13.11 Injection Attacks

XML and LDAP injection attacks - an injection attack can target other types of protocols where the application takes user input to construct a query, filter or document.

Extensible markup language (xml) injection - xml is used by apps for authentication and authorizations and for other types of data exchange and uploading.

Lightweight directory access protocol (ldap) injection - ldap is another example of query language. ldap is specifically used to read and write network directory databases. a threat actor could exploit either unauthenticated access or a vulnerability in a client app to submit arbitrary ldap queries. This could allow accounts to be created or deleted or for the attacker to change authorizations and privileges.

For example a web form could construct a query from authenticating the valid credentials for bob and pa$$w0rd like this:

(& (username = bob)(password = pa$$w0rd))

If the form input is not sanitized, the threat actor could bypass the password check by entering a valid username plus an ldap filter string

(& (username = bob)(&))

Directory traversal & command injection attacks - directory traversal is another type of injection attack performed against a web server.

The threat actor submits a request for a file outside the web server's root directory by submitting a path to navigate to the parent directory (../)

The threat actor might use a **canonicalization** attack to disguise the nature of the malicious input.

Canonicalization refers to the way the server converts between different methods by which a resource (file path or url) may be represented and submitted to the simplest method used by the server to process the input.

Server-side request forgery (SSRF) - SSRF causes the server application to process an arbitrary request that targets another service either on the same host or a different one.

It exploits both the lack of authentication between the internal servers and services and weak input validation allowing the attacker to submit unsanitized requests or api parameters.

SECTION 14 -

SUMMARIZE SECURITY GOVERNANCE CONCEPTS

14.1 Regulations, Standards & Legislation

Key Frameworks, Benchmarks And Configuration Guides May be Used to Demonstrate Compliance With A Country's Legal Requirements.

Due Diligence Is a Legal Term meaning that Responsible Persons have not been negligent in Discharging their Duties.

- Sarbanes-Oxley Act (Sox) Mandates The Implementation Of Risk Assessments, Internal Controls And Audit Procedures.
- The Computer Security Act (1987) Requires Federal Agencies To Develop Security Policies For Computer Systems That Process Confidential Information.
- In 2002, The Federal Information Security Management Act (Fisma) Was Introduced To Govern The Security Of Data Processed By Federal Government Agencies.

Some Regulations Have Specific Cybersecurity Control Requirements While Others Simply Mandate "Best Practice" As Represented By A Particular Industry Or International Framework.

Personal Data And General Data Protection Regulation (GDPR)

This legislation focuses on information security as it affects privacy or personal data.

GDPR means that personal data cannot be collected, processed or retained without the individual's informed consent.

Compliance issues are complicated by the fact that laws derive from different sources e.g gdpr does not apply to american data subjects but it does apply to american companies that collect or process the personal data of people in eu countries.

National, Territory Or State Laws

In the US there are federal laws such as the gramm-leach-bliley act (GLBA) for financial services and the health insurance portability and accountability act (HIPAA).

14.2 ISO and Cloud Frameworks

ISO 27k - The International Organization For Standardization (ISO) Has Produced A Cybersecurity Framework In Conjunction With The International Electro Technical Commission (IEC).

Unlike The NIST Framework, The ISO 27001 Must be Purchased. The ISO 27001 Is part of an Overall 27000 Series Of Information Security Standards Also Known As 27k.

There Are 3 Main Versions Of The ISO 27k

- **27002 -** Security Controls
- **27017 & 27018 -** Cloud Security
- **27701 -** Personal Data & Privacy

ISO 31k - This Is An Overall Framework For Enterprise Risk Management (ERM). Erm Considers Risks And Opportunities Beyond Cybersecurity By Including Financial, Customer Service And Legal Liability Factors.

Cloud Security Alliance (CSA) - The Not-For-Profit Organization Produces Various Resources To Assist Cloud Service Providers (CSP) In Setting Up And Delivering Secure Cloud Platforms.

Security Guidance - A Best Practice Summary Analyzing The Unique Challenges Of Cloud Environments And How On-Premises Controls Can Be Adapted To Them.

Enterprise Reference Architecture - Best Practice Methodology And Tools For CSPs To Use In Architecting Cloud Solutions.

Cloud Controls Matrix - Lists Specific Controls And Assessment Guidelines That Should Be Implemented By CSPs.

Statements On Standards For Attestation Engagements (SSAE) - the SSAE are audit specifications developed by the American institute of certified public accountants (AICPA). These audits are designed to assure consumers that service providers (notably cloud providers) meet professional standards.

Within SSAE No. 18, There Are Several Levels Of Reporting:

Service Organization Control (Soc2) - Soc2 Evaluates The Internal Controls Implemented By The Service Provider To Ensure Compliance With Trust Services Criteria (TSC) When Storing And Processing Customer Data.

An Soc Type 1 Report Assesses The System Design, While A Type 2 Report Assesses The Ongoing Effectiveness Of The Security Architecture Over A Period Of 6-12 Months.

Soc2 Reports Are Highly Detailed And Designed To Be Restricted.

Soc 3 - A Less Detailed Report Certifying Compliance With Soc2. They Can Be Freely Distributed.

14.3 Governance Structure

Enterprise Governance - This is a system that holds to account, directs and controls all entities involved in an organization.

Governance is useful in identifying roles and responsibilities.

A role is a specific position or job title that an individual occupies within an organization. Stewardship is the responsible oversight and protection of something entrusted to one's care. Responsibility refers to the specific duties or tasks that an individual is expected to fulfill within a given role.

Board of Directors

- Determine the desired future state of information/cyber security and provide funding.
- Exercise Due Care (providing the standard of care that a prudent person would have provided under the same conditions.)
- A fiduciary is a person or organization who holds a position of trust
- They also provide oversight and authorization of organizational activities.

Executive Management Duties

- Make decisions to achieve strategic goals and objectives
- Manage risks to an acceptable risk and also comply with applicable laws and regulations.
- Manage resources and the budget efficiently
- Evaluate performance measures
- Implement oversight process

Information Security Steering Committee

- Make decisions to achieve information security strategic goals and objectives
- Set a cybersecurity budget, authorize risk decisions and report to the board of committee.
- They provide an effective communication channel for ensuring the alignment of the security program and business objectives.

Chief Information Security Officer (CISO) - Interprets strategic decisions and is ultimately responsible for the success or failure of the information security program.

Supporting roles include Information Assurance Officer/Manager (IAO/IAM), Information Security Officer (ISO)

Complimentary Organization Roles

- **Privacy Officer -** Responsible for developing and implementing all aspects of the privacy program.
- **Compliance Officer -** Responsible for identifying all applicable regulatory and contractual requirements.
- **Physical Security Officer -** Responsible for ensuring that appropriate physical security procedures are implemented
- **Internal Audit -** Responsible for providing independent and objective assurance services.

Functional Roles

- **Owners -** Responsible for oversight and decisions related to access control and protection.
- **Custodians -** Responsible for advising, managing and monitoring data protection controls.
- **Users -** Responsible for treating data in accordance with security policies and objectives.

14.4 Governance Documents

These are used to communicate direction, expectations and rules.

They are typically derived from the information security strategy which is also derived from the desired future state.

Policies

- These codify the high-level requirements for securing information assets and ensure CIA
- They should be approved and authorized by the organization's highest governing body
- Modifications should be minor over extended periods of time

Standards, Baselines & Guidelines

- Standards serve as precise specifications for the implementation of policy and dictate mandatory requirements.
- Baselines are the aggregate of standards for a specific category or grouping such as a platform, device type or location
- Guidelines assist in helping to understand and conform to a standard. Guidelines are not mandatory.

Procedures - Procedures are instructions for how to carry out an action. They focus on discrete actions or steps with a specific starting and ending point.

- **Simple Step -** Lists sequential actions. There is no decision making
- **Hierarchical -** Organizes the instructions in a hierarchical structure where each level is nested within the one above it.
- **Graphic -** Presents in pictorial or symbol form.
- **Flowchart -** Is used to communicate a process and when decision making is required.

Plan - This is a detailed strategy or tactic for doing or achieving something.

The function of the plan is to provide instructions and guidance on how to execute or respond to a situation within a certain timeframe usually with defined stages and with designated resources.

Acceptable Use Policy (AUP) - This details user community obligations pertaining to

Information and information systems. It contains rules that specifically pertain to acceptable behavior and actions that are prohibited.

It's a teaching document that develops security awareness and must be written in a way that is easy to understand.

Non-disclosure Agreement (NDA) - Establishes data ownership and the reason why the data is being provided.

It's primarily used to prevent data disclosure and prevents forfeiture of patent rights.

Acceptable Use Policy Agreement - When a user signs it, they acknowledge that they understand and agree to abide by the AUP including violation sanctions up to and including termination.

Agreement should be executed prior to being granted access to information and information systems.

14.5 Change Management

The objective is to drastically minimize the risk and impact a change can have on business operations.

Types of Changes

- **Standard -** Occurs frequently, is low risk and has a pre-established procedure with documented tasks for completion (updates, patch management)
- **Normal -** Not standard but also not an emergency. Can be approved by the change control board (change of anti-malware product)
- **Major -** May have significant financial implications and could be high risk. May require multiple levels of management approval (change to new Operating system)
- **Emergency -** This is one that must be assessed and implemented without prior authorization to quickly resolve a major incident (switch to a backup server)

Configuration Management KPIs - Key Performance Indicators (KPIs) are business metrics used to measure performance in relation to strategic goals and objectives.

- **Successful Changes -** The higher the better
- **Backlog of Changes -** Changes not yet completed and should not grow over time
- **Emergency Changes -** It should not trend upward

14.6 Configuration Management

This is a set of practices designed to ensure that Configuration Items (CI) are deployed in a consistent state and stay that way through their frame. The primary goal is to minimize risk and ensure the configuration of services are known, good and trusted.

Configuration Management Elements

- **Configuration Item (CI) -**This is an aggregation of information system components and treated as a single entity throughout the configuration management process.
- **Baseline Configuration (BC) -** A set of specifications for a CI that has been reviewed and agreed upon and can be changed only through change control procedures.

Automated Provisioning - This is the ability to deploy information technology (IT) or operational technology (OT) systems and services using predefined automated procedures without requiring human intervention.

The primary goal is to reduce or eliminate manual dependencies and human error.

Provisioning Processes

- **Demand -** Generated Resource Allocation - is the automatic provisioning and deprovisioning of resources based upon demand.
- **Idempotence -** Is a principle that every time an automated configuration script is run, the same exact result is produced.
- **Immutable System -** Immutability is the principle that resources should not be changed, only created and destroyed (replace not fix).
- **Infrastructure as Code -** Is using code to manage configurations and automate provisioning of infrastructure. Supports Idempotence.

14.7 Scripting, Automation & Orchestration

Scripting - This is a set of instructions (interactive/non-interactive) used to automate a sequence of repetitive tasks.

Usually written in a scripting language which means they are interpreted and not compiled (the scripts are read and executed line-by-line by the processor at runtime).

Scripting Tools

- **Python -** Interpreted, open-source programming language with an extensive available library.
- **PowerShell -** Microsoft automation and configuration management framework
- **Bash -** Linux | Unix shell command line interface (CLI) and scripting language.
- **Macro -** An automated input sequence that imitates keystrokes or mouse actions.

Adversarial Scripting

- **Python -** Very easy to learn and is used for writing attack code and tools
- **PowerShell -** Can be used to direct the execution of a local script, retrieve and execute remote resources using various network protocols and encode payloads.
- **Bash -** Can be used to direct the execution of a local script, retrieve and execute remote resources using various network protocols and automate tasks on a LINUX/UNIX platform
- **Macro -** A macro virus can infect a software program and trigger a set of actions when the program is opened or run.

Automation - This is the execution of tasks without human intervention.

The goals are to eliminate manual dependencies and human error, improve quality of service, increase agility and reduce risk. Typically requires significant investment.

Orchestration - Orchestration is the coordination and management of multiple computer systems, applications and/or services, stringing together multiple tasks in order to execute a larger workflow or process.

SECTION 15 - EXPLAIN RISK MANAGEMENT

15.1 Risk management process

Risk management involves all processes from assessing the risk to managing it.

- **Identify Assets** - Humans, data, emails, hardware (scoping)
- **Identify Vulnerabilities** - Weak passwords, unpatched systems
- **Identify Exploits & Threats** - Hackers, natural disasters
- **Determine Safeguards & Countermeasures** - Security policies, backups, patches, updates etc
- Determine which risks are acceptable or not

Enterprise risk management - Risk management is treated very differently in companies of different sizes and compliance requirements. most companies will institute enterprise risk management (erm) policies and procedures based on frameworks such as nist's rmf

Risk Types

- External
- Internal
- Multiparty (Supply Chain Attack)
- Intellectual Property (Ip) Theft
- Software Compliance/Licensing
- Legacy Systems

Quantitative risk assessment - This aims to assign concrete values to each risk factor:

- **Single loss expectancy (sle) -** The amount that would be lost in a single occurrence of the risk factor. it's calculated by multiplying the value of the asset by an exposure factor (ef). ef is the percentage of the asset value that would be lost.
- **Annualized loss expectancy (ale) -** The amount that would be lost over the course of a year. done by multiplying the sle by the annualized rate of occurrence (aro)

It's important to realize that the value of an asset isn't just about its material value but also the damage its compromise could cost the company (e.g a server is worth more than its cost).

Qualitative risk assessment - Seeks out people's opinions of which risk factors are significant. assets and risks may be placed in categories such as high, medium or low value and critical, high, medium or low probability respectively.

Risk Factor	Impact	ARO	Cost Of Control	Overall Risk
Legacy Windows Clients	⚠	✖	⚠	✖
untrained Staff	✔	⚠	✔	⚠
No Antivirus Software	⚠	✖	⚠	✖

15.2 Risk Controls

Risk Mitigation - This is the most common method of handling risk and typically involves the use of countermeasure or safe guards. The likelihood of the risk occurring must be reduced to the absolute minimum.

Risk Avoidance - The cost of the risk involved is too high and must be avoided. Mitigation means the risk probabilities are reduced to the maximum while avoidance means the risk is eliminated completely

Risk Transference - This involves assigning or transferring the risk to another entity or organization. In other words, the risk is outsourced because the organization cannot mitigate the risk on it's own due to cost.

Risk Acceptance - The cost of mitigating the risk outweighs the cost of losing the asset. Risk can also be accepted when there isn't a better solution.

Risk Appetite & Residual Risk - Where risk acceptance has the scope of a single system, risk appetite has a project or institution-wide scope and is typically constrained by regulation and compliance. Where inherent risks are the risks before security controls have been applied, residual risks are those carried over after the controls have been applied.

Control risk is a measure of how much less effective a security control has become over time e.G antivirus.

Risk Register - A document showing the results of risk assessments in a comprehensible format.

Business Impacts and Risk Value

	Risk Criticality	Overall Projected Loss	Critical Systems Downtime	Non-Critical Systems Downtime	Data Leak	Brand Damage	Compliance	Calculated Value
5	Critical	>50 M	>30 min	>24 Hrs	Highly sensitive PII for more than 5 people	Re-branding, loss of major accounts	Major (Ex. License loss)	$100 M
4	High	5-50 M	Up to 30 min	5-24 Hrs	Detailed PII for multiple people	Major damage sustained for years	Fines >$200k, investigation impacting business	$50 M
3	Medium	500k-5 M	None	1-5 Hrs	General PII for multiple people or senstive PII for up to 5	Moderate reputational damage	Fines $200k-2 M, investigation not impacting business	$5 M
2	Low	50k-500k	None	Up to 1 Hr	None	Minor	Fines <$10k	$500k
1	Very Low	<50k	None	None	None	None	None	$5k

15.3 Business Impact Analysis

Business Impact Analysis (BIA) - This is the process of assessing what losses might occur for a range of threat scenarios.

Where BIA identifies risks, the business continuity plan (BCP) identifies controls and processes that enable an organization to maintain critical workflows in the face of an incident.

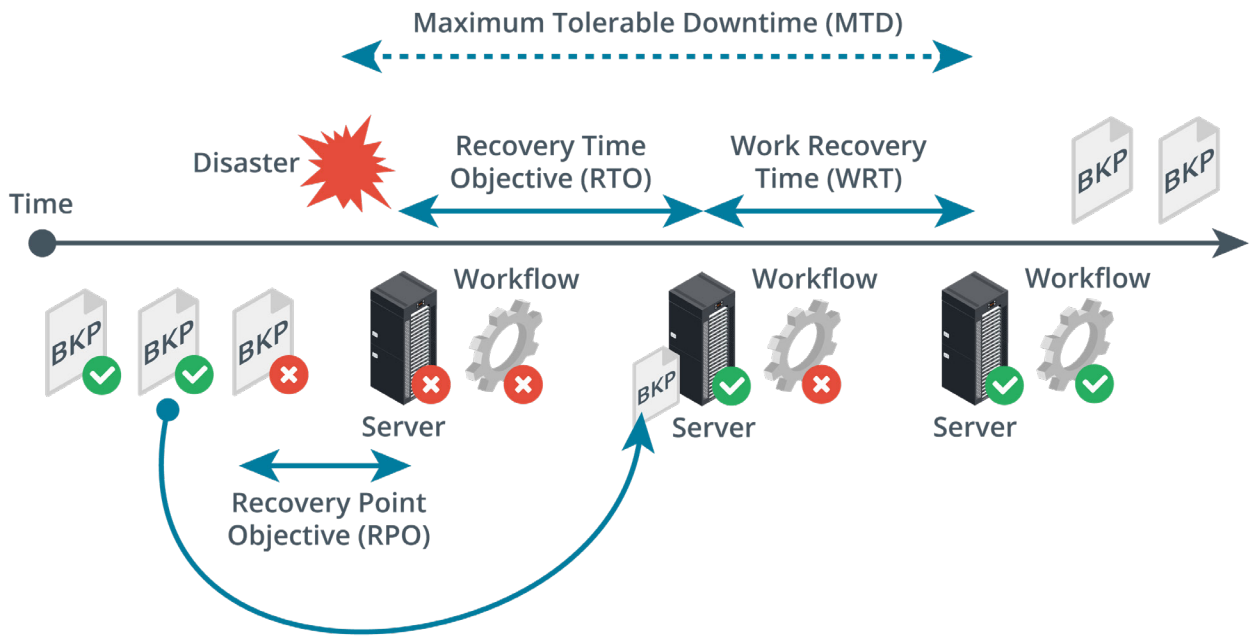
Mission Essential Function (MEF) - This is one that cannot be deferred. the business must be able to perform the function as close to continually as possible.

Maximum Tolerable Downtime (MTD) - The maximum amount of time a business can be down before it can no longer recover in a reasonable time or manner.

Recovery Time Objective (RTO) - The targeted amount of time to recover business operations after a disaster.

Work Recovery Time (WRT) - Following systems recovery, there may be additional work to reintegrate different systems, test overall functionality and brief system users on any changes.

Recovery Point Objective (RPO) - Refers to the maximum amount of data that can be lost after recovery from a disaster before the loss exceeds what is tolerable to an organization.



Identification of critical systems - Asset types include:

- People
- Tangible assets
- Intangible assets (ideas, reputation, brand)
- Procedures (supply chains, critical procedures)

Single points of failure - A SPOF is an asset that causes the entire workflow to collapse if it is damaged or unavailable. Can be mitigated by provisioning redundant components.

Mean time to failure (MTTF) and **mean time between failures (MTBF)** represent the expected lifetime of a product. MTTF should be used for non-repairable assets for example, a hard drive can be described with an MTTF while a server with MTBF.

- Calculation for mtbf is the total time divided by the number of failures. For example 10 devices that run for 50 hours and two of them fail, the mtbf is 250.
- Calculation for mttf for the same test is the total time divided by number of devices so 50 hours/failure.

Mean time to Repair (MTTR) is a measure of the time taken to correct a fault so that the system is restored to full operation. This metric is important for determining the overall RTO.

Disasters

- **Internal Vs External -** Internal Could Be System Faults Or Malicious/Accidental Act By An Employee
- **Person-Made -** War, Terrorism, Pollution
- **Environmental -** Natural Disaster

A Site Risk Assessment Should Be Conducted To Identify Risks From These Factors.

Disaster Recovery Plans

- Identify Scenarios For Natural And Non-Natural Disasters And Options For Protecting Systems
- Identify Tasks, Resources And Responsibilities For Responding To A Disaster

- Train Staff In The Disaster Planning Procedures And How To React Well To Change.

Functional Recovery Plans

- Walkthroughs, Workshops And Seminars
- **Tabletop Exercises -** Staff “Ghost” The Same Procedures As They Would In A Disaster Without Actually Creating Disaster Conditions.
- **Functional Exercises -** Action Based Sessions Where Employees Can Validate The Drp By Performing Scenario-Based Activities In A Simulated Environment
- **Full-Scale Exercises -** Action Based Sessions That Reflect Real Situations. Held On Site And Uses Real Equipment And Real Personnel.

15.4 Third-Party Risk Management & Security Agreements

A root of trust is only trustworthy if the vendor has implemented it properly. Anyone with time and resources to modify the computer’s firmware could create some sort of backdoor access.

For a tpm to be trustworthy, the supply chain of chip manufacturers, firmware authors and the administrative staff responsible for providing the computing device to the user must all be trustworthy.

When assessing suppliers for risk, it is helpful to distinguish two types of relationship

- **Vendor -** This means a supplier of commodity goods and services possibly with some level of customization and direct support.
- **Business partner -** This implies a closer relationship where two companies share quite closely aligned business goals.

End of life systems - When a manufacturer discontinues the sales of a product, it enters an **end of life (EOL)** phase in which support and availability of spares and updates become more limited.

An end of service life (EOSL) system is one that is no longer supported by its developer or vendor.

Windows versions are given five years of mainstream support and five years of extended support (during which only security updates are provided).

Organizational security agreements - It is important to remember that although one can outsource virtually any service to a third party, one cannot outsource legal accountability for these services.

Issues of security risk awareness, shared duties and contractual responsibilities can be set out in a formal legal agreement.

Memorandum of understanding (mou) - A preliminary agreement to express an intent to work together. They are usually intended to be relatively informal and not contract binding.

Business partnership agreement (bpa) - The most common model of this in it are the agreements between large companies and their resellers and solution providers.

Nondisclosure agreement (NDA) - Used between companies and employees/contractors/ other companies as a legal basis for protecting information assets.

Service level agreement (SLA) - A contractual agreement describing the terms under which a service is provided.

Measurement systems analysis (MSA) - A means of evaluating the data collection and statistical methods used by a quality management process to ensure they are robust.

15.5 Audit & Assurance

Information security assessment - This is the process of determining how effectively the entity being evaluated meets the specific security requirements.

- **Examination -** is the process of interviewing, reviewing, inspecting, studying and observing to facilitate understanding, comparing standards or to obtain evidence (audit)
- **Testing -** is the process of exercising objects under specified conditions to compare actual and expected behaviors (pen testing)

Assurance -This is the measure of confidence that intended controls, plans and processes are effective in their application.

The objective of an audit is to provide independent assurance based on evidence.

Audit plan - This is a high-level description of audit work to be performed in a specific time frame.

The plan may include objectives, resource requirements and reporting expectations. The final audience for the audit results is either an executive or board audit committee.

Audit focus

- **Compliance -** Meeting laws, regulations and industry standards.
- **Security & privacy -** Attaining required levels of cia and privacy
- **Internal controls -** Evaluation of the design of the controls and assessment of the operational effectiveness and efficiency of the controls
- **Alignment -** Assure alignment with organizational and control objectives.

Sampling - This is used to infer characteristics about a population based upon the characteristics of a sample of that population.

Evidence sampling is applying a procedure to less than 100% of the population.

Audit examination opinions

- **Unqualified -** Rendered when the auditor does not have any significant reservations (clean report)
- **Qualified -** Rendered when there are minor deviations or scope limitations.
- **Adverse -** Rendered when the target is not in conformance with the control objectives or when the evidence is misleading or misstated.
- **Disclaimer -** This means the auditor was not able to render an opinion due to certain/ named circumstances.

Audit framework - This is a structured and systematic approach used by auditors to plan, execute and report on an audit engagement. They are typically developed by auditing standards-setting bodies.

- Isaca cobit 5
- Aicpa (ssae18)

Ssae 18 soc versions

- Soc1 is a report of controls relevant to user entities financial statements
- Soc2 is based upon trust services principles (tsp) reports on controls intended to mitigate risk related to security, cia and privacy
- Soc 3 is similar to soc2 but does not detail testing performed and is designed for public distribution.

15.6 PenTest Attack Life Cycle

- **Reconnaissance -** Is typically followed by an initial exploitation phase where a software tool is used to gain some sort of access to the target's network.
- **Persistence -** this is the tester's ability to reconnect to the compromised host and use it as a remote access tool (rat) or backdoor.
- **Privilege escalation -** The tester attempts to map out the internal network and discover the services running on it.
- **Lateral movement -** Gaining control over other hosts and usually involves executing the attack or scripting tools such as powershell.
- **Pivoting -** If a pen tester achieves a foothold on a perimeter server, a pivot allows them to bypass a network boundary and compromise servers on an inside network.
- **Actions on objectives -** For a threat actor, this means stealing data while for a tester it would be a matter of the scope definition.
- **Cleanup -** For an attacker, this means removing evidence of the attack while for a pen tester, this means removing any backdoors or tools and ensuring the system is not less secure than its pre-engagement state.

SECTION 16 -

SUMMARIZE DATA PROTECTION AND COMPLIANCE CONCEPTS

16.1 Privacy & Sensitive Data Concepts

The value of an information asset can be determined by how much damage its compromise would cause the company.

It is important to consider how sensitive data must be secured not just at rest but also in transit.

Information life cycle management

- Creation/collection
- Distribution/use
- Retention
- Disposal

Data roles & responsibilities - A data governance policy describes the security controls that will be applied to protect data at each stage of its life cycle.

Data owner - A senior executive role with ultimate responsibility for maintaining the cia of the information asset. The owner also typically chooses a steward and custodian and directs their actions and sets the budget and resource allocation for controls.

Data steward - Primarily responsible for data quality. Ensuring data is labeled and identified with appropriate metadata and that it is stored in a secure format

Data custodian - This role handles managing the system on which the data assets are stored. This includes responsibility for enforcing access control, encryption and backup measures.

Data privacy officer (dpo) - This role is responsible for oversight of any personally identifiable information (pii) assets managed by the company.

In the context of legislation and regulations protecting personal privacy, the following two institutional roles are important

Data controller - The entity responsible for determining why and how data is stored, collected and used for ensuring that these purposes and means are lawful. The controller has ultimate responsibility for privacy breaches and is not permitted to transfer that responsibility.

Data processor - An entity engaged by the data controller to assist with technical collection, storage or analysis tasks. A data processor follows the instructions of a data controller with regard to collection or processing.

Data classifications - Data can be classified based on the degree of confidentiality required.

- **Public (unclassified) -** no restrictions and can be viewed by the public. Poses no real risk to the company.
- **Confidential (secret) -** Highly sensitive information to be viewed only by authorized people and possibly by trusted parties under an nda.
- **Critical (top secret) -** Extremely valuable information and viewing is severely restricted.

Data can also be classified based on the kind of information asset.

- **Proprietary/intellectual property (ip) -** Information created and owned by the company typically about the products they make.
- **Private/personal data -** Information that relates to an individual identity.
- **Sensitive -** Refers to company data that could cause serious harm or embarrassment if it is leaked to the public. Sensitive personal data includes political opinions, sexual orientation, health records , tax records etc.

Data types

Personally identifiable information (PII) - This is data that can be used to identify, contact or locate an individual such as a social security number.

An IP address can also be used to locate an individual and could be considered to be a type of pii.

Customer data -This can be institutional information but also personal information about the customer's employees such as sales and technical support contacts.

Financial information -This refers to data held about bank and investment accounts plus tax returns and even credit/debit cards. The payment card industry data security standard (pci dss) defines the safe handling and storage of this information.

Government data - Government agencies have complex data collection and processing requirements. The data may sometimes be shared with companies for analysis under very strict agreements to preserve security and privacy.

Data retention -This refers to backing up and archiving information assets in order to comply with business policies and applicable laws and regulations.

16.2 Data Sovereignty, Privacy Breaches & Data Sharing

Data sovereignty & geographical considerations - Some states and nations may respect data more or less than others and likewise some nations may disapprove of the nature and content of certain data.

Data sovereignty refers to a jurisdiction preventing or restricting processing and storage from taking place on systems that do not physically reside within that jurisdiction. For example gdpr protections are extended to any eu citizen while they are within the eu borders.

Geographic access requirements fall into two different scenarios

- Storage locations might have to be carefully selected to mitigate data sovereignty issues. Most cloud providers allow choice of data centers for processing and storage, ensuring that information is not illegally transferred from a particular privacy jurisdiction without consent.
- Employees needing access from multiple geographic locations. Cloud-based file and database services can apply constraint-based access controls to validate the user's geographic location before authorizing access.

A data breach occurs when information is read, modified or deleted without authorization.

Notification & escalation - Responses to a data breach must be configured so the appropriate personnel are notified immediately of the breach.

The first responders might be able to handle the incident if its a minor issue however in more serious cases, the case may need to be escalated to a more senior manager.

In certain cases, a timescale might also be applied. For example with gdpr, all affected individuals must be informed of the breach within 72 hours after the breach occurred.

Data sharing & privacy terms of agreement

- **Service level agreement (SLA) -** A contractual agreement setting out the detailed terms under which a service is provided.
- **Interconnection security agreement (ISA) -** ISAS set out a security risk awareness process and commits the agency and supplier to implementing security controls.
- **Nondisclosure agreement (NDA) -** This is a legal basis for protecting information assets.
- **Data sharing and use agreement -** Personal data can only be collected for a specific purpose but data sets can be subject to deidentification to remove personal data. However there are risks of re identification if combined with other data sources. A data sharing and use agreement is a legal means of preventing this risk. It can specify terms for the way a data set can be analyzed and proscribe the use of re identification techniques.

16.3 Privacy And Data Controls

Data can be described as being in one of three states:

- **Data at rest -** Data is in some sort of persistent storage media. This data can be encrypted and acls can also be applied to it
- **Data in transit -** This is the state when data is transmitted over a network. In this state it can be protected by a transport encryption protocol such as tls or ipsec.
- **Data in use/processing -** This is the state when data is present in volatile memory such as the ram cache. Trusted execution environment (tee) mechanisms e.G intel software guard extensions are able to encrypt the data as it exists in memory.

Data exfiltration - Data exfiltration can take place via a wide variety of mechanisms:

- Copying the data to removable media such as usb drive or smartphone
- Using a network protocol such as ftp, http or email
- Communicating it orally over a phone or even with the use of text messaging.

Data protection against exfiltration

- All sensitive data is encrypted at rest
- Create and maintain offsite backups of data
- Ensure that systems storing or transmitting sensitive data are implementing access controls.
- Restrict the types of network channels that attackers can use to transfer data from the network to the outside.
- Train users about document confidentiality and the use of encryption to store and transmit data securely.

Data loss prevention

Dlp products automate the discovery and classification of data types and enforce rules so that data is not viewed or transferred without proper authorization.

- **Policy server -** to configure classification, confidentiality and privacy rules and policies, log incidents and compile reports
- **Endpoint agents -** to enforce policy on client computers even when they are not connected to the network
- **Network agents -** to scan communications at network borders and interface with web and messaging servers to enforce policy.

Remediation is the action the dlp software takes when it detects a policy violation.

- Alert only
- **Block -** The user is prevented from copying the original file but retains access to it. User may not alerted to the policy violation but it will be logged as an incident by the management engine.
- **Quarantine** - Access to the original file is denied to the user.
- **Tombstone -** The original file is quarantined and replaced with one describing the policy violation and how the user can release it again.

Privacy enhancing technologies - data minimization is the principle that data should only be processed and stored if that is necessary to perform the purpose for which it is collected.

Data minimization affects the data retention policy and its necessary to track how long a data point has been stored for and whether continued retention is necessary for a legitimate processing function.

Pseudo-anonymization modifies identifying information so that reidentification depends on an alternate data source which must be kept separate. With access to the alternated data, pseudo-anonymization methods are reversible.

Database identification methods

Data masking - Can mean that all or part of the contents of a field are redacted by substituting all character strings with “x”.

Tokenization - Means that all or part of data in a field is replaced with a randomly generated token. The token is stored with the original value on a token server or vault separate to the production database. It’s often used as a substitute for encryption.

Aggregation/binding - Another identification technique is to generalize the data such as substituting a specific age with a broader age band.

Hashing & salting - A cryptographic hash produces a fixed-length string from arbitrary-length plaintext data using an algorithm such as sha. If the function is secure, it should not be possible to match the hash back to a plaintext. A salt is an additional value stored with the hashed data field. The purpose of salt is to frustrate attempts to crack the hashes.

16.4 Privacy Principles

Privacy - This is the right of an individual to control the use of their personal information.

Data minimization approach limits data collection to only what is required to fulfill a specific purpose.

Privacy Statement - This describes how an organization collects, uses, shares and protects personal information collected from individuals.

Right to be Forgotten - This pertains to an individual’s right to have their personal information removed or deleted from online platforms, search engine results or other publicly accessible sources.

It is not an absolute right and needs to be balanced against other rights such as freedom of expression, public interest or legal obligations.

Privacy Enhancing Technologies

- **Data Masking -** A technique used to protect sensitive data by replacing it with fictional or deidentified data
- **Tokenization -** A technique used to desensitize data by replacing the original data with an unrelated value of the same length and format.
- **Anonymization -** Is the process in which individually identifiable data is altered in a way it can no longer be traced back to the original owner
- **Pseudo-Anonymization -** Is a method to substitute identifiable data with a reversible consistent value

Privacy Management Components

- **Privacy Program -** Privacy statement, tools for data mapping, executive sponsorship and privacy impact assessment
- **Operations -** Cookie compliance, privacy enhancing technologies, reporting and assessment and consent mechanisms
- **Incident and Breach Response -** Incident prevention, detection, management, notification triggers and reporting obligations.

16.5 Compliance Monitoring

Compliance - This means acting in accordance with applicable rules, laws, policies and obligations.

Organizations are responsible for complying with all local, state, federal and union laws and regulations, international treaties as well as contractual obligations.

Jurisdiction - This is the power or right of a legal or political body to exercise their authority over a person, subject or territory.

Consequences of Non-Compliance

- Fines & Sanctions
- Loss of License
- Reputational Damage
- Contractual Impact
- Resource Utilization

Compliance Monitoring - This is the active process of evaluating activities and behaviors to verify compliance and identify any deviations or non-compliant actions.

Monitoring activities include:

- Manual Inspections
- Audits
- Data Analysis
- Automated Systems
- Specialized Tools

Automated Compliance Monitoring - This utilizes automated tools to monitor and assess compliance.

Automated systems can analyze large volumes of data in real time to identify compliance breaches and also generate alerts when specific conditions or thresholds are met.

16.6 Education, Training & Awareness

Security	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Object	Understanding	Skill	Behavior
Method	Discussion, Seminar, Reading	Lecture, case study, hands-on	Interactive vedio, posters, games
Measure	Essay	Problem solving	True/false,multiple choice
Impact	Long-term	Intermediate	Shorts-terms

16.7 Personnel Policies

- Acceptable use policy (aup)
- Code of conduct and social media analysis
- Use of personally owned devices in the workplace
- Clean desk policy

User and role-based training - Appropriate security awareness training needs to be delivered to employees at all levels including end users, technical staff and executives.

- Overview of the organization's security policies
- Data handling
- Password & account management
- Awareness of social engineering and phishing

Diversity of training techniques - Using a diversity of training techniques helps to improve engagement and retention.

- Phishing campaigns
- Capture the flag - Usually used in ethical hacker training programs and gamified competitions.
- Computer-based training and gamification