Cyber Security Foundations | CySec

Summary

CONTENTS

1. INFORMATION SECURITY

Term	*Definition*
Information	An organization's data that has been processed, organized, or structured in a way that gives it meaning and value to an organization or individual.
Information security	Protection of the integrity, confidentiality and availability of information data whether in storage, transit or processing.
non-repudiation	prevents parties from denying actions they have performed.
accountability	ability to trace actions and decisions back to a specific person or system.
authentication	verifies the identity of a user or system.
authorization	determines what actions an authenticated entity is allowed to perform.
access control	restricts access to resources based on defined rules.
business continuity	ensures critical operations continue during disruptions.
security policy	a rule or expectation for protecting information.
compliance	adherence to laws, regulations, and (security-)standards.
asset	any item of value belonging to an organization – For example: information, systems, people and processes
attack	an act that intends to damage, steal or degrade an organizations assets
vulnerability	a flaw or weakness in a system that can be abused
exploit	a technique or method used to take advantage of a vulnerability
threat	an event or action with the potential to cause harm by exploiting a vulnerability
risk	the likelihood of a threat exploiting a vulnerability and the potential harm that could cause
control	a measure designed to reduce the potential risk of an attack – Can be achieved through training employees, enforcing policies or implementing technology

TODO:
CySec / IT-Sec / Info-Sec visualization

1.1. TYPES OF INFORMATION

- Personal information
- Business information
- Financial information
- Intellectual property
  - Copyright
  - Trademarks
  - Patents
  - Trade secrets
- System information

1.2. HOW CAN INFORMATION BE ATTACKED

TODO:
Vulnerabilities diagram

– In storage
– In transit
– In use

1.3. COMPONENTS OF AN INFORMATION SYSTEM (IS)

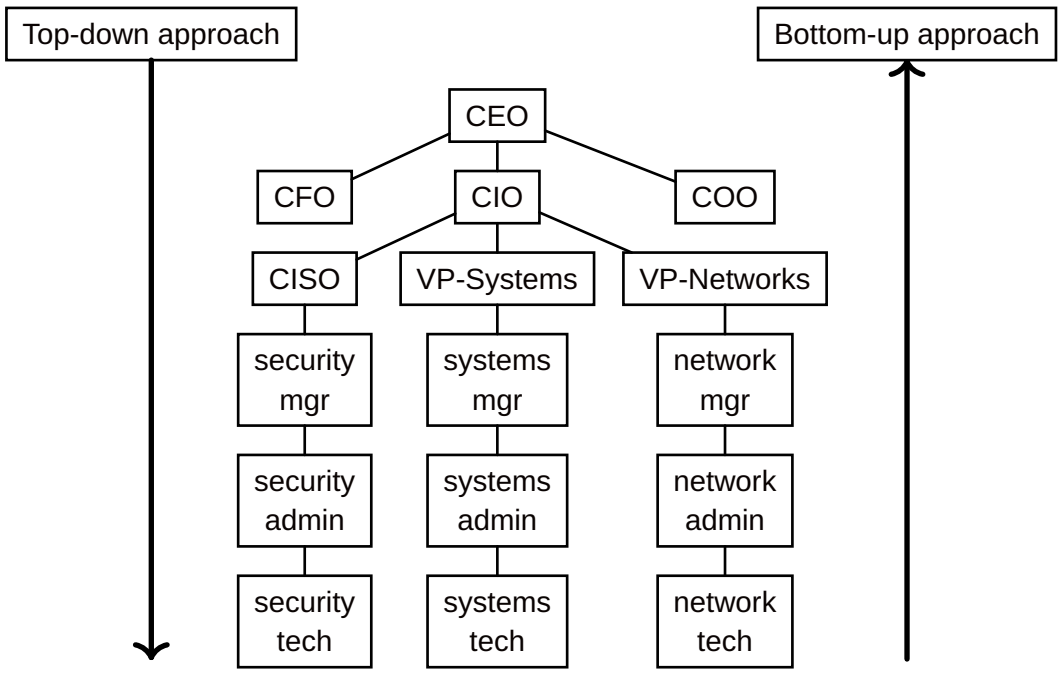
– Software
– Hardware
– Data
– People
– Procedures
– Networks

1.4. BALANCING SECURITY AND SYSTEM USABILITY

– Obtaining perfect information security is impossible.
– Security needs to protect the system without slowing people down.
– Too much security can lead to workarounds.
  – Example: If strong passwords are enforced, people might start writing them down on sticky notes.
– Too much convenience exposes the system to unnecessary risks.
– It's all about finding that sweet spot between security and usability.
  – Example Solution: Employees must use multi-factor authentication. This way, they are free to use a less secure password without compromising the overall security.
– An even better, continuously review policies and involve users to find the best solution.

1.5. IMPLEMENTATION OF INFORMATION SECURITY

TODO:
pyramid diagram



Bottom-Up | ***Top-Down***

– Initiated by an organization's technical staff (system engineers, admins, etc.). – Implementations happen before policies are defined. – Often lacks support from management, budget and consistency. – Generally less effective and not scalable in large organizations.	– Initiated and supported by an organization's upper management. – Policies come first and provide guidance for implementations. – Ensures proper funding, authority and organization-wide enforcement. – Generally more effective and in-line with the business strategy

1.6. CIA TRIAD

The CIA triad is a foundational information-security model stating that systems should protect:

– **Confidentiality** - Keeping information secret
– **Integrity** - Keeping information correct and unaltered
– **Availability** - Ensuring information and systems remain accessible

	Confidentiality	***Integrity***	***Availability***
Goal	Prevent or minimize unauthorized access to information	Protecting the reliability and correctness of information.	Ensuring that subjects have timely and uninterrupted access to information.
Steps to ensure it	– Encryption – Access Control – Allow / enforce advanced authentication mechanisms	– Digital Signatures – Hashing and Checksums – Change Management	– Redundance and Backups – DDoS Protection – Incident Response

1.7. NON-REPUDIATION AND ACCOUNTABILITY

Example of security controls through which non-repudiation can be established: Digital certificates, session identifiers, transaction logs, etc.

1.7.1. Non-Repudiation

– Ensures that the subject of an activity or who caused an event cannot deny having performed an action or cannot deny that the event occurred.
– Non-Repudiation prevents a subject from claiming not to have sent a message, not to have performed an action, or not to have been the cause of an event.

1.7.2. Accountability

– Being responsible or obligated for actions and results.
– Non-Repudiation is an essential part of accountability. A suspect cannot be held accountable if they can repudiate the claim against them.

1.8. STRIDE MODEL

A structured model developed by Microsoft used in cybersecurity to identify and categorize threats to systems by looking at how they can be attacked.

TODO:
Authenticity

Term	***Definition***
S(poofing)	Pretending to be someone else. (see Authenticity)
T(ampering)	Unauthorized data modification or altering. (see Integrity)

Term	Definition
R(epudiation)	Denying actions without proof. (see Non-Repudiation)
I(nformation disclosure)	Exposing sensitive information. (see Confidentiality)
D(enial of service)	Making systems or services unavailable. (see Availability)
E(levation of privilege)	Gaining unauthorized rights or privileges. (see Authorization)

1.9. MCCUMBER CUBE

> ***TODO:***
> Cube visualization

Y-Axis: Security Goals (C.I.A. Triad)
– Defines what needs to be protected.

X-Axis: Information States
– Describes where the information exists.

Z-Axis: Safeguards / Controls
– Defines how protection is implemented.

2. THREAT CATEGORIZATION

Term	Definition
Social Engineering	Manipulating people to reveal confidential information.
Software Attacks	Exploiting vulnerabilities in software to gain access to a system or steal data.
Denial of Service	Overloading one or multiple systems to make it unavailable.
Web Application Attacks	Exploiting vulnerabilities in websites or servers hosting websites.
Password / Authentication Attacks	Attempting to bypass or compromise login systems to gain unauthorized access.
Physical Attacks	Bypassing technical controls by accessing physical infrastructure directly.

2.1. SOCIAL ENGINEERING

The psychological manipulation of individuals to trick them into revealing confidential information or performing actions that can compromise security.

Term	Definition
Phishing	Forged emails impersonating legitimate entities.
Spear Phishing	Targeted phishing against specific individuals.
Vishing	Voice-based phishing over phone or video calls.
Smishing	SMS / Text-based phishing.

2.2. SOFTWARE ATTACKS

Attacks involving malicious code or malware designed to damage systems, steal sensitive data, or gain unauthorized access to systems or services.

Term	Definition
Virus	Malware that attaches to programs and spreads.

Term	*Definition*
Worms	Self-replicating malware that spreads over a network.
Trojan Horse	Malicious software disguised as legitimate applications.
Ransomware	Malware that encrypts victim's data and demands payment to restore access.
Rootkits	Stealthy tools that hide malicious activity and maintain privileged access.

2.3. DENIAL OF SERVICE

Attacks aims at making a system or service unavailable by overwhelming it with excessive traffic or requests.

Term	*Definition*
DoS	Single source denial of service attacks.
DDoS	Denial-of-service attacks performed by multiple attackers or attacking devices.
Botnet	A network of compromised computers and other devices controlled by an attacker and used to together to flood a target with excessive traffic.
SYN-Flood Attack	Sending many connection requests without completing them.
Reflection Attack	Attacker sends requests to a service and spoofs the victim's IP making the service send (many) replies to the victim instead of back to the attacker.

2.4. WEB APPLICATION ATTACKS

Exploits vulnerabilities in web applications to steal data, manipulate content, or gain unauthorized access.

Term	*Definition*
SQL Injection	An attacker inserts malicious SQL commands into an input to manipulate a database and access, modify, or delete data.
Cross-Site Scripting (XSS)	An attacker injects malicious scripts into a website that execute in other users' browsers to steal sensitive data.
Cross-Site Request Forgery (CSRF)	An attacker tricks a logged-in user's browser into sending unauthorized requests to a web application on their behalf.
Broken Authentication	Weak authentication mechanisms allow attackers to compromise passwords, sessions, or identities to gain unauthorized access.

2.5. PASSWORD / AUTHENTICATION ATTACKS

Attacks that attempt to bypass or compromise login systems to gain unauthorized access to a system or service.

Term	*Definition*
Rainbow Table Attacks	Attackers using precomputed hash lookup tables to reverse weakly hashed passwords back into plaintext.
Password Spraying	Attackers trying a few common password like "password" across many accounts to avoid lockouts or timeouts.
Credential Stuffing	Attackers using leaked usernames and passwords from previous breaches to attempt logins on other services.
Brute Force Attack	Attackers repeatedly try many username and password combinations until they successfully gain access to an account.

2.6. PHYSICAL THREATS

Threats or attacks that affect the physical infrastructure supporting information systems, usually bypassing technical controls overall.

Term	*Definition*
Theft of devices	Attackers physically steal hardware to gain direct access to stored data, credential, internal systems, or other sensitive data.
Hardware tampering	An attacker modifies or implants malicious components in physical equipment to intercept data, bypass security, or disrupt operations.
Power disruption	Attackers interrupt or manipulate power supply to shut down or destabilize critical systems or services impacting availability and business continuity.
Environmental damage	Natural or deliberate environmental events that damage infrastructure, causing data loss, downtime, or destruction of critical systems (e.g., earthquake, fire).