industrial and manufacturing systems are often described using one of two terms. **Industrial controls systems (ICSs)** are a broad term for industrial automation, and **Supervisory Control and Data Acquisition (SCADA)** often refers to large systems that run **power and water** distribution or other systems that cover large areas. Since the terms overlap, they are often used interchangeably.

- Large-scale, multi-site **Industrial Control Systems (ICS)**
- One can monitor status of all equipment like power generation, refining, manufacturing equipment, facilities, energy consumption, logistics and so on.
- Can give real-time information.
- Requires extensive segmentation.

Securing IOT

IoT devices bring several security and privacy concerns, and security analysts must be aware of these common issues:

- **Poor security practices**, including weak default settings, lack of network security (firewalls), exposed or vulnerable services, lack of encryption for data transfer, weak authentication, use of embedded credentials, insecure data storage, and a wide range of other poor practices.
- **Short support lifespans**—IoT devices may not be patched or updated, leaving them potentially vulnerable for most of their deployed lifespan.
- **Vendor data** - handling practice issues, including licensing and data ownership concerns, as well as the potential to reveal data to both employees and partners of the vendor and to government and other agencies without the device owner being aware.

Asset Management

Enumeration is typically associated with scanning to identify assets, and some organizations use port and vulnerability scans to help identify systems that aren't part of their inventory.

Decommissioning typically involves removing a device or system from service, removing it from inventory, and ensuring that no sensitive data remains on the system. Certificates can also be decommissioned.

Retention may be required for legal purposes with set retention periods determined by law, or retention may be associated with a legal case due to a legal hold.
The Asset Management process includes:

Acquisition/procurement process:

- It deals with the purchasing process of the assets.
- Start with a request from the user
- Negotiate with the suppliers
- Purchase, invoice, payment

Assignment/account:

- After acquiring the asset, a central **asset tracking system** is used.
- Ownership: associate person with an asset.
- **Classification:** of asset based on device type.

Monitoring/ asset tracking:

- Inventory of every asset.
- Associate a support ticket with a device make and model.
- Add a physical asset tag which has barcode or RFID

Media sanitization:

- Completely remove data before giving to another employee.
- No usable information remains.
- Should be one-way trip so that it also cannot be recovered with forensic tools.

Physical Destruction:

- Shredder
- Drill
- Hammer
- Electromagnetic degaussing which removes the magnetic field which makes drive unusable.

Certificate of destruction:

- Destruction is often done by third party.
- Need confirmation that your data is destructed.

Data Retention:

- **Backing up** of data answering How much and where?
- Regulatory compliance
- Can be helpful in accidental deletion and disaster recovery.

Chapter 12 – Network Security

Infrastructure Considerations

Attack Surface: An attack surface is the total set of vulnerabilities and entry points in a system that an attacker could exploit. Understanding an organization's attack surface is a key part of security and infrastructure design.

Device placement is a key concern. Devices may be placed to secure a specific zone or network segment, to allow them to access traffic from a network segment, VLAN, or broader network, or may be placed due to capabilities like maximum throughput.

Security zones are frequently related to device placement. Security zones are network segments, physical or virtual network segments, or other components of an infrastructure that can be separate from less secure zones through logical or physical means.

Connectivity considerations involve the organization's internet connection type, speed, redundancy, security controls from providers, and physical path diversity to prevent disruptions from single events.

Organizations must consider ***failure modes***: should a security device fail by blocking all traffic **(fail-closed)** or allowing all traffic **(fail-open)**? The choice depends on business priorities—balancing operational continuity against the risk of temporarily losing security controls.

Network taps monitor or access traffic and can be **active** (powered) or **passive** (non-powered). **Passive taps** avoid power-related failures. They can operate inline, directing all traffic through them, or as monitors, copying traffic without altering the original network flow.

SPAN (Switched Port Analyzer) ports *are used to:*

- Mirror network traffic from one or more switch ports to a monitoring device.
- Enable traffic analysis for troubleshooting and performance monitoring.
- Support security tools like IDS/IPS for packet inspection.
- Facilitate data collection for network forensic investigations.

Network Design Concepts

Physical isolation is the idea of separating devices so that there is no connection between them. Commonly known as **"air-gapped"** design because there is "air" between them.

Logical segmentation is done using software or settings rather than a physical separation using different devices. Virtual local area networks (VLANs) are a common method of providing logical segmentation.

High availability (HA) ensures that a system or service remains consistently accessible with minimal downtime, even during maintenance, failures, or load changes, allowing continuous operation and reliability. Solutions like **clustering and load balancing** are used.

Implementation of secure protocols is a common part of ensuring that communications and services are secure. Examples of secure protocols are the use of HTTPS (TLS) instead of unencrypted HTTP, using SSH instead of Telnet, and wrapping other services using TLS. **Can also use security by obscurity concept by running services on different port.**

Reputation services track IP addresses, domains, and hosts involved in malicious activities. They help organizations monitor or block potential threats and are often integrated with threat feeds and log monitoring for enhanced insight into possible attacks.

Software-defined networking (SDN) uses software-based network configuration to control networks. Enables quick customization of security zones and allows dynamic adjustments based on performance.

Software-defined wide area network (SD-WAN) is a virtual network that integrates multiple connectivity services, such as MPLS, 4G/5G, and broadband. It enhances high availability, routes traffic based on application needs and reduces costs by utilizing more affordable connection options when feasible. **SD-WAN** is commonly used to replace ***MPLS*** **(*Multiprotocol Label Switching*)**

Secure Access Service Edge (SASE, pronounced "sassy") integrates virtual private networks, SD-WAN, and cloud security tools, such as firewalls and CASBs, to **ensure secure access** for devices anywhere. It protects endpoints, secures data in transit, and enforces policy-based security across an organization's infrastructure and services.

Network Segmentation

Network segmentation divides a network into logical or physical groupings that are frequently based on trust boundaries, functional requirements, or other reasons that help an organization apply controls or assist with functionality.

Several network design concepts describe specific implementations of network segmentation:

- ***Screened subnets, or DMZs*** (demilitarized zones), are network areas that host systems exposed to less trusted environments, often used for web servers or Internet-facing devices.
- ***Intranets*** are internal networks for sharing information with employees, protected from external access.
- ***Extranets*** allow controlled access for partners or customers.

Zero Trust

- Zero trust is a holistic approach to network security.
  - Covers every device, every process, and every person.
- Everything must be verified.
  - Nothing is inherently trusted.
  - Multifactor authentication, encryption, system permissions, additional firewalls, monitoring, and analytics, etc.

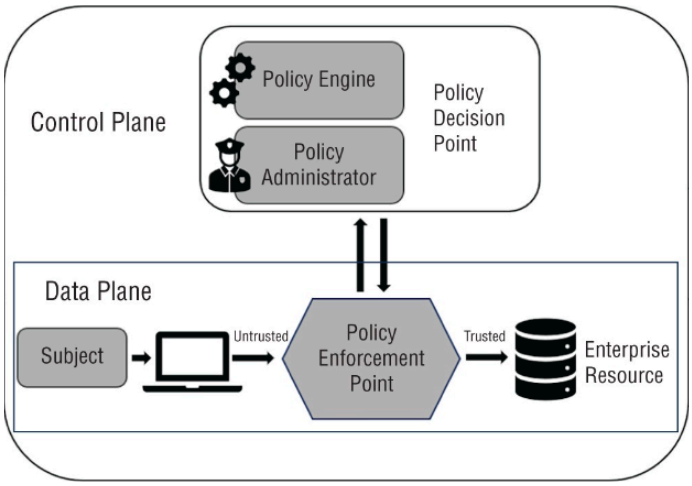

Figure 4 - NIST Zero Trust Logical Components

Data Plane

- ***Subjects*:** Users, services, or systems that request access to resources.
- ***Policy Engines:***
  - Make access decisions based on rules and external systems (e.g., threat intelligence).
  - Evaluates each decision based on policy and other information sources.
  - Grant, deny, or revoke.
- ***Policy Administrator***
  - Communicates with the PEP
  - Generates access tokens or credentials.
  - Tells the PEP to allow or disallow access.
- ***Policy enforcement point (PEP):***
  - Subjects and systems
    - End users, applications, non-human entities.
  - Policy enforcement point (PEP) acts as a gatekeeper.
  - Allow, monitor, and terminate connections.
  - Can consist of multiple components working together.
- ***Implicit trust zones***, which allow use and movement once a subject is authenticated by a Zero Trust Policy Engine.

Control Plane

- ***The Policy Administrator,*** which as described in the NIST model executes decisions made by a Policy Engine.

- ***Policy Decision Point*,** a process for making an authentication decision.
- ***Adaptive Identity**:* Context-based authentication that evaluates user login conditions and requests additional validation if security requirements aren't met.
- ***Threat Scope Reduction***: Limits user access to minimize potential damage from security incidents, relying on least privilege and identity-based network segmentation.
- ***Policy-Driven Access Control**:* Core concept of Zero Trust, where Policy Engines enforce decisions made by Policy Administrators and Policy Enforcement Points.

NAC (Network Access Control)

Network segmentation divides networks into logical security zones, while Network Access Control (NAC) helps manage and secure connections. NAC verifies whether a device meets network security standards before allowing access.

- ***Agent-based vs. Agentless***: Agent-based NAC uses software to assess security status (patches, settings, antivirus, etc.), offering more control, but requires installation and maintenance. Agentless NAC, run via browser or similar methods, is easier but provides less insight.
- ***Preadmission vs. Postadmission**:* Preadmission NAC checks devices before they connect, blocking unsafe devices. Postadmission NAC monitors and can disconnect risky devices post-connection.
- ***Policy Enforcement**:* NAC can quarantine non-compliant devices, permitting remediation, or block them entirely to maintain network security.

Virtual Private Networks and Remote Access

A virtual private network (VPN) creates a virtual link over a public network, enabling endpoints to operate as if on the same network. While often encrypted, encryption isn't a mandatory feature of VPNs.

Two major VPN technologies,

- ***IPSec VPN:***
  - Operates at layer 3.
  - Require a client.
  - Can operate in either transport or tunnel mode.
  - Used for site-to-site VPN.
- ***SSL VPN:***
  - Can use portal-based approach.
  - Users can access VPNs via a web page for service connections or use tunnel mode, like in IPSec VPNs, for a more secure, dedicated link.
  - Can be used without a client
  - SSL VPNs enable granular application access segmentation without needing complex configurations or separate VPN names and hosts, unlike many IPSec VPN tools.

Tunnelling

VPNs can be set up as full-tunnel or split-tunnel.
- ***Full-tunnel*** VPNs secure all traffic by sending it through the VPN.
- ***Split-tunnel*** VPNs only route specific traffic for the trusted network, reducing bandwidth but leaving other traffic unprotected.

Network Appliances and Security Tools

Jump Servers

Jump servers, or jump boxes, allow secure access to systems in different security zones. They are secured, monitored, and often accessed via SSH or RDP, equipped with necessary tools for admin tasks. Jump servers should log activity with secure, separate storage for auditing and incident investigations.

Load Balancing

Load balancers distribute traffic among multiple servers, offering redundancy, easy maintenance, and scalability. They use a virtual IP (VIP) to receive requests, which are then directed to servers in a pool.

Modes of Operation

Active/Active: Shares load among all servers online.
Active/Passive: Uses backup servers, activated only if the main server fails.

Load-Balancing Algorithms

Round-Robin: Sends traffic sequentially.
Least Connection: Routes to the server with the fewest active connections.
Agent-Based Adaptive: Adjusts based on server load reports.
Source IP Hashing: Uses client IP for traffic assignment.

Weighted Algorithms

- Weighted Least Connection and Weighted Response Time consider server capacity and response time.

Proxy Servers

Proxy servers handle and forward requests, allowing central control over access, filtering, and caching. They also support IP-based access restrictions.

Types of Proxy Servers:

Forward Proxies: Positioned between clients and servers, they route client requests while hiding the client's identity. Useful for anonymizing traffic or bypassing regional restrictions.

Reverse Proxies: Positioned between servers and clients, they help with load balancing and caching, distributing client requests across multiple servers for efficiency.

Web Filters

Web filters, sometimes called content filters, are centralized proxy devices or agent-based tools that allows, or block traffic based on content rules. These can be as simple as conducting Uniform Resource Locator (URL) scanning and blocking specific URLs, domains, or hosts, or they may be complex, with pattern matching, IP reputation, and other elements built into the filtering rules.

Data Protection (DP/DLP)

Ensuring that data isn't extracted or inadvertently sent from a network is where a data loss prevention (DLP) solution comes into play.
When an organization has concerns about sensitive, proprietary, or other data being lost or exposed, a DLP solution is a common option.

Intrusion Detection and Intrusion Prevention Systems

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitor network traffic for threats, with IPS having the ability to block them. Both use detection methods:

Signature-based detection: Identifies threats by matching known signatures.
Anomaly-based detection: Detects unusual behaviour by comparing it to a baseline.

An IPS needs to be in line with traffic to actively block threats, while both IDS and IPS can be passively deployed to detect but not stop threats; in this case, an IPS functions as an IDS.

Configuration Decisions for Network Security Devices

Inline vs. Tap

- ***Inline devices*** handle traffic directly, enabling interaction (e.g., blocking threats), but can cause network outages if they fail, although some are designed to fail open.
- ***Taps*** replicate traffic without direct interaction, thus avoiding outages, and are primarily used for monitoring and analysis.

Active vs. Passive Taps

- ***Active taps*** need power and have separate ports; power issues can interrupt traffic.
- ***Passive taps*** have a direct connection, ensuring continuous traffic flow even if power is lost.

SPAN/Mirror Ports Found on routers and switches, SPAN ports copy traffic like taps but may be less secure due to potential vulnerabilities in network devices.

Firewalls

Types of Firewalls:

Stateless Firewalls (Packet Filters):
- Filter each packet based on headers (source/destination IP, port, protocol).
- Basic form of firewall.

Stateful Firewalls (Dynamic Packet Filters):
- Track ongoing traffic sessions, allowing continued communication once approved.
- Use a state table to provide context for security decisions.

Advanced Firewall Technologies:

Next-Generation Firewalls (NGFWs)
- All-in-one network security devices with features like deep packet inspection, IDS/IPS, and antivirus.
- Generally faster and capable of higher throughput than UTMs.

Unified Threat Management (UTM) Devices
- Combine firewall, IDS/IPS, antimalware, URL filtering, data loss prevention, and more.
- Provide a comprehensive “out-of-the-box” solution, often for small to mid-sized organizations.
- Centralized management for multiple UTM devices.

Web Application Firewalls (WAFs)
- Intercept and analyse web traffic, focusing on preventing attacks targeting web applications.
- Combine firewall and intrusion prevention capabilities for deeper traffic inspection.

Firewall Rules
- Govern what traffic is allowed or blocked.
- Typically include:
  - Source (IP addresses, hostnames, domains)
  - Ports and protocols
  - Allow or deny statement
  - Destination (IP addresses, hosts, domains)

Access Control Lists (ACLs)

Access Control Lists (ACLs) are rules that permit or deny specific actions on network devices, like firewall rules. They can range from simple to complex, consisting of one or multiple entries that apply to network traffic.

Types of ACLs:

Static ACLs: Fixed rules that don't change unless manually modified.

*Dynamic ACLs***:** Adjust based on certain conditions or time-based criteria.

Deception and Disruption Technologies

*Deception**: Misleading or causing someone to believe something untrue.*
*Disruption**: Radically altering or interrupting the normal course of something, often with innovative ideas or technologies.*

Honeypots
- Attracts the bad guys and trap them there.
- "Attacker" is probably a machine.
- Makes an interesting recon.

Honeynets
- A real network which includes more than a single device like servers, workstations, routers, switches, firewalls.

Honeyfiles
- These are files with fake information.
- Bait for the honeynet (passwords.txt)
- Add many honeyfiles to file shares.
- An alert is sent if the file is accessed.

Honeytokens
- Track the malicious actors.
- These are traceable data to the honeynet i.e., if the data is stolen, you'll know where it came from.
- Eg: Fake API credentials, fake emails, database records, browser cookies, etc.

Network Security, Services, and Management

Out-of-Band Management (OOBM) is a secure way for administrators to access a network device's management interface without exposing it to regular network traffic, reducing security risks and ensuring reliable access when needed. Typically, this is done through:

Separate Management VLAN or Network: Devices are managed on a different VLAN or even a separate physical network, isolating management traffic from normal operations.

*Physical Access***:** Used as a backup, where administrators connect directly to the device using USB, serial, or other interfaces—mainly reserved for emergencies as it's time-intensive and less convenient than remote access.

DNS

The ***Domain Name System (DNS)*** helps devices find websites using human-readable names, making it a critical service but also a target for attackers. However, DNS lacks security features—it transmits data unencrypted and unauthenticated.

- To improve security, ***DNSSEC (Domain Name System Security Extensions)*** adds authentication, ensuring DNS data integrity even if it's unencrypted. **DNS security practices** include limiting zone transfers, enabling DNS logging, and blocking requests to malicious domains.
- ***DNS filtering*** can also block access to harmful sites by redirecting users to a warning page. This is useful against phishing, allowing fast updates to block lists in response to new threats and leveraging community knowledge on harmful domains.

Email Security

For email security, ***three main methods*** help verify legitimate messages and protect against spoofing: ***DKIM, SPF,*** *and* ***DMARC****.*

- ***DKIM (DomainKeys Identified Mail)****:* Adds a digital signature to email messages, confirming they're from the claimed sender. It signs parts of the email with a header called DKIM-Signature, which can be checked against the sender's public key stored in DNS.
- ***SPF (Sender Policy Framework)****:* Lists authorized email servers for a domain in DNS. If an email comes from a server not on the list, it's rejected, helping prevent unauthorized use of the domain.
- ***DMARC (Domain-based Message Authentication Reporting and Conformance)*** uses SPF and DKIM to verify email authenticity and enforce handling policies for unverified messages (accept, reject, or quarantine). This strengthens email security by reducing spoofing and phishing.

Secure Sockets Layer/Transport Layer Security

Encryption for Data Transfer: TLS encrypts data across protocols (e.g., HTTPS), securing data in transit.

Ephemeral Keys: Each connection generates a unique, temporary key via ephemeral ***Diffie–Hellman.***

Perfect Forward Secrecy (PFS): Even if a key is compromised, past and future sessions remain secure.

Simple Network Management Protocol (SNMP)

SNMP is used to monitor and manage network devices, organized in a ***Management Information Base (MIB).*** When issues occur, SNMP-enabled devices send notifications, known as SNMP traps, to an SNMP manager. Standard traps include:

- ***coldStart*** and ***warmStart*** (device restarts)
- ***linkDown*** and ***linkUp*** (link status changes)
- ***authenticationFailure*** (failed access attempts)

- ***egpNeighborLoss*** (neighboring network loss)

Custom traps can be added for specific devices, providing detailed information to the SNMP manager for action.

Secure Protocols

Unsecure protocol	Original port	Secure protocol option(s)	Secure port	Notes
DNS	UDP/TCP 53	DNSSEC	UDP/TCP 53	
FTP	TCP 21 (and 20)	FTPS	TCP 21 in explicit mode and 990 in implicit mode (FTPS)	Using TLS
FTP	TCP 21 (and 20)	SFTP	TCP 22 (SSH)	Using SSH
HTTP	TCP 80	HTTPS	TCP 443	Using TLS
IMAP	TCP 143	IMAPS	TCP 993	Using TLS
LDAP	UDP and TCP 389	LDAPS	TCP 636	Using TLS
POP3	TCP 110	POP3	TCP 995 – Secure POP3	Using TLS
RTP	UDP 16384-32767	SRTP	UDP 5004	
SNMP	UDP 161 and 162	SNMPv3	UDP 161 and 162	
Telnet	TCP 23	SSH	TCP 22	.

Figure 5 - Unsecure and Secure Protocols

- ***DNSSEC***: Provides integrity but not confidentiality for DNS. Uses digital signatures for verifying DNS data, enabling a chain of trust for IPSec, SSH, and other records.
- ***SNMPv3***: Enhances SNMP with authentication, message integrity, and encryption at authPriv security level, though insecure implementations are possible.
- ***SSH***: A secure alternative to Telnet, supporting console access and file transfers (SFTP). Uses SSH keys for authentication, but weak passwords and poor key management reduce security.
- ***HTTPS***: Uses TLS for secure HTTP traffic, ensuring data integrity and confidentiality.
- ***SRTP***: Secures audio/video streams, encrypting data and authenticating sessions to prevent replay and DoS attacks. Paired with secure RTCP for quality monitoring.
- ***LDAPS***: Adds TLS protection to LDAP, securing directory access with confidentiality and integrity.
- ***POP/IMAP with TLS***: Secures traditional email protocols (POPS, IMAPS) for email client-server communication.

- ***S/MIME***: Encrypts and signs email content and attachments, supporting confidentiality, integrity, and nonrepudiation but requiring certificate management, which limits adoption.

IPSec (Internet Protocol Security)

IPSec is a suite of protocols to secure IP traffic with encryption and authentication.

- ***Authentication Header (AH)***: Ensures ***data integrity*** and ***authenticates*** packet sources by hashing and a shared secret. AH protects both the IP payload and headers.
- ***Encapsulating Security Payload (ESP)***: Provides encryption in ***transport mode*** (protecting only the payload) and ***tunnel mode*** (protecting the entire packet). ESP can be used with AH for enhanced security but may cause issues if IP or port changes are needed.
- ***Internet Key Exchange (IKE):*** Manages the exchange of keys and security parameters between peers.
- ***Internet Security Association and Key Management Protocol (ISAKMP)*** is a framework for key exchange and authentication. It relies on protocols such as Internet Key Exchange (IKE) for implementation of that process.

DNS Attacks

- ***Domain Hijacking****:* Attackers take control of a domain through technical vulnerabilities, user system access, or social engineering. They can then intercept traffic, send emails, or impersonate the legitimate domain owner. Domains can also be taken over if owners fail to renew them. Detection is often hard for users, but domain owners can use security tools from registrars for monitoring and protection.
- ***DNS Poisoning****:* Attackers inject false DNS information to redirect traffic, either by pretending to be an authoritative server or exploiting vulnerabilities. This can lead to **DNS cache poisoning**, where cached malicious entries persist on a system until cleared, prolonging the impact even if security defences block the attack.

Credential Replay Attacks

In credential replay attacks, attackers capture and resend or delay network data to gain unauthorized access, often by re-sending authentication hashes. Modern authentication systems mitigate this with session IDs and encryption.

Common Indicators*:*

- Altered gateways or network routes, often associated with on-path (Man-in-the-Middle) attack signs.

Chapter 13 – Wireless and Mobile Security

Building Secure Wireless Networks

Cellular

Cellular networks connect mobile devices by dividing areas into "cells" with tower coverage, allowing wireless communication. Modern networks use LTE (4G) and the newer 5G, which requires more antennas but provides higher bandwidth and throughput.

- Unlike Wi-Fi, cellular connectivity is typically managed by a third-party carrier, meaning it operates independently of an organization's network and should be treated as an external connection.

Wi-Fi

- Wi-Fi encompasses wireless protocols that use the ***2.4 GHz and 5 GHz*** bands, allowing multiple networks to coexist through separate channels.
- Wi-Fi signals ***reach long distances*** but are ***affected by obstacles*** like walls and trees, with security concerns as signals may extend beyond an organization's-controlled space.
- Current standards include ***802.11ac and 802.11ax***, though older standards like 802.11n and 802.11g are still in use.
- Wi-Fi networks use ***service set identifiers (SSIDs)*** to identify their network name.
- SSIDs can be ***broadcast or kept private.***

Wi-Fi Generation	Generation Name	Maximum Speed	Frequencies
802.11b		11 Mbit/s	2.4 GHz
802.11a		54 Mbit/s	5 GHz
802.11g		54 Mbit/s	2.4 GHz
802.11n	Wi-Fi 4	600 Mbit/s	2.4 GHz and 5 GHz
802.11ac	Wi-Fi 5	6.9 Gbit/s	5 GHz
802.11ax	Wi-Fi 6 and Wi-Fi 6E	9.6 Gbit/s	2.4 GHz, 5 GHz, 6 GHz
802.11be	Wi-Fi 7	40+ Gbit/s	2.4 GHz, 5 GHz, 6 GHz

Bluetooth

- Bluetooth is a low-power, short-range (typically 5–30 meters) wireless technology operating in the 2.4 GHz range, commonly used for direct, point-to-point connections through pairing with a PIN for validation.
- Bluetooth has four security modes,
  - ***Security Mode 1:*** no security
  - ***Security Mode 2:*** Service-level enforced security

- ***Security Mode 3:*** Link-level enforced security
- ***Security Mode 4:*** Standard pairing with Security Simple Pairing (SSP)

RFID

A short-range wireless technology (from under a foot to ~100 meters) that uses tags and receivers to exchange information.

- ***Types of RFID Tags****:*
  - ***Active***: Have their own power source; constantly transmit signals.
  - ***Semi-active***: Battery-powered but activated by the reader.
  - ***Passive***: Powered entirely by the reader.
- ***Frequency Ranges****:*
  - ***Low-Frequency****:* Short-range, low power; used for entry access and ID; varies globally.
  - ***High-Frequency****:* Up to 1 meter range; faster communication; used in NFC and rewritable tags.
  - ***Ultra-High Frequency****:* Longest range and fastest; ideal for distant reader needs.
- ***Applications****:* Inventory, anti-theft, pet ID, toll way tags, etc.
- ***Security Risks****:* Vulnerable to physical damage, reprogramming, cloning, and modification.

GPS (Global Positioning System)

- Uses satellites to send signals received by GPS devices, allowing accurate location detection and timing.
- Besides U.S. GPS, alternatives like ***Russia's GLONASS*** and regional systems exist.
- ***Uses****:* Enables precise geolocation, geofencing, and time synchronization; often integrated with Wi-Fi, Bluetooth, and cellular data for richer location data.
- ***Security****:* Vulnerable to jamming and spoofing; GPS spoofing can mislead devices, but attacks are rare in typical use.

NFC

- Near-field communication (NFC) is used for very short-range communication between devices. You've likely seen NFC used for payment terminals using Apple Pay or Google Pay with cell phones.
- NFC is typically limited to less than 4 inches of range and often far shorter distances, meaning that it is not used to build networks of devices and instead is primarily used for low-bandwidth, device-to-device purposes.
- That doesn't mean that NFC can't be attacked, but it does mean that threats will typically be in close proximity to an NFC device.
- Intercepting NFC traffic, replay attacks, and spoofing attacks are all issues that NFC implementations need to account for.
- At the same time, NFC devices must ensure that they do not respond to queries except when desired so that an attacker cannot simply bring a receiver into range and activate an NFC transaction or response.

Attacks against Wireless Networks and Devices

Evil Twin Access Points

- Malicious APs mimic trusted networks to trick users.
- Attackers use stronger signals or proximity to attract victims.
- Once connected, attackers intercept user traffic, capturing sensitive data.
- Often used to present fake websites/login screens to steal credentials.

Rogue Access Points

- Unauthorized APs connected to a network, either intentionally or accidentally.
- Serve as potential entry points for attackers or unwanted users.
- Regular monitoring is essential to detect and remove rogue APs.

Bluetooth Attacks, security Issues and Mitigation

Bluetooth Attack Types:
Bluejacking: Sends unsolicited (un-requested) messages to Bluetooth devices.
Bluesnarfing: Gains unauthorized access to a device, often to steal data (e.g., contacts).

Bluetooth Security Issues:

- Many devices use weak default pairing codes (e.g., "0000").
- Session keys are derived from long-term keys, making attacks easier.

Mitigation Tips:

- Turn off Bluetooth when not in use.
- Change the default pairing code if possible.
- Keep Bluetooth devices updated with the latest patches.
- Note: Older or unsupported devices may remain vulnerable.

RF and Protocol Attack Types

Disassociation Attack

- Forces devices to disconnect (disassociate) from an access point.
- Attackers use deauthentication frames to trigger disassociation by spoofing the victim's MAC address.
- Common with WPA2 due to unencrypted management frames; WPA3 prevents this by requiring protected management frames.

Jamming Attack

- Blocks Wi-Fi or Bluetooth traffic by causing RF interference.
- Can be intentional or unintentional due to other devices using the same frequency range.

Purpose of These Attacks

- To disconnect devices, create opportunities for evil twin attacks, or capture data during reconnection attempts.

Sideloading

- Transferring files to a mobile device via USB, MicroSD, or Bluetooth to install apps outside the official store.
- Common on Android, but possible on both Android and iOS.
- Allows installation of region-restricted, unsigned, or custom apps.
- Not inherently malicious but often blocked by organizations for security reasons.

Jailbreaking

- Exploits OS vulnerabilities to gain root access and escalate privileges.
- Allows users to install unauthorized apps, modify system settings, or customize the OS.
- Can be used for malicious purposes and bypasses security restrictions.

Designing a Wireless Network

Key Points on Designing a Wi-Fi Network:

WAP (Wireless Access Point) Placement and Configuration

- Proper placement is critical for performance, usability, and security.
- Avoid overlapping channels between multiple WAPs to prevent performance degradation.
- Control signal reach to limit network access outside intended areas (e.g., buildings or premises).

Site Survey

- Walkthrough the facility to assess existing networks and physical layout.
- Critical in existing structures; often part of design in new construction.

Site Survey Tools

- Use tools to measure signal strength, map positions (using GPS), and create heatmaps.
- Heatmaps show signal strength, access point location, and channel usage, influenced by building structure and interference.

Channel Selection

- ***2.4 GHz Band***: 11 channels with overlap, commonly using channels 1, 6, and 11 to avoid interference.
- Overlap can occur in urban or crowded areas, affecting performance.
- Channels 12 and 13 are available outside the U.S. (e.g., Japan, Indonesia).

Access Point Channel Selection

- Many access points automatically select the best channel.
- Wi-Fi management software monitors for interference, adjusts channels, and manages rogue access points.

Wi-Fi Analyzer Tools

- Used to survey networks, generate heatmaps, determine channel mapping, conduct speed tests, and gather client info.
- Essential for network planning and troubleshooting.

Advanced Network Management

- Enterprise Wi-Fi controllers can adjust broadcast power to avoid interference and manage rogue devices.
- These steps are crucial for ensuring optimal performance, security, and coverage in a wireless network design.

Wi-Fi Security Standards

Feature	***WPA-2***	***WPA-3***
Modes	- WPA2-Personal (WPA2-PSK)	- WPA3-Personal
	- WPA2-Enterprise	- WPA3-Enterprise
Authentication	- User authentication (via PSK or RADIUS)	- User & network authentication
Encryption	- CCMP with AES	- Stronger encryption with optional 192-bit security mode
	- Stronger than WEP	- Enhanced encryption and key management
Password Protection	- Pre-shared key (PSK)	- Simultaneous Authentication of Equals (SAE) for stronger password protection
Brute-force Protection	No additional protection	- SAE makes brute-force attacks more difficult
Forward Secrecy	- Not available	- Perfect forward secrecy for added security
Network Authentication	- No network authentication	- Provides both user and network authentication
Deployment	- Widely used, but less secure than WPA3	- Required since mid-2020 for all Wi-Fi devices
Security Improvements	- AES encryption over WEP	- Stronger encryption, better key management, and enhanced protection
Target Users	- Home networks (WPA2-Personal)	- Home and enterprise networks (WPA3-Personal & WPA3-Enterprise)

CBC (Cipher Block Chaining): Encrypts data blocks with chaining for security.
GCM (Galois/Counter Mode): Combines counter mode with hashing for security and efficiency.
ECB (Electronic Codebook): Encrypts data blocks independently, no dependency.
CFB (Cipher Feedback): Converts block cipher to stream cipher using feedback.

Managing Secure Mobile Devices

Mobile Device Deployment Methods

Type	***Who owns the device?***	***Who controls and maintains the device?***	***Description***
BYOD – Bring Your Own Device	User	User	Employees use their personal devices for work purposes. Lower cost to org but greater risk.
CYOD – Choose Your Own Device	Organization	Organization	The organization owns and maintains the device, but allows the user to select it.
COPE – Corporate Owned, Personally Enabled	Organization	Organization	Corporate-provided devices allow reasonable personal use while meeting enterprise security and control needs.
COBO – Corporate Owned, Business Only	Organization	Organization	Company provides devices strictly for business use, with no personal use allowed.

- **Virtual Desktop Infrastructure (VDI):**
  - Provides secure access to a managed environment from low-security devices.
  - Allows users to perform tasks remotely without storing data on the device.
- **Containerization Tools:**
  - Separates work and personal environments on a device.
  - Prevents data mixing, enhancing security and privacy for both uses.

Mobile Device Management

Challenges of Mobile Device Management

- Device variability (OS, hardware, carrier settings).
- Limited built-in controls for personal-use devices.

Management Tools

MDM (Mobile Device Management): Targets mobile devices like phones and tablets.
UEM (Unified Endpoint Management): Manages a range of devices (mobiles, desktops, etc.).

Key Features in MDM/UEM

- ***Application Management:*** Control over app deployment, usage, and updates.
- ***Content Management (MCM):*** Secures and restricts access to organizational data.
- ***Remote-Wipe:*** Option to erase full device or just business data remotely.
- ***Geolocation & Geofencing:*** Allows control based on device location.
- ***Screen Locks & Passwords:*** Sets requirements for passwords and PINs.
- ***Biometrics:*** Integrates fingerprint/facial recognition for security.
- ***Context-Aware Authentication:*** Adjusts access based on location, behaviour, etc.
- ***Containerization & Storage Segmentation:*** Separates personal and work data/apps.
- ***Full-Device Encryption (FDE):*** Protects data on lost/stolen devices.
- ***Push Notifications:*** Centralized messaging for alerts and updates.

Additional Controls

- ***Application Store Management:*** Limits third-party app downloads.
- ***Rooting / Jailbreaking Detection:*** Monitors for unauthorized device modifications.
- ***Device Capabilities Control:*** Restricts camera, microphone, SMS/MMS, GPS tagging.
- ***Wireless Connectivity Management:*** Limits Wi-Fi, Bluetooth, NFC, and tethering options.

Chapter 14 – Monitoring and Incident Response

Incident Response

Incident Response *is a structured approach to managing and addressing security breaches or cyberattacks. It aims to quickly identify, contain, and mitigate incidents to minimize damage and restore normal operations.*

Incident Response Process

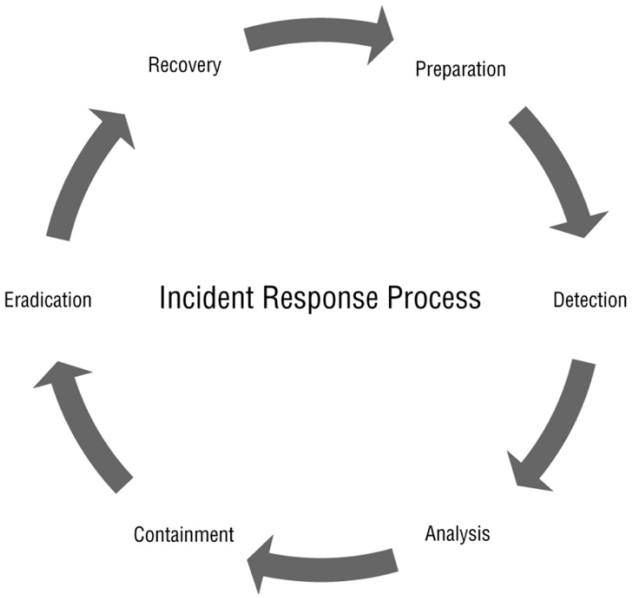

Figure 6 - Incident Response Cycle

Preparation: Establish and train the incident response team, develop response processes, and acquire necessary tools.

Detection: Monitor for indicators of compromise and analyze events to identify potential incidents.

Analysis: Investigate identified incidents to understand the scope, impact, and related events.

Containment: Isolate and control the incident to prevent further spread or damage.

Eradication: Remove malicious elements and restore affected systems to ensure full elimination.

Recovery: Return systems to normal operations and implement measures to prevent recurrence.

Lessons Learned: Review the incident to improve processes and prevent future issues, feeding back into preparation.

Incident Response Team

- ***Management/Leadership:*** Makes key decisions, communicates with senior management, and leads during emergencies.
- ***Information Security Staff:*** Core team with IR skills; handles containment using security tools (e.g., firewalls, IPS).
- ***Technical Experts (e.g., Sysadmins, Developers):*** Provide expertise on systems and architecture; aid in identifying unusual artifacts.
- ***Communications/Public Relations:*** Manages internal and external communication to protect the organization's reputation.
- ***Legal and HR:*** Advises on legal/HR matters, especially in insider or HR-related incidents.
- ***Law Enforcement (optional):*** Engaged when incidents require legal intervention or reporting.

Exercises

Tabletop Exercises use discussions among assigned personnel to validate disaster plans, identifying gaps with minimal disruption but lacking real-world accuracy.

Simulation Exercises involve practice drills where staff simulate their roles in a disaster, minimizing disruptions but requiring clear communication that it's not a real event.

Parallel Processing Exercises test backup systems or sites by moving processing to them, with some risk of disruption if systems are not fully separated.

Failover Exercises fully test switching to alternate sites or systems, offering the most realistic scenario but with the highest risk of disruption.

Building Incident Response Plans

Communication Plan: Defines roles and processes for communicating internally and externally during an incident. Ensures clear, accurate information flow to prevent confusion and missteps.

Stakeholder Management Plan: Outlines how to communicate and interact with internal and external stakeholders, prioritizing their needs and providing channels for input during the response.

Business Continuity (BC) Plan: Ensures the organization's critical systems and services remain operational during incidents, often through alternative methods or backup systems.

Disaster Recovery (DR) Plan: Focuses on restoring services after a disaster, detailing steps to recover facilities, infrastructure, and essential functions in extreme cases.

Threat Hunting

Threat hunting helps organizations achieve the detection and analysis phases of the incident response process. Threat hunters look for indicators of compromise (IoCs) that are commonly associated with malicious actors and incidents.

- ***Account Lockout:*** Repeated lockouts can signal brute-force attempts or unauthorized access attempts.
- ***Concurrent Sessions:*** Multiple sessions, especially from different locations, may indicate account compromise.
- ***Blocked Content:*** Attempted access to blocked domains or IPs often suggests malicious activity or malware.
- ***Impossible Travel:*** Logins from distant locations in short time frames point to unauthorized access.
- ***High Resource Consumption:*** Unusual disk or bandwidth usage could indicate data exfiltration or compromise.
- ***Resource Inaccessibility:*** Unexpected downtime or inaccessibility may result from malicious actions.
- ***Out-of-Cycle Logging:*** Activity occurring outside normal patterns (e.g., late-night logins) may signal suspicious behaviour.
- ***Missing Logs:*** Missing log data may suggest log tampering to hide an attacker's activity.

Understanding Attacks and Incidents

MITRE ATT&CK

- A comprehensive knowledgebase detailing adversary tactics and techniques across the threat lifecycle.
- Covers phases from ***reconnaissance*** to ***execution***, ***persistence***, ***privilege escalation***, and ***impact***.
- Provides ***enterprise matrices*** for various platforms (Windows, macOS, Linux, cloud, iOS, Android).
- Includes ***data sources***, ***threat actor groups***, and ***software*** examples for threat modeling and assessment.
- Widely regarded as the most extensive free database of adversary tactics and techniques.

Incident Response Data and Tools

Monitoring Computing Resources

Three types of monitoring:

System Monitoring:

- Uses system logs and central management tools, including cloud-based options.
- Aggregates health and performance data for analysis on central logging servers.

Application Monitoring:

- Relies on application logs, management interfaces, and performance tools.
- Monitoring requirements vary by application; each setup requires tailored monitoring.

Infrastructure Monitoring:

- Infrastructure devices use SNMP and syslog for logging.
- Vendor-specific management tools monitor and manage infrastructure devices.

Security Information and Event Management (SIEM)

- ***Core Functions:*** Collects and aggregates logs from multiple sources, performs correlation, and applies rules and analytics.
- ***Data Sources:*** Ingests data from systems, network security devices, infrastructure, and packet capture for deep network analysis.
- ***Advanced Capabilities:*** Uses machine learning/AI for behavioural analysis, sentiment analysis, and alerting on user behaviour.
- ***Alerting & Response:*** Provides alerts, reporting, and response tracking, often integrating ticketing and workflow for incident management.

Sensors

- ***Purpose*****:** Gather additional data for SIEM from locations with unique data needs (e.g., cloud infrastructure, remote datacentres).
- ***Types:*** Usually software agents but can also be virtual machines or dedicated devices.
- ***Functionality:*** Collect and forward data to SIEM, sometimes pre-processed for efficiency.
- ***Deployment & Security*****:** Strategically placed for optimal data collection and secured to prevent compromise.

Sensitivity and Thresholds

- Set thresholds and filtering rules to control alert volume and manage SIEM sensitivity.
- Alerts can be triggered based on frequency, affected systems, or high-value targets to avoid alert fatigue and reduce false positives.

Trends

- Trend analysis in SIEM reveals emerging issues, exploits, and common malware.
- Tracking trends helps identify rising threats and prioritize responses based on prevalent issues.

Alerts and Alarms

- Alerts are categorized by time, severity, source/destination, and incident type (e.g., malware infection).
- Detailed information is available for analysts to drill down and investigate.

Alert Tuning

- Adjust alerts to reduce noise and prevent unnecessary notifications.
- Involves setting thresholds, filtering out false positives, and refining for accuracy to ensure responders focus on critical events.

Log Aggregation, Correlations, and Analysis

- ***Correlation in investigations****:* Key to investigations, correlating data points (e.g., time, systems, user accounts) helps narrow down relevant information.
- ***SIEM capabilities****:* Allows searching and filtering data across multiple data points to focus on incident-related info.
- ***Automated correlation and analysis***: Matches known events and indicators of compromise to build a complete incident dataset for analysis.
- ***SIEM tools:*** Offer features like tagging and investigation, although terminology may vary between tools (e.g., AlienVault SIEM).
- ***Log aggregation tools:*** Centralized tools (e.g., syslog-ng, rsyslog) help aggregate and analyse logs.
- ***Blurring lines***: Many security tools overlap in functionality, including SIEM, SOAR, and other analysis tools.

Rules

- ***Alarm and alert rules****:* The core of SIEM functionality, rules drive alarms, alerts, and correlation engines by using conditions and logic to determine when to trigger actions.
- ***Rule conditions****:* Logic determines if/when a rule activates, triggering actions such as alerts or programmatic actions (e.g., adjusting firewall rules).
- ***Rule issues****:* Poorly constructed rules can miss events, cause false positives, or trigger overly broad detections. Mis-triggered rules with active responses can cause outages or other infrastructure issues.
- ***Rule management****:* Rules must be carefully built, tested, and regularly reviewed to ensure effectiveness.
- ***Custom-built rules****:* While default rules exist, custom rules tailored to specific environments are crucial for successful SIEM deployments.
- ***Data lifecycle and compliance****:* SIEM devices manage data retention and lifespan, often supporting compliance requirements with prebuilt rules or modules for specific standards.

Log Files

Logs provide critical incident-related data but can also be targeted by attackers. Ensuring logs are untampered and accurate (e.g., with correct timestamps) is essential.

- ***Windows Event Viewer**:* A common tool to view logs on Windows systems. In enterprise environments, logs are often sent to secure infrastructure for reliable storage.
- ***Firewall logs**:* Provide information on blocked and allowed traffic, and more advanced firewalls (NGFW, UTM) offer application-layer and IDS/IPS details.
- ***Application logs**:* Include details like installer information, errors, and license checks. Web servers (e.g., Apache, IIS) track requests and help identify attacks such as SQL injections.
- ***Endpoint logs***: Include system and service logs, as well as application installation logs, from endpoint systems and devices.
- ***OS-specific security logs**:* Windows logs record failed/successful logins and other authentication info; Linux stores authentication data in /var/log/auth.log and /var/log/secure.
- ***IDS/IPS logs***: Provide information on detected attack traffic or blocked threats by IPS.
- ***Network logs**:* Include logs from routers, switches, and packet analyzers (e.g., Wireshark) detailing configuration changes, traffic info, and network flows.
- ***Log review tools**:* SIEM tools and manual tools like grep and tail help security practitioners search for specific log entries relevant to incidents. Event IDs for Windows and log entries in Linux are often well-documented.

Going Beyond Logs – Using Metadata

Metadata provides valuable context for system operations, communications, and other activities, acting as data about other data.

- ***Email metadata**:* Includes headers with details such as sender, recipient, timestamps, attachments, email system paths, and anti-spam data.
- ***Mobile metadata**:* Collected from mobile devices, including call logs, SMS data, data usage, GPS location, and cellular tower info. Offers powerful geospatial data.
- ***Web metadata**:* Found in website code (e.g., metatags, headers, cookies) for SEO, functionality, advertising, tracking, and supporting site features.
- ***File metadata**:* Provides detailed info about files, such as creation time, modification history, author, GPS location, and device used. Exif Tool can extract metadata from photos, including camera settings and GPS coordinates if enabled.

Benchmarks and Logging

Benchmarks are used to configure systems to a standard security configuration, including log settings. They ensure systems log critical events, centralize logs, and set proper alerting levels to support security operations.

***Benchmark importance**:* At scale, benchmarks help ensure systems, services, and devices log important information in consistent, useful ways for security monitoring.

Reporting and Archiving

***Reporting**:* Involves identifying trends and providing visibility into log changes that could indicate issues requiring management attention.

***Archiving**:* Organizations must consider log data retention cycles, archiving older logs not in active use to optimize space in SIEM and maintain manageable log sizes for analysis.

Mitigation and Recovery

Security Orchestration, Automation, and Response (SOAR)

SOAR platforms help manage multiple security technologies by integrating various data sources to assess an organization's security posture and status.

- ***Challenges SOAR addresses**:* SOAR helps with integrating data from different security systems, managing security operations, and automating the remediation of issues.
- ***Mitigation and recovery**:* SOAR platforms provide tools to quickly assess an organization's attack surface, system status, and identify issues. They also automate remediation and restoration workflows to improve response efficiency.

Containment, Mitigation and Recovery Techniques

- ***Application allow lists (whitelisting)**:* Only allows specific, approved applications and files to run on a system, blocking anything not listed.
- ***Application deny lists (blacklisting)**:* Blocks known malicious or unauthorized applications and files from being installed or executed.
- ***Isolation or quarantine**:* Places suspect or infected files in a secure zone (e.g., quarantine) to prevent further damage while preserving them for investigation.
- ***Monitoring**:* Crucial for containment and mitigation, as it helps verify if systems are still compromised, detect any ongoing malicious actions, and identify other compromised resources or actions taken by attackers' post-remediation.

Configuration Changes in Remediation and Containment

Configuration changes are crucial for addressing security vulnerabilities and isolating systems or networks during an incident. These changes should be carefully tracked and recorded, as they may need to be reversed after the incident response process.

- ***Firewall rule changes**:* Adding, modifying, or removing firewall rules to restrict or allow specific traffic.
- ***Mobile Device Management (MDM) changes***: Applying new policies, remotely wiping devices, locating devices, or using MDM tools to support incident response.
- ***Data Loss Prevention (DLP) tool changes***: Adjusting DLP settings to prevent unauthorized data from leaving the organization or to detect new data types being shared.
- ***Content and URL filtering***: Blocking access to malicious or suspicious sites to prevent malware communication or phishing attacks.
- ***Updating or revoking certificates***: Revoking or updating compromised certificates, especially if attackers have access to private keys.

Broader Actions in Incident Response

In some cases, more extensive actions, such as removing systems or network segments, are required to stop the spread of an incident or when the source of the incident cannot be quickly identified.

Techniques for Broader Actions:

- ***Isolation****:* Moving a system to a protected network or space to prevent it from interacting with other systems. This can be done by disconnecting the system from the network or moving it to an isolated VLAN or environment with security rules.
- ***Containment****:* Keeping the system in place while preventing further malicious actions. This can be done through network-level containment (e.g., firewall rules) or system/application-level containment, though the latter can be complex without impacting the system's state for forensic analysis.
- ***Segmentation****:* Dividing systems into different zones or segments based on their function or security level. This can be done **before or during** an incident response to separate infected systems from unaffected systems, or to protect critical systems in more secure segments.

Root Cause Analysis (RCA)

Identifies the underlying cause of an incident and addresses systemic issues to prevent recurrence.

- ***Techniques***:
  - ***Five Whys****:* Repeatedly asking "why" to uncover the root cause.
  - ***Event Analysis****:* Determining if each event is a cause or effect.
  - ***Cause and Effect Diagramming****:* Using tools like fishbone diagrams to map causes and effects.
- ***Purpose****:* RCA helps prevent future incidents and improves preparation by addressing root causes.

Chapter 15 – Digital Forensics

Digital Forensics Concepts

Data Acquisition and Analysis

- Involves acquiring and analyzing digital forensic data.
- Data sources include drives, files, live memory, and other digital artifacts.
- Planning data gathering is crucial for a complete picture.
- Careful documentation and detailed analysis follow data collection.

Documentation Process

- Document observations, conclusions, and supporting evidence.
- Create timelines and sequences of events.
    - Use timestamps, file metadata, event logs, and other clues.
    - Goal is to piece together a complete picture of what occurred.

Human Element

- Interviews with involved individuals can provide important clues.
- Requires both technical expertise and understanding of human behaviour.

Key Skills

- Knowledge of computer science and digital artifacts.
- Investigative and analytical skills.
- Documentation and reporting abilities.
- Understanding of legal and procedural requirements.

Importance of Planning

- Proper planning is essential for comprehensive data gathering
- Ensures all potential sources of evidence are considered

Legal Holds and e-Discovery

E-Discovery Overview

- Electronic version of the legal discovery process
    - Allows parties to obtain evidence from each other in legal cases
    - Also used for public records, FOIA requests, and investigations
    - Legal holds often initiate the e-discovery process

EDRM (Electronic Discovery Reference Model) Stages

Information Governance

- Pre-emptive assessment of existing data
- Scoping and controlling data to be provided

Identification

- Locating relevant electronically stored information (ESI)

Preservation

- Ensuring data integrity and preventing changes/destruction

Collection

- Gathering information for processing and management

Processing

- Removing irrelevant data
- Formatting and collating for review and analysis

Review

- Ensuring only appropriate information is included
- Removing privileged or sensitive data

Analysis

- Identifying key elements (topics, terms, individuals, organizations)

Production

- Providing information to third parties or legal proceedings

Presentation

- Preparing data for court testimony
- Facilitating further analysis with experts or involved parties
- This EDRM framework provides a structured approach to managing the e-discovery process, ensuring thoroughness and compliance with legal requirements.

Conducting Digital Forensics

Acquiring Forensic Data

Here are the key points about the order of volatility and common forensic locations:

Order of Volatility

1. CPU registers and cache (most volatile).
2. Routing table, ARP cache, process table, kernel statistics.
3. Memory (RAM).
4. Temporary file systems and swap space.
5. Disk.
6. Remote logging and monitoring data.
7. Physical configuration, network topology.
8. Archival media (least volatile).

Importance of Order of Volatility

- Guides forensic data acquisition
- Helps prevent loss of volatile data
- Critical for capturing data intact

Common Forensic Locations

CPU cache and registers
- Rarely captured directly
- Constantly changing and highly volatile

Ephemeral data
- Process table, kernel statistics, ARP cache
- Captured through memory and disk acquisition
- Represents a specific moment in time

Random Access Memory (RAM)
- Contains encryption keys, application data
- Useful for investigations and incident response

Swap and pagefile information
- Supplements physical memory
- Can provide insights into running processes

Disk files and data
- Primary focus of many investigations
- Entire disk capture allows analysis of deleted files and artifacts

Operating system
- Windows Registry is a common analysis target

Mobile and IoT devices
- Smartphones, tablets, embedded systems

Firmware
- Less common target
- May be necessary if modified during an incident

Virtual machine snapshots
- Increasingly common artifact

Network traffic and logs
- Provides details on communications and activities

Physical artifacts
- Devices, printouts, media related to investigations

By following this order and considering these locations, forensic practitioners can maximize the preservation of critical evidence during investigations.

Cloud Forensics

Challenges faced in Cloud Forensics:

Right-to-Audit Clauses
- Part of contracts between cloud providers and organizations.
- May provide direct audit ability or agreement to use third-party auditors.
- Smaller organizations often get access to third-party audit statements instead.
- Specific audit requirements should be addressed in contracts if possible.

Regulatory and Jurisdiction Concerns

- Laws governing data may differ based on provider's location.
- Data may be stored/used in multiple global locations.
- Local jurisdictions may claim access rights to data
- Organizations address this through:
  - Contractual terms.
  - Service choices limiting data storage locations.
- Technical controls like managing own encryption keys.

Data Breach Notification Laws

- Vary by country and state (in the US)
- Contracts often specify maximum notification time
- Important to ensure breach notification clause meets organizational needs
- Some vendors may delay notifications significantly

Forensic Data Acquisition Challenges

- Directly acquiring forensic data from cloud providers is unlikely.
- May recover some data from logs or infrastructure in IaaS environments.
- Forensic data from the service itself rarely provided to customers.

Planning for Incidents and Investigations

- Organizations must have plans that don't rely on direct forensic techniques.
- Alternative approaches needed for potential incidents in cloud environments.

These considerations highlight the need for organizations to carefully plan their cloud adoption strategies, focusing on contractual agreements, regulatory compliance, and alternative forensic approaches when using cloud services.

Acquisition Tools

Some tools are:

dd (Linux command-line utility)

- Creates bit-for-bit copies of drives/devices
- Can adjust block size for better performance
- Commonly used for creating raw disk images

FTK Imager

- **Free** tool for creating forensic images
- Supports multiple formats: raw (dd), SMART, E01, AFF
- Can image physical drives, logical drives, folders, CD/DVDs
- Provides MD5 and SHA1 hash validation
- Can capture live memory from systems
- Includes option to save in AD1 native FTK format

WinHex

- Disk editing tool that can also acquire disk images
- Creates raw format and WinHex format images
- Useful for directly reading/modifying data from:
  - Drives
  - Memory
  - RAID arrays
  - Various filesystems

Acquiring Network Forensic Data

- Increasingly important role in forensic investigations
- Covers traditional wired/wireless networks, cellular networks, etc.
- Network traffic is ephemeral, requiring proactive capture and logging.

Data Sources

- Direct network traffic capture (if actively logged)
- Secondary sources:
  - Firewall logs
  - IDS/IPS logs
  - Email server logs
  - Authentication logs

Analysis Tools

- Packet analyzers like Wireshark for detailed traffic review.
- Examine packets, traffic flows, and metadata.

Collection Methods

- Network taps, span ports, port mirrors.
- Can result in massive data volumes.
- Selective capture often used for specific purposes.
- Most organizations rely on logs, metadata, and traffic flow information.

Forensic Acquisition from Other Sources

Virtual Machines

- Requires additional planning
- Challenges:
  - Running in shared environments.
  - Potential disruption to other services.
- Solution: Virtual machine snapshots
- Provide necessary information for forensic analysis.
- Can be imported into forensic tools

Containers

- Growing in use, creating new forensic challenges.
- Characteristics:
  - Designed to be ephemeral.
  - Often use shared resources.
  - Create fewer forensic artifacts than VMs or physical machines.
- Challenges:
  - Difficult to capture and return to forensically sound state.
- Emerging solutions:
  - Specialized forensic and incident response tools for containers.
  - Require additional planning.

Validating Forensic Data Integrity

Importance of Validation

- Ensures a complete, accurate copy before analysis.
- Documents data provenance.
- Ensures nonrepudiation of data and process.

Hash Validation Method

- Create hash of forensic copy and original drive.
- Compare hashes to verify identical copies.
- MD5 and SHA1 still useful for quick forensic image hashing.
- Hashes stored as part of chain-of-custody documentation.

Forensic vs. Logical Copies

- Logical copies preserve data but not exact drive state
- Forensic copies preserve full bit-by-bit content, including:
  - Deleted file remnants
  - Metadata
  - Timestamps
- Hashes of logical and forensic copies will differ

Documentation Best Practices

- Critical part of forensic process
- Tools like FTK Imager have built-in documentation support
- Include case numbers, examiner details
- Document provenance (origin and handling of evidence)
- Manual documentation should include:
  - Pictures
  - Written notes
  - Chain of custody information
  - Processes and steps taken

Data Recovery

- ***Common Use**:* Recover data from accidental deletions or system issues.
- ***File Deletion**:*
  - Deleting a file typically only removes it from the file index, not the actual data blocks.
  - Quick formatting also only clears the index; data remains recoverable.
- ***Recovery Process**:*
  - Tools/manual methods locate data by scanning for file headers/metadata.
  - Partial recovery is possible if files are partially overwritten (e.g., only overwritten blocks are unrecoverable).
- ***Slack Space**:*
  - Unused drive space (slack space) can retain valuable forensic data.
  - Forensic analysis often includes slack space review for hidden evidence.
- ***Anti-Forensics**:*
  - Secure delete tools overwrite deleted files to prevent recovery.
  - Properly overwritten data has a minimal recovery chance.

Forensic Suites and a Forensic Case Example

Forensic Suites:

- Comprehensive tools for forensic acquisition, analysis, and reporting.
- ***Examples**:*
  - ***FTK** & **EnCase***: Leading commercial suites.
  - ***Autopsy***: Open-source with extensive forensic capabilities.

Reporting

Importance of the Report

- Final product; must be clear, relevant, and concise.

Typical Forensic Report Structure

- ***Summary**:* Overview of the investigation and findings.
- ***Forensic Process**:* Details on tools used and assumptions made.
- ***Findings**:* Sections per device/drive with evidence-backed conclusions.
- ***Recommendations**:* Detailed suggestions beyond the summary.

Accuracy

- Findings must be precise, with conclusions strongly supported by evidence.

Full Documentation

- Analysts may include a comprehensive report for complete transparency.

Digital Forensics and Intelligence

Primary Uses

- Legal cases, internal investigations, and incident response.
- Strategic intelligence & counterintelligence in national defense.

Capabilities

Adversary Analysis: Analyzing advanced threat tools and tactics.

Data Recovery: Forensic analysis of recovered or acquired devices for intelligence purposes.

Tools & Techniques:

- Overlaps with traditional forensics, but with added methods for:
- Encryption Breaking
- Software/Hardware Analysis
- Anti-tamper Data Recovery

Chapter 16 – Security Governance and Compliance

Security Governance

Purpose: Establish procedures and controls for organizational direction.
Importance: Essential for large organizations to avoid chaos and ensure coordinated efforts.
Function:

- Coordinates work across all organizational layers.
- Aligns tasks and processes with the organization's strategy and goals.

Corporate Governance

Purpose: Guide the strategic direction, planning, and execution for large organizations, particularly publicly traded corporations.

Governance Model:

Shareholders: Owners of the corporation but too numerous/uninvolved for daily decisions.
Board of Directors: Elected by shareholders; holds ultimate authority and represents shareholder interests.

- Composed of major shareholders and experts; independent directors required by stock exchanges.

CEO: Hired by the board to manage operations, with oversight and performance reviews by the board.

Hierarchical Delegation:

- CEO delegates to senior executives → senior executives manage middle managers → middle managers supervise individual contributors.
- Governance cascades down to ensure strategic alignment and effective management.

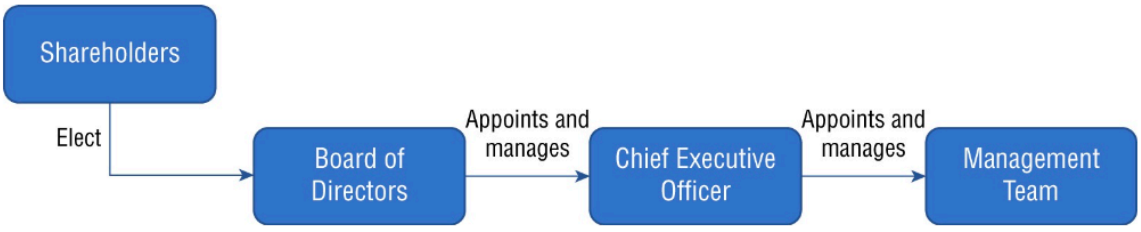

Figure 7 - Typical Corporate Governance Model

Information Security Governance Essentials

Integration with Corporate Governance

***Hierarchy**:* CEO delegates information security to the CISO, aligning security governance with corporate goals.

Role of the CISO:

- Collaborates with the CEO and senior management to align security strategy with organizational objectives.
- Designs an information security governance framework tailored to the organization's management structure.

Governance Framework:

- Establishes a management structure for the cybersecurity team.
- Includes policies and mechanisms to enforce security across the organization.

Authority and Communication:

- Follows corporate governance channels; establishes escalation procedures for management support when needed.

Governance Structure

- ***Centralized**:* Top-down approach where a central authority sets policies/standards for organization-wide enforcement.
- ***Decentralized**:* Bottom-up approach, allowing individual business units flexibility to meet cybersecurity goals.

Understanding Policy Documents

An organization's information security policy framework contains a series of documents designed to describe the organization's cybersecurity program.

Policies: High-level statements setting overall security direction.
Standards: Specific, mandatory security requirements.
Procedures: Step-by-step instructions to implement standards.
Guidelines: Recommended practices that provide flexibility.

Policies

Definition: High-level statements of management intent, with mandatory compliance.

An information security policy will generally contain broad statements about cybersecurity objectives, including the following:

Importance of Cybersecurity: Emphasizes cybersecurity's critical role within the organization.

Approval and Flexibility: Policies often require high-level approval, such as from the CEO, and remain broad to allow flexibility in adapting specific security measures as the business and technology landscape changes.

Confidentiality, Integrity, Availability (CIA): Requires all staff and contractors to protect the organization's information and systems.

Ownership: Clarifies the ownership of information created or possessed by the organization.

CISO or Responsible Executive: Designates the CISO or another executive as responsible for cybersecurity efforts.

Delegation of Authority: Empowers the CISO to create standards, procedures, and guidelines to implement the policy.

Information Security Policy Library

Organizations commonly include the following documents in their information security policy library:

Information security policy that provides high-level authority and guidance for the security program

Incident response policy that describes how the organization will respond to security incidents

Acceptable use policy (AUP) that provides network and system users with clear direction on permissible uses of information resources

Business continuity and disaster recovery policies that outline the procedures and strategies to ensure that essential business functions continue to operate during and after a disaster, and that data and assets are recovered and protected.

Software development life cycle (SDLC) policy that establishes the processes and standards for developing and maintaining software, ensuring that security is considered and integrated at every stage of development.

Change management and change control policies that describe how the organization will review, approve, and implement proposed changes to information systems in a manner that manages both cybersecurity and operational risk.

Standards

Purpose: Standards provide specific, mandatory requirements to implement information security policies, often subject to more frequent updates than policies.

Example: UC Berkeley's "Minimum Security Standards for Electronic Information" outlines required controls based on data sensitivity, including secure configurations.

Industry Compliance: Following established industry standards can mitigate legal risks and is often seen as a best practice.

Key Standards:
- ***Password requirements*** (length, complexity, etc.)
- ***Access control*** (account life cycle management)
- ***Physical security*** (premises and asset protection)
- ***Encryption*** (for data in transit and at rest)

Procedures

- ***Purpose:*** Procedures are mandatory, ***step-by-step instructions*** that guide consistent, repeatable actions to meet security objectives in specific scenarios.
- ***Common Examples:***
  - ***Change Management Procedures:*** Outlines steps for performing change management activities per policy, potentially using tools like version control.
  - ***Onboarding and Offboarding Procedures:*** Defines processes for adding new user accounts and removing them when no longer needed.
  - ***Incident Response Playbooks:*** Provides specific actions for the incident response team to follow during particular incident types.
- ***Usage:*** Procedures vary based on an organization's operational needs, covering tasks like system setup, code releases, and security incident handling.

Guidelines

- ***Purpose:*** Guidelines offer best practices and recommendations for specific concepts, technologies, or tasks, aiding in consistent and effective security practices.
- ***Compliance:*** Following guidelines is optional, though adherence can vary by organizational culture, with some encouraging stricter observance.
- ***Usage:*** Serves as helpful advice for tasks without strict requirements, providing flexible support for informed decision-making across security practices.

Monitoring and Revision

- ***Policy Monitoring:*** Involves continuous evaluation of policy implementation and effectiveness using tools like SIEM systems, audits, and assessments to ensure alignment with security needs, regulations, and tech updates. Gathering feedback from staff is key.
- ***Policy Revision:*** When issues are identified, policies are updated to address gaps or adapt to new requirements. Revised policies must be communicated to relevant staff, with training as needed for compliance.
- ***Importance:*** Regular monitoring and timely revision help maintain a responsive and resilient security posture.

Change Management

Change Management Process is a structured approach for reviewing, approving, and implementing modifications to an organization's systems or policies. It aims to minimize risk, ensure continuity, and maintain security by controlling how changes are planned, tested, and communicated across teams.

Change Management Process and Controls

Change Approval Process:

A formal process for managing change which avoids downtime, confusion, and mistakes.

Steps:

1. ***Request the Change****:* Personnel submit change requests via internal platforms, which log the request and track its status.
2. ***Review the Change****:* Experts evaluate the change, often involving various stakeholders and possibly a formal Change Advisory Board (CAB) for larger changes.
3. ***Approve/Reject the Change***: Changes are approved or rejected based on the review. A rollback or backout plan is created if needed.
4. ***Test the Change****:* The approved change is tested in a nonproduction environment to identify potential issues.
5. ***Schedule and Implement the Change***: Changes are scheduled to minimize system impact, with a backout plan in place to revert the system if necessary.
6. ***Document the Change****:* The change is recorded in the configuration management system to ensure all parties are informed and to assist in restoring the system if needed.

Impact analysis

- Determine a risk value: high, medium, low.
- The risks can be minor or far-reaching.
- The “fix” might not actually fix anything.
- The “fix” breaks something else.
- Operating system failures.
- Data corruption.

- What's the risk with NOT making a change?
  - Security vulnerability
  - Application unavailability
  - Unexpected downtime to other services.

Test Results

- Sandbox testing environment.
  - Has no connection to the real world or production system.
  - A technological safe space.
- Use before making a change to production.
  - Try the upgrade, apply the patch.
  - Test and confirm before deployment.
- Confirm the backout plan.
  - Move everything back to the original.
  - A sandbox can't consider every possibility.

Backout plan

- You should always have a way to revert your changes. (Prepare for the worst, hope for the best)
- Some changes are difficult to revert.
- Always have backups.

Maintenance window

- When is the change happening?
- During the workday may not be the best option as a potential downtime would affect a large part of production.
- Overnights are often a better choice.
- The time of the year may be a consideration.

Standard operating procedure

- Change management is critical.
  - Affects everyone in the organization.
- The process must be well documented.
  - Should be available on the internet along with the standard processes and procedures.
- Changes to the process are reflected in the standards.

Technical Change Management

- Puts the change management process into action.
- Change management is often considered with “what” needs to change.
- The technical team is concerned with “how” to change it.
- Includes:
  - Allow list, deny list.
  - Restricted activities
  - Downtime
  - Restart
  - Legacy applications
  - Dependencies
  - Documentation
  - Version Control

Version Control

Version control tracks software changes over time using a labelling or numbering system, ensuring access to the latest version and careful management through the release process.

Documentation

Documentation records the current system configuration, including responsibilities, purposes, and changes to the baseline. It is stored in a formal configuration management system and must be updated after every change to ensure accuracy.

Personnel Management

Least Privilege: Employees should only be granted the minimum permissions necessary for their job. This prevents privilege creep, where an employee accumulates unnecessary access over time.
Separation of Duties: Critical tasks should be divided so that no single employee has full control over both. This reduces the risk of fraud, as collusion is required to bypass controls (e.g., no one person should create vendors and issue checks).
Two-person Control: Similar to separation of duties, this requires two employees to perform a sensitive action, ensuring oversight and reducing fraud risk.
Job Rotation and Mandatory Vacations: Rotating employees in sensitive roles and enforcing mandatory vacations helps uncover fraud by disrupting concealment activities, allowing others to detect issues.
Clean Desk Space: Employees must secure sensitive information before leaving their desks to protect confidentiality.
Onboarding and Offboarding: Standardized processes for hiring and terminating employees ensure controlled access to organizational assets, including background checks for new hires and proper revocation of credentials upon departure.
Nondisclosure Agreements (NDAs): Employees must protect confidential information during and after their employment, with reminders given at hire and during exit interviews.

Social Media: Organizations may implement social media policies to guide employee behaviour on personal and professional platforms, aligning with organizational interests and security.

Third-Party Risk Management

Vendor Selection

- Organizations must carefully evaluate vendors during selection, especially those handling critical processes or sensitive information.
- This involves assessing financial stability, reputation, security practices, and compliance. Conflicts of interest should also be identified and managed.

Vendor Assessment

- After selection, continuous evaluation is essential.
- Methods include penetration testing, audits, third-party assessments, and supply chain analysis.
- Regular questionnaires can track performance and compliance.

Vendor Agreements

Master Service Agreements (MSA): Contracts covering ongoing and future vendor relationships.

Service Level Agreements (SLA): Define performance expectations and remedies.

Memorandums of Understanding (MOU): Informal agreements to clarify relationships.

Memorandums of Agreement (MOA): Formal documents specifying roles, responsibilities, and terms.

Business Partner Agreements (BPA): Define partnership terms, including responsibilities, management, operations and profit-sharing.

Work Order (WO): A document that authorizes, initiates, and tracks the progress and completion of a ***particular job*** or task.

Statement of Work (SOW): A detailed agreement between a client and a vendor that describes the work to be performed ***on a project***.

Complying with Laws and Regulations

Complying with Laws and Regulations*:* Cybersecurity regulations aim to protect individuals, government, and society from the impact of cybersecurity vulnerabilities. Different regions have specific compliance requirements:

HIPAA (Health Insurance Portability and Accountability Act): Applies to U.S. healthcare providers, insurers, and health information clearinghouses, focusing on security and privacy of health-related data.

PCI DSS (Payment Card Industry Data Security Standard): Specifies rules for handling, storing, and transmitting credit/debit card information. Although not a law, it is a contractual obligation for merchants and service providers globally.
GLBA (Gramm-Leach-Bliley Act): Requires U.S. financial institutions to have formal security programs to protect customer financial data.

SOX (Sarbanes-Oxley Act): Applies to U.S. publicly traded companies, ensuring that IT systems that store or process financial records are secure and reliable.

GDPR (General Data Protection Regulation): Enforces security and privacy for personal information of EU residents, applicable globally.

FERPA (Family Educational Rights and Privacy Act): Mandates U.S. educational institutions to protect student educational records.

Compliance Reporting

Organizations conduct both internal and external compliance reporting to ensure adherence to regulations and maintain transparency.

Internal Compliance Reporting: Regular reports are generated for management or the board, summarizing compliance status, identifying gaps, and offering recommendations. This helps decision-makers understand the compliance environment, prioritize resources, and align compliance goals with organizational strategy.

External Compliance Reporting: Often mandated by regulators or **contracts**, this involves submitting evidence to demonstrate regulatory adherence. For example, organizations handling credit card data may report to the PCI SSC, while those under GDPR must provide documentation to data protection authorities. External reporting maintains regulatory good standing, helps avoid penalties, and builds trust with customers and partners by showcasing a commitment to security and privacy.

Consequences of Noncompliance

Financial Penalties: Large fines (e.g., GDPR fines up to 4% of global turnover).
Operational Restrictions: Possible suspension or revocation of licenses critical to operations.
Reputational Damage: Loss of customer trust and damage to brand image.
Contractual Losses: Contract terminations and lost business opportunities.
Legal Action: Risk of lawsuits, leading to additional costs and resource diversion.

Compliance Monitoring

Due Diligence: Continuous research on relevant legal and regulatory requirements.
Due Care: Regularly reviewing, updating, and maintaining policies and controls.

Attestation & Acknowledgment: Ensuring employees and partners confirm awareness and adherence to compliance policies.
Internal Monitoring: Conducting internal audits, reviews, and checks to verify compliance.
External Monitoring: Engaging third-party audits for unbiased compliance assessment.
Automation: Using automated solutions for efficient monitoring, policy enforcement, and reporting, minimizing errors and saving resources

Adopting Standard Frameworks

Purpose: Standard frameworks provide a structured approach for building or evaluating cybersecurity programs.

NIST Cybersecurity Framework (CSF)

Widely used framework with applications across sectors, helping organizations develop a standardized security program.

Objectives

- Describe current and target cybersecurity states.
- Identify improvement opportunities.
- Track progress toward goals.
- Communicate cybersecurity risks internally and externally.

Components of NIST CSF

- ***Framework Core****:* Five security functions ***(Identify, Protect, Detect, Respond, Recover)*** divided into categories and subcategories.
- ***Implementation Tiers****:* Maturity model with four tiers assessing cybersecurity readiness.
- ***Framework Profile****:* Tailored approach that reflects an organization's current and desired security posture.

ISO Standards

ISO 27001

- Focuses on Information Security Management System (ISMS).
- Covers 14 categories, including security policies, access control, cryptography, incident management, and compliance.
- Certification available for organizations in highly regulated sectors.

ISO 27002

- Expands on ISO 27001 by detailing specific security controls.
- Used for selecting, implementing, and managing information security controls.

ISO 27701

- Privacy extension to ISO 27001/27002.
- Provides guidance for implementing privacy controls.

ISO 31000

- General risk management guidelines applicable across various risks, not limited to cybersecurity.

Security Awareness and Training

User Training: Regular, varied training sessions, including computer-based training, help users understand and mitigate risks.

Role-Based Training: Tailors training based on job roles, e.g., technical staff vs. customer-facing staff, ensuring relevance and effectiveness.

Phishing and Anomalous Behaviour

- Anti-phishing campaigns and simulations educate users on recognizing phishing attempts.
- Anomalous behaviour recognition helps detect insider threats.

Essential Training Topics

- Security policies and situational awareness.
- Insider threats and password management.
- Risks of removable media and social engineering.
- Operational security practices and hybrid/remote work security.

Training Frequency: Conduct initial training for new hires and annual refreshers, balancing time and benefits.

Development and Execution

- Develop content based on a risk assessment and use engaging, real-world examples.
- Deliver training through various methods (workshops, e-learning) to suit different learning styles.

Reporting and Monitoring

- Track participation and assess knowledge through quizzes.
- Provide regular reports to stakeholders and update content as needed based on feedback and trends.

Chapter 17 – Risk Management and Privacy

Analyzing Risk

Risks are an inherent part of daily life, but manageable with simple precautions.

Key Terms:

Threats: Events that could harm information confidentiality, integrity, or availability.
Vulnerabilities: Weaknesses in systems or controls exploitable by threats.
Risks: Result from the intersection of a threat and a vulnerability. Both must be present for a risk to exist.

Enterprise Risk Management (ERM):

Definition: A structured approach to assess and manage risks within an organization.
Process: Identify risks, evaluate their severity, and choose suitable risk management strategies.

Risk Identification

Risk Sources

- Risks can originate from various sources such as hackers, natural disasters, and operational failures.

Risk Types

- **External Risks**: Arise from outside the organization (e.g., cyber threats, natural disasters).
- **Internal Risks**: Originate within the organization (e.g., insider threats, human errors, equipment failures).
- **Multiparty Risks**: Affect multiple organizations (e.g., power outages, SaaS provider data breaches).
- **Legacy System Risks**: Outdated systems with unpatchable vulnerabilities require extra protection.
- **Intellectual Property (IP) Theft Risks**: Disclosure of proprietary information risks business advantage.
- **Software Compliance/Licensing Risks**: Non-compliance with software licensing can lead to financial and legal issues.

Risk Categories

- Financial, reputational, strategic, operational, and compliance risks should all be considered.

Risk Assessment

Risk Assessment Factors
- **Likelihood of Occurrence**: The probability that a risk will occur.
- **Magnitude of Impact**: The potential severity of the risk.

Risk Severity = Likelihood * Impact

Severity Evaluation
- Combining likelihood and impact gives a conceptual risk score to prioritize mitigation.

Regulatory Considerations
- Regulations like GDPR can significantly affect the risk impact assessment.

Types of Risk Assessments
- **One-time Risk Assessments**: Snapshot of risk at a specific time.
- **Ad Hoc Risk Assessments**: Assessments done in response to specific events.
- **Recurring Risk Assessments**: Regular assessments to track risks.
- **Continuous Risk Assessments**: Ongoing monitoring of risks for quick responses.

Risk Analysis

Risk Analysis Methodologies
- **Quantitative Risk Analysis**: Uses numerical data for prioritization.
- **Qualitative Risk Analysis**: Uses subjective judgment for risks that are hard to quantify.

Quantitative Risk Analysis Steps
- **Asset Value (AV)**: The dollar value of the asset at risk.
- **Annual Rate of Occurrence (ARO)**: The expected annual frequency of the risk.
- **Exposure Factor (EF)**: The percentage of asset damage if the risk occurs.
- **Single Loss Expectancy (SLE)**: The financial loss from a single risk event (AV × EF).
- **Annualized Loss Expectancy (ALE)**: The yearly financial loss from the risk (SLE × ARO).

Formula:

ALE = ARO x SLE

SLE = AV x EF

Example
- **Risk**: Denial-of-service (DoS) attack on an email server.
- **Asset**: The ability to send emails generating $1,000 per hour in sales.
- **Risk Probability (ARO)**: 3 times per year.
- **Exposure Factor (EF)**: 90% (server capacity lost during the attack).
- **SLE**: $2,700 (asset value × exposure factor).
- **ALE**: $8,100 (SLE × ARO).

Qualitative Risk Analysis:

- **Purpose:** Assesses risks that are hard to quantify, like reputational damage or employee morale.
- **Method:** Uses subjective judgment on probability and impact (e.g., Low/Medium/High).
- **Example:** Risks like stolen unencrypted devices and spearphishing attacks, both rated high for probability and impact, help prioritize actions like full-disk encryption and secure email gateways.

Risk Mitigation

- **Definition**: Applying security controls to reduce the likelihood or impact of a risk.
- **Controls**: Can be single or multiple measures, aiming to reduce the probability, impact, or both.
- **Example 1 (Theft of Laptops)**:
  - **Control 1**: Cable locks reduce theft probability.
  - **Control 2**: Tamperproof registration tags act as a deterrent and help recover stolen devices.
- **Example 2 (DDoS Attack)**:
  - **Control 1**: Increase bandwidth and server capacity to absorb attacks.
  - **Control 2**: Use third-party DDoS mitigation services to block malicious traffic before it reaches the network.

Risk Avoidance

- Involves changing business practices to eliminate a risk entirely.
- **Drawback**: Often has a significant negative impact on operations.
- **Example**: Banning laptops to prevent theft or shutting down a website to avoid DDoS attacks.

Risk Transference

- Shifts the impact of a risk to another entity (e.g., insurance).
- **Example**: Purchasing property insurance for stolen laptops or cybersecurity insurance for DDoS attacks.

Risk Acceptance

- Accepting the risk when mitigation is too costly or unnecessary.
- **Example**: Deciding not to invest in laptop insurance or DDoS mitigation if the costs outweigh the impact.
- **Exemptions/Exceptions**: Formal processes to allow temporary acceptance of a risk under certain conditions.

Risk Tracking

The key terms related to risk management:
Inherent Risk: The original level of risk present before any controls are implemented. It is the natural risk inherent in an organization's operations.

Residual Risk: The remaining risk after controls are applied to mitigate, avoid, or transfer the inherent risk.

Risk Appetite: The level of risk an organization is willing to accept in pursuit of its objectives.

Risk Threshold: The specific point at which a risk becomes unacceptable. It is often more quantitative and triggers action when exceeded.

Risk Tolerance: The organization's ability to endure risks without significant impact on its operations.

Key Risk Indicators (KRIs): Metrics that provide early warning signals for rising risks, helping track the effectiveness of risk mitigation efforts and ensuring residual risk stays within the risk appetite.

Risk Owner: The person or entity responsible for managing and monitoring risks, ensuring controls are in place, and mitigating risks effectively.
These concepts help guide an organization's approach to risk management by progressively reducing inherent risk until it falls within acceptable levels defined by the organization's risk appetite and tolerance.

Risk Register

A **risk register** tracks and manages risks, helping risk managers communicate with business leaders. It includes details like:

Risk Owner: The person responsible for managing the risk.
Risk Threshold: The level at which a risk becomes unacceptable.
Key Risk Indicators (KRIs): Metrics that signal rising risks.

For senior leaders, a **risk matrix** or **heat map** summarizes risks and highlights the most significant ones.

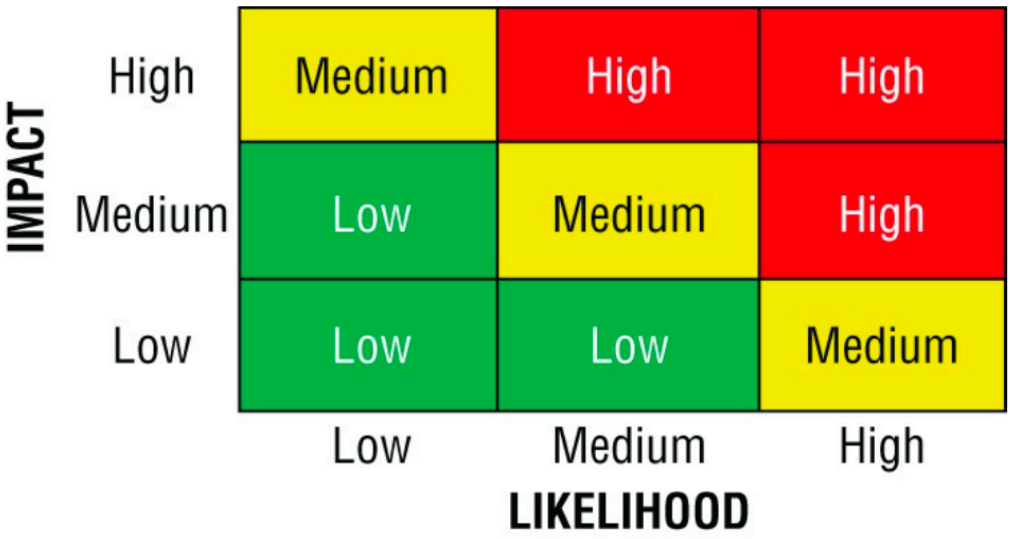

Figure 8 - Risk Matrix

Risk Reporting

Risk Reporting communicates the status and evolution of risks to stakeholders, ensuring informed decision-making. Types of reports include:
Regular Updates: Routine reports on risks, controls, and developments.
Dashboard Reporting: Visual summaries with graphs and charts for real-time monitoring.
Ad Hoc Reports: Produced as needed for specific events or situations.
Risk Trend Analysis: Analyses historical data to predict future risks.
Risk Event Reports: Documents specific incidents and responses.

Disaster Recovery Planning

Disaster Recovery Planning (DRP) focuses on creating plans to restore operations quickly after a disaster, whether natural or human made. The goal is to minimize disruption and recover normal operations.

Disaster Types

Disasters can be external or internal, including environmental and human-made events. A disaster recovery plan is activated when a disaster disrupts business operations.

Business Impact Analysis (BIA)

This formal process identifies mission-essential functions and critical systems. Key BIA metrics include:

- **Mean Time Between Failures (MTBF)**: Expected time between system failures.
- **Mean Time to Repair (MTTR)**: Average time to restore systems after failure.

- **Recovery Time Objective (RTO)**: Maximum acceptable downtime for a system.
- **Recovery Point Objective (RPO)**: Maximum acceptable data loss during an outage.

Single Points of Failure

Identify critical systems that, if they fail, could cause a significant outage. Redundancy (e.g., extra power supplies or servers) resolves these risks.

Privacy

Cybersecurity professionals protect the confidentiality, integrity, and availability of information, including Personally Identifiable Information (PII), to prevent privacy breaches, which could lead to identity theft, reputational damage, fines, and loss of intellectual property.

Privacy Risks

Privacy risks have legal and financial implications, and organizations must understand privacy requirements across local, national, and global jurisdictions. Privacy notices and statements in customer agreements can help organizations formalize privacy practices.

Data Inventory

Organizations need a data inventory of sensitive information, including:
PII: Information identifying an individual.
PHI: Health-related data (e.g., HIPAA).
Financial Information: Personal financial data (e.g., GLBA, PCI DSS).
Intellectual Property: Trade secrets, formulas, strategies.
Legal Information: Documents related to legal affairs.
Regulated Information: Data governed by laws or regulations.

Information Classification

Classifying data by sensitivity helps prevent unauthorized disclosure. Examples include:
Top Secret: Highest protection.
Secret: Significant protection.
Confidential: Some protection.
Unclassified: Not publicly released without authorization.
Businesses may use terms like "Highly Sensitive" and "Internal" for similar categories.

Data Roles and Responsibilities

Data Owners: Senior executives responsible for specific data types (e.g., HR data handled by HR VP).
Data Subjects: Individuals whose data is processed, with rights to access or delete their data
Data Controllers: Entities that determine the reasons and methods for processing personal data.
Data Stewards: Individuals who implement data controller policies.
Data Custodians: Those responsible for the secure safekeeping of data.
Data Processors: Third-party service providers processing data on behalf of the data controller.

Data Protection Officers (DPO)

Organizations should designate a DPO to oversee data privacy efforts, particularly under the EU's GDPR. The DPO ensures compliance without undue oversight.

Information Life Cycle

Data protection should be maintained throughout the information life cycle:

Data Minimization: Collect only necessary data
Purpose Limitation: Use data only for its intended purpose
Retention Standards: Retain data only as long as necessary
Secure Destruction: Safely destroy data once its life cycle ends.

Privacy Enhancing Technologies (PETs):

De-identification: Removes identifiers to prevent linking data to individuals.
Hashing: Converts data into a fixed hash value, but can be vulnerable to rainbow table attacks.
Tokenization: Replaces sensitive data with a unique identifier, requiring a secure lookup table for recovery.
Data Masking: Redacts part of sensitive data (e.g., replacing digits in credit card numbers with "X"s).

Privacy and Data Breach Notification:

In case of a breach, organizations must activate their **incident response plan** and notify affected parties.

- **U.S.**: Varies by state with industry-specific laws.
- **EU GDPR**: Requires notification within 72 hours.
  Organizations should consult legal experts to comply with breach notification laws.

Glossary/Acronyms and Abbreviations

1. **EDR (Endpoint Detection and Response):** EDR solutions monitor and respond to security threats on endpoints like desktops and laptops. They provide real-time threat detection, investigation, and response capabilities.
2. **SIEM (Security Information and Event Management):** SIEM aggregates and analyses log data from various sources to provide a unified view of an organization's security posture, enabling real-time alerts and compliance reporting.
3. **SOAR (Security Orchestration, Automation, and Response):** SOAR platforms automate security operations, threat intelligence, and response tasks to reduce response times and enhance efficiency in incident handling.
4. **SLE (Single Loss Expectancy):** The single loss expectancy (SLE) is the amount of financial damage expected each time a risk materializes. It is calculated by multiplying the AV by the EF.
5. **Annualized Rate of Occurrence (ARO):** number of times the risk is expected each year.
6. **IDS/IPS (Intrusion Detection/Prevention Systems):** IDS monitors network traffic for suspicious activity, while IPS can also take action to block threats in real time, enhancing network security.
7. **DLP (Data Loss Prevention):** DLP tools prevent unauthorized access, use, and transmission of sensitive data, helping to safeguard information from leaks or breaches, especially in compliance-heavy industries.
8. **RPO (Recovery Point Objective)** is the maximum acceptable amount of data loss measured in time.
9. **RTO (Recovery Time Objective)** is the maximum acceptable time to restore systems and resume normal operations after a disaster.
10. **WAF (Web Application Firewall):** WAFs protect web applications by filtering, monitoring, and blocking malicious HTTP traffic, commonly used to defend against common web-based attacks like SQL injection or XSS.
11. **NGFW (Next-Generation Firewall):** NGFWs offer advanced traffic filtering, including application awareness and control, integrated intrusion prevention, and the ability to block sophisticated malware.
12. **NAC (Network Access Control):** NAC ensures only authorized and compliant devices can access network resources by enforcing policies that restrict unauthorized devices or users from connecting.
13. **UEBA (User and Entity Behaviour Analytics):** UEBA solutions use machine learning to identify abnormal behaviours from users and devices, helping to detect insider threats, fraud, and compromised accounts.
14. **IAM (Identity and Access Management):** IAM solutions manage digital identities and enforce policies ensuring that the right users have the appropriate access to critical resources at the right times.
15. **PKI (Public Key Infrastructure):** PKI provides encryption, identity verification, and digital certificates to enable secure communication and authentication over public networks.
16. **XDR (Extended Detection and Response):** XDR integrates security tools and data sources across endpoints, networks, and clouds to provide a holistic threat detection and response capability.

17. **VPN (Virtual Private Network):** VPNs secure communication by encrypting internet traffic between a user's device and the internet, often used to protect data and maintain privacy on public networks.
18. **CASB (Cloud Access Security Broker):** CASBs enforce security policies between cloud service users and providers, offering visibility and control over cloud applications and data in transit.
19. **SAST (Static Application Security Testing):** SAST tools analyze source code to detect security vulnerabilities during the development phase, allowing developers to fix issues early in the software lifecycle.
20. **DAST (Dynamic Application Security Testing):** DAST tools assess running applications for vulnerabilities by simulating attacks to identify weaknesses in the application's behaviour and security controls.
21. **Vulnerability scanners (Nessus, Qualys, OpenVAS):** These tools scan networks, systems, and applications for known vulnerabilities, providing reports and recommendations for remediation.
22. **Antivirus/Anti-malware tools**: These tools detect, prevent, and remove malicious software like viruses, worms, and trojans to protect individual systems and networks.
23. **Password managers (LastPass, Bitwarden):** These tools securely store and manage passwords, ensuring strong, unique passwords are used without needing to remember them all manually.
24. **Encryption tools (GPG, BitLocker):** These tools encrypt files, disks, and communications to protect sensitive data from unauthorized access, ensuring confidentiality and integrity.
25. **RAID - Redundant Arrays of Inexpensive Disks:** Common solution that uses multiple disks with data either striped (spread across disks) or mirrored (completely duplicated), and technology to ensure that data is not corrupted or lost (parity).
26. **Packet analysis tools (Wireshark):** Wireshark captures and analyzes network traffic to help security analysts understand and troubleshoot network issues and detect potential security incidents.
27. **Metasploit:** A penetration testing framework used to identify and exploit vulnerabilities in systems, allowing ethical hackers to assess the security posture of networks.
28. **Burp Suite:** A web vulnerability scanner that helps identify security issues in web applications by automating and manual testing methods, commonly used for penetration testing.
29. **Scapy:** A packet manipulation tool that allows users to craft, send, and analyze network packets for tasks such as network testing, packet sniffing, and attack simulation.

Cryptography Tools

1. **AES (Advanced Encryption Standard):** AES is a symmetric encryption algorithm used to protect data by transforming plaintext into ciphertext, widely adopted for securing sensitive data.
2. **DSA (Digital Signature Algorithm)** - is a cryptographic standard for generating and verifying digital signatures using modular arithmetic and discrete **logarithms**.
3. **RSA (Rivest-Shamir-Adleman):** RSA is an asymmetric encryption algorithm used for secure data transmission, commonly employed for digital signatures and secure key exchanges.

4. **ECC (Elliptic Curve Cryptography):** ECC provides strong encryption with **smaller key sizes** compared to RSA, making it efficient for mobile devices and modern cryptographic systems. **Asymmetric algorithm.**
5. **ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)**: leverages ECC for enhanced security and efficiency.
6. **ECDSA (Elliptic Curve Digital Signature Algorithm)** - is a cryptographic algorithm used for creating secure digital signatures based on elliptic curve cryptography.
7. **SHA (Secure Hash Algorithm):** SHA is a family of cryptographic hash functions that generate fixed-length digests for data integrity checks, commonly used in digital signatures and certificates.
8. **HMAC (Hash-based Message Authentication Code):** HMAC combines a cryptographic hash function with a secret key to ensure data integrity and authenticity during transmission.
9. **Diffie-Hellman (DH):** Diffie-Hellman is a key exchange algorithm that enables two parties to securely exchange cryptographic keys over a public channel without prior communication.
10. **DES/3DES (Data Encryption Standard/Triple DES):** DES is a now-outdated symmetric encryption algorithm, replaced by AES, while 3DES improves security by encrypting data three times using different keys.
11. **GPG (GNU Privacy Guard):** GPG is a free tool for encrypting and signing data and communications using public-key cryptography, often used for securing emails and files.
12. **Digital Signatures:** These cryptographic techniques ensure data authenticity and integrity by allowing the sender to sign a message, providing proof of origin and protecting against tampering.
13. **TLS (Transport Layer Security):** TLS is a cryptographic protocol that provides end-to-end security for communications over networks, primarily used for securing HTTPS traffic.
14. **Quantum Cryptography:** An emerging field leveraging quantum mechanics principles to enhance security, particularly through quantum key distribution (QKD), which enables ultra-secure key exchange.
15. **PGP (Pretty Good Privacy):** PGP is a popular encryption program used for securing emails and files, using a combination of symmetric and asymmetric encryption to protect data confidentiality.
16. **SSL (Secure Sockets Layer):** SSL is an older cryptographic protocol for securing communications over the internet, replaced by TLS but still widely referred to in legacy contexts.
17. **S/MIME (Secure/Multipurpose Internet Mail Extensions):** A technology for securing email communications through encryption and digital signatures, often integrated into modern email platforms.
18. **IKE (Internet Key Exchange):** A protocol used in establishing secure VPN connections, it helps in setting up shared cryptographic keys for securing communications between devices.

Acronyms and Abbreviations

1. ACL – Access Control List
2. AES – Advanced Encryption Standard
3. AIS – Automated Indicator Sharing
4. APT – Advanced Persistent Threat
5. AV – Antivirus
6. BYOD – Bring Your Own Device
7. CA – Certificate Authority
8. CAPTCHA – Completely Automated Public Turing test to tell Computers and Humans Apart
9. CC – Common Criteria
10. CIO – Chief Information Officer
11. CISO – Chief Information Security Officer
12. CIRT – Cyber Incident Response Team
13. CSP – Cloud Service Provider
14. CSRF – Cross-Site Request Forgery
15. CVE – Common Vulnerabilities and Exposures
16. CVSS – Common Vulnerability Scoring System
17. DDoS – Distributed Denial of Service
18. DES – Data Encryption Standard
19. DLP – Data Loss Prevention
20. DKIM – DomainKeys Identified Mail
21. DMARC – Domain-based Message Authentication Reporting and Conformance
22. DNS – Domain Name System
23. DNSSEC – Domain Name System Security Extensions
24. DoS – Denial of Service
25. DRP – Disaster Recovery Plan
26. EDR – Endpoint Detection and Response
27. ESP – Encapsulating Security Payload
28. FIM – File Integrity Monitoring
29. FIPS – Federal Information Processing Standards
30. FRR – False Rejection Rate
31. FTP – File Transfer Protocol
32. GPG – GNU Privacy Guard
33. GPS – Global Positioning System
34. HIDS – Host-Based Intrusion Detection System
35. HIPAA – Health Insurance Portability and Accountability Act
36. HMAC – Hash-based Message Authentication Code
37. HSM – Hardware Security Module
38. HTTP – Hypertext Transfer Protocol
39. HTTPS – Hypertext Transfer Protocol Secure
40. IAM – Identity and Access Management
41. ICMP – Internet Control Message Protocol
42. ICS - Industrial controls systems
43. IDS – Intrusion Detection System
44. IEC – International Electrotechnical Commission

45. IKE – Internet Key Exchange
46. IMAP – Internet Message Access Protocol
47. IoC – Indicator of Compromise
48. IoT – Internet of Things
49. IP – Internet Protocol
50. IPS – Intrusion Prevention System
51. ISAC - Information Sharing and Analysis Center
52. ISMS – Information Security Management System
53. ISO – International Organization for Standardization
54. ISP – Internet Service Provider
55. IT – Information Technology
56. IV – Initialization Vector
57. KMS – Key Management System
58. LDAP – Lightweight Directory Access Protocol
59. MAC – Media Access Control
60. MFA – Multi-Factor Authentication
61. MITM – Man-In-The-Middle
62. ML – Machine Learning
63. MSSP – Managed Security Service Provider
64. MTTR – Mean Time to Repair
65. NAC – Network Access Control
66. NAT – Network Address Translation
67. NDA – Non-Disclosure Agreement
68. NIDS – Network Intrusion Detection System
69. NIST – National Institute of Standards and Technology
70. NGFW – Next-Generation Firewall
71. NOC – Network Operations Center
72. OCSP – Online Certificate Status Protocol
73. OID - identifier used for PKI objects
74. OAUTH – Open Authorization
75. OWASP – Open Web Application Security Project
76. PAM – Privileged Access Management
77. PCI DSS – Payment Card Industry Data Security Standard
78. PGP – Pretty Good Privacy
79. PII – Personally Identifiable Information
80. PKI – Public Key Infrastructure
81. PSK – Pre-Shared Key
82. RAT – Remote Access Trojan
83. RAID - Redundant Arrays of Inexpensive Disks
84. RBAC – Role-Based Access Control
85. RDP – Remote Desktop Protocol
86. RSA – Rivest-Shamir-Adleman
87. SAML – Security Assertion Markup Language
88. SAST – Static Application Security Testing
89. SCADA - Supervisory Control and Data Acquisition
90. SIEM – Security Information and Event Management
91. SLE – Single Loss Expectency

92. SMB – Server Message Block
93. SMTP – Simple Mail Transfer Protocol
94. SOC – Security Operations Center
95. SOAR – Security Orchestration, Automation, and Response
96. SOP – Standard Operating Procedure
97. SPF – Sender Policy Framework
98. SQLi – SQL Injection
99. SSH – Secure Shell
100. SSL – Secure Sockets Layer
101. STIX - Structured Threat Information eXpression
102. TAXII - Trusted Automated eXchange of Intelligence Information
103. TFA – Two-Factor Authentication
104. TLS – Transport Layer Security
105. UEBA – User and Entity Behaviour Analytics
106. URL – Uniform Resource Locator
107. USB – Universal Serial Bus
108. VPN – Virtual Private Network
109. VoIP – Voice over Internet Protocol
110. WAF – Web Application Firewall
111. WAN – Wide Area Network
112. WPA – Wi-Fi Protected Access
113. XDR – Extended Detection and Response
114. XML – Extensible Markup Language
115. XSS – Cross-Site Scripting