1

FOUNDATIONAL CONCEPT IN
Computer Security

Introduction

What is Security in general?

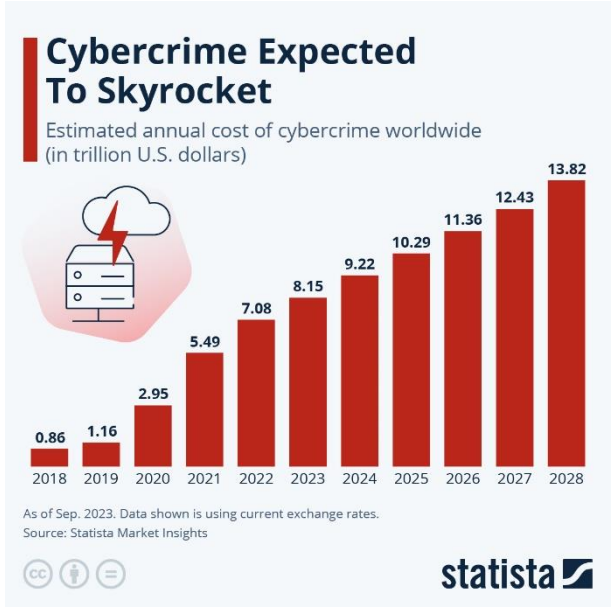
- Security is about protecting assets from damage or harm
  - Focuses on all types of assets
    - Example: your body, possessions, the environment, the nation

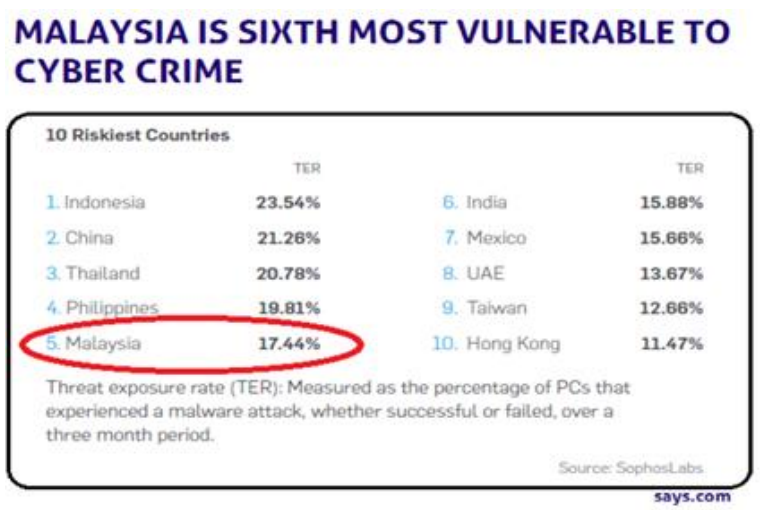
- Examples of Security-related concepts
  - National security (political stability)
  - Safety (health)
  - Environmental security (clean environment)
  - Information security
  - Computer Security
  - Computing Security

Why study SECURITY?

1 Increasing XSecurity Cases

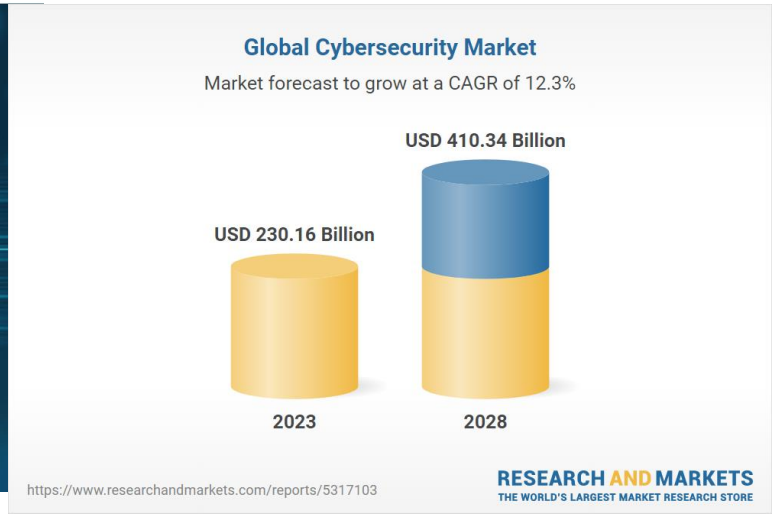
In 2020, a Twitter breach targeted 130 accounts, including those of past presidents and Elon Musk, resulted in attackers swindling $121,000 in Bitcoin through nearly 300 transactions.





Why study SECURITY?

2 Increasing XSecurity Job Demands



The Malaysia ICT Market size is estimated at USD 27.20 billion in 2024, and is expected to reach USD 39.18 billion by 2029, growing at a CAGR of 7.57% during the forecast period (2024-2029).

Source: https://www.mordorintelligence.com/industry-reports/malaysia-ict-market

Malaysia need 25,000 cybersecurity personnel by 2025."

Source: https://www.malaymail.com/news/malaysia/2023/11/24/pm-anwar-malaysia-needs-25000-workers-in-cyber-security-by-2025/103994

"As digital transformation agendas continue to dominate, a bigger cybersecurity budget is necessary. Almost all companies are looking at technologies such as robotics, machine learning, artificial intelligence, blockchain and so on. All of that change will come with additional cyber risks and necessary investments."

- Mike Maddison,
- EY EMEIA
- Cybersecurity Leader

Why Security is Needed?

More reliance on Cyber Technologies and devices

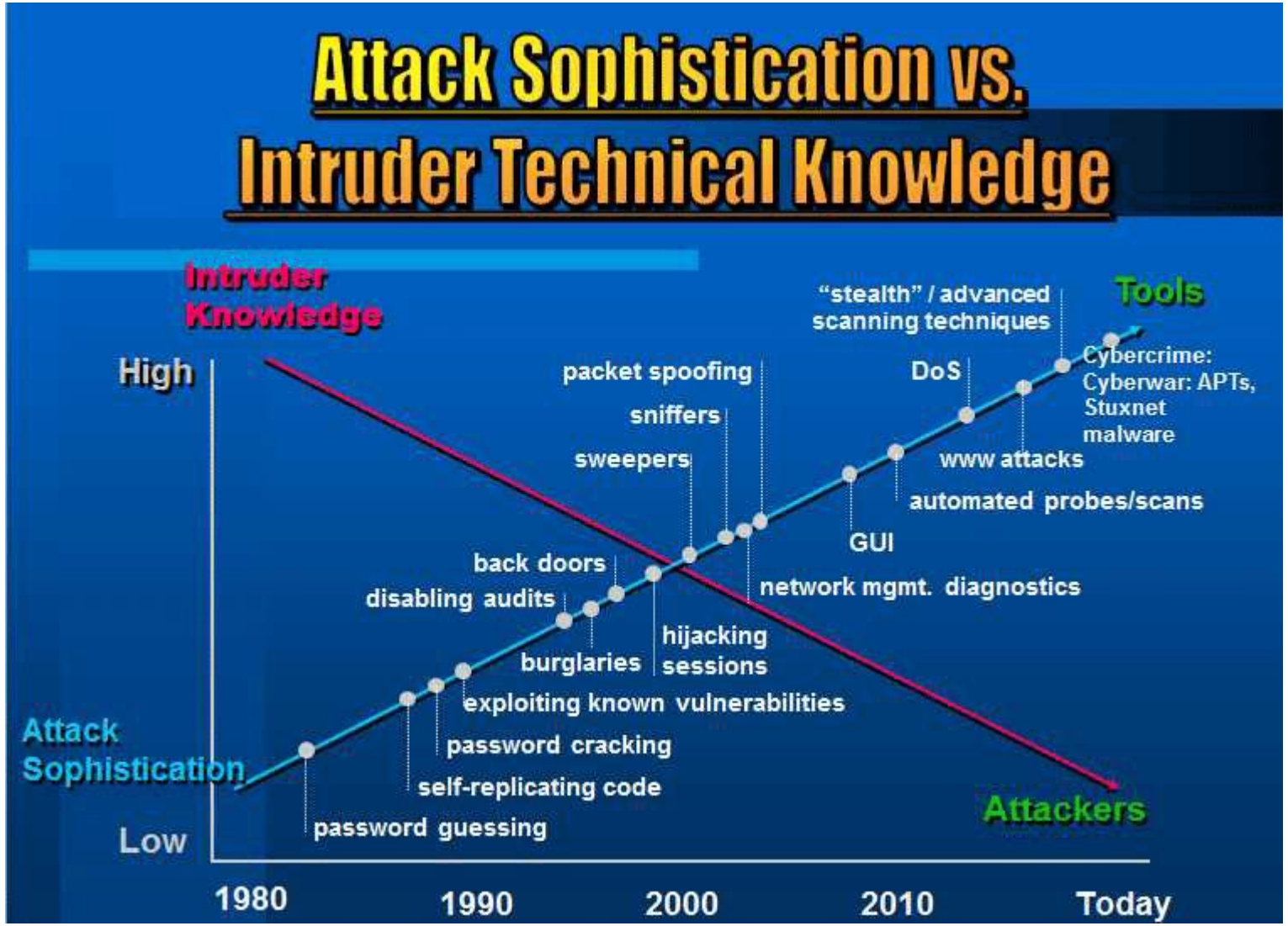
Rising costs of breaches

More sophisticated cyberattacks

Increase of hacking tools

Proliferation of Internet of Things (IoT) devices

Why Security is Needed?



Ref: https://www.researchgate.net/figure/Attack-sophistication-vs-intruder-technical-knowledge_fig2_326786055

UNIVERSITI TEKNOLOGI PETRONAS

01 Foundational Concept

Objectives

01 ▪ To understand the definition of computer security

02 ▪ To know the Security Services (CIA Triad)

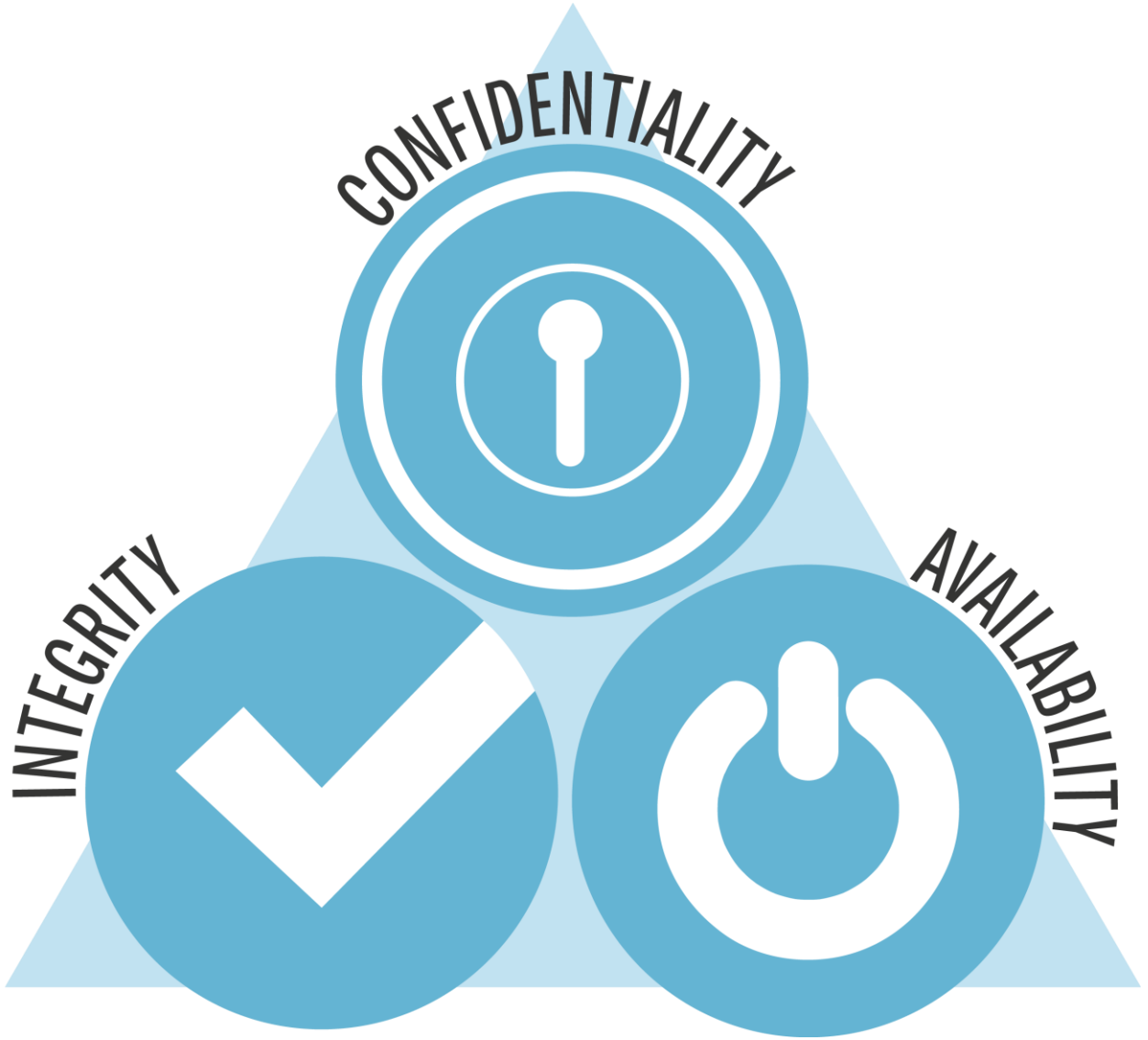
03 To know the security terminology and taxonomy

04 To know the assets to be protected for a computer system

DEFINITION OF COMPUTER SECURITY

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)
- *National Institute of Standards and Technology (NIST) 1995*

Security Services (CIA Triad)



Security Services (CIA Triad)

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. That is, information must be trustable.

Availability

- Ensuring timely and reliable access to and use of information. Available anytime anywhere.

Security Services (CIA Triad)

- **Confidentiality**
  - Data confidentiality: Assures that confidential information is not disclosed to unauthorized individuals
  - Privacy: Assures that individual control or influence what information may be collected and stored

- **Integrity**
  - Data integrity: assures that information and programs are changed only in a specified and authorized manner
  - System integrity: Assures that a system performs its operations in unimpaired manner

- **Availability**
  - Assure that systems works promptly and service is not denied to authorized users

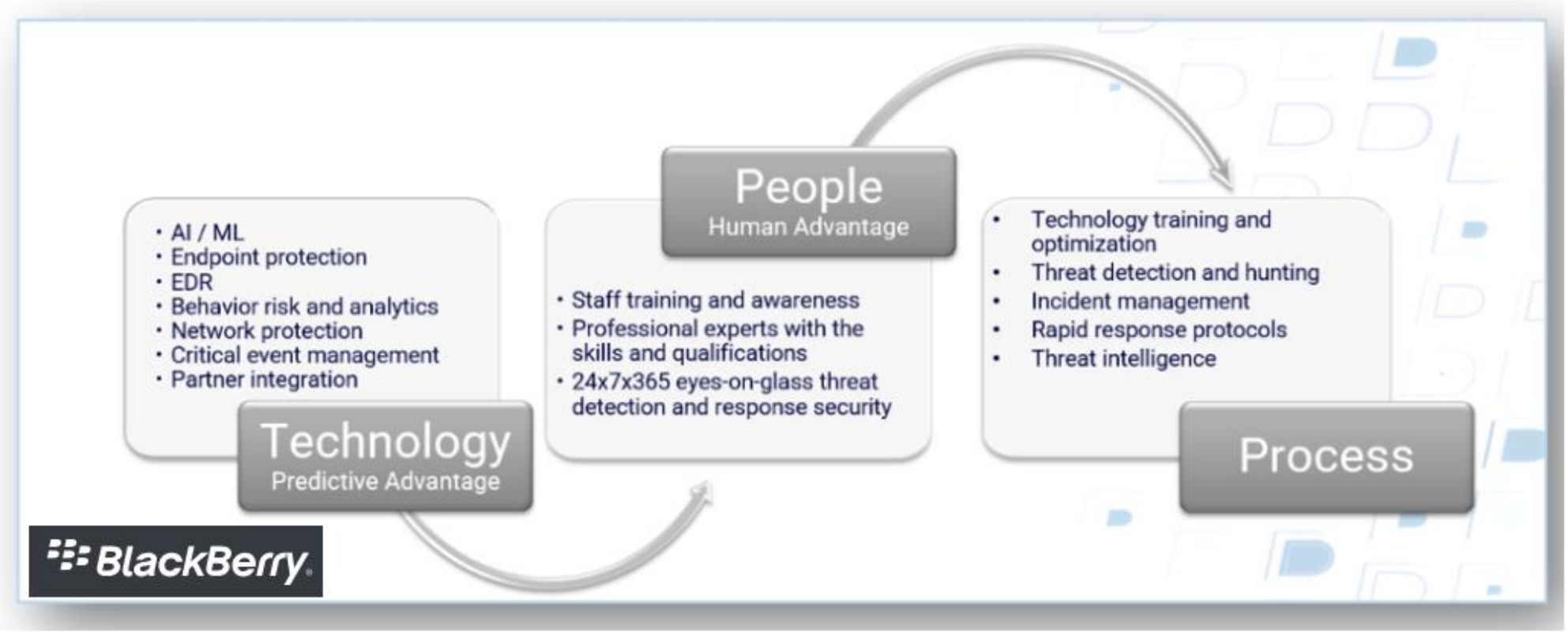
Other Security Services / Requirements

- **Authentication**
  - Security service "designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorizations to receive specific categories of information"

- **Non-repudiation**
  - "The assurance the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data"

Information security pillars

- The 3 Pillars of Information Security: People, Process, and Technology



Security Terminology

Adversary

An entity that attacks or is a threat to a system

Attack

is an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Threat

is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger enabling the exploitation of a vulnerability.

Vulnerability

is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network

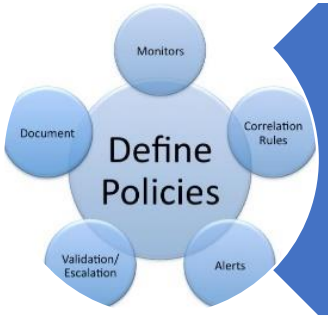
Security Terminology

Risk

is the potential for loss, damage or destruction of assets or data caused by a cyber threat

Countermeasure

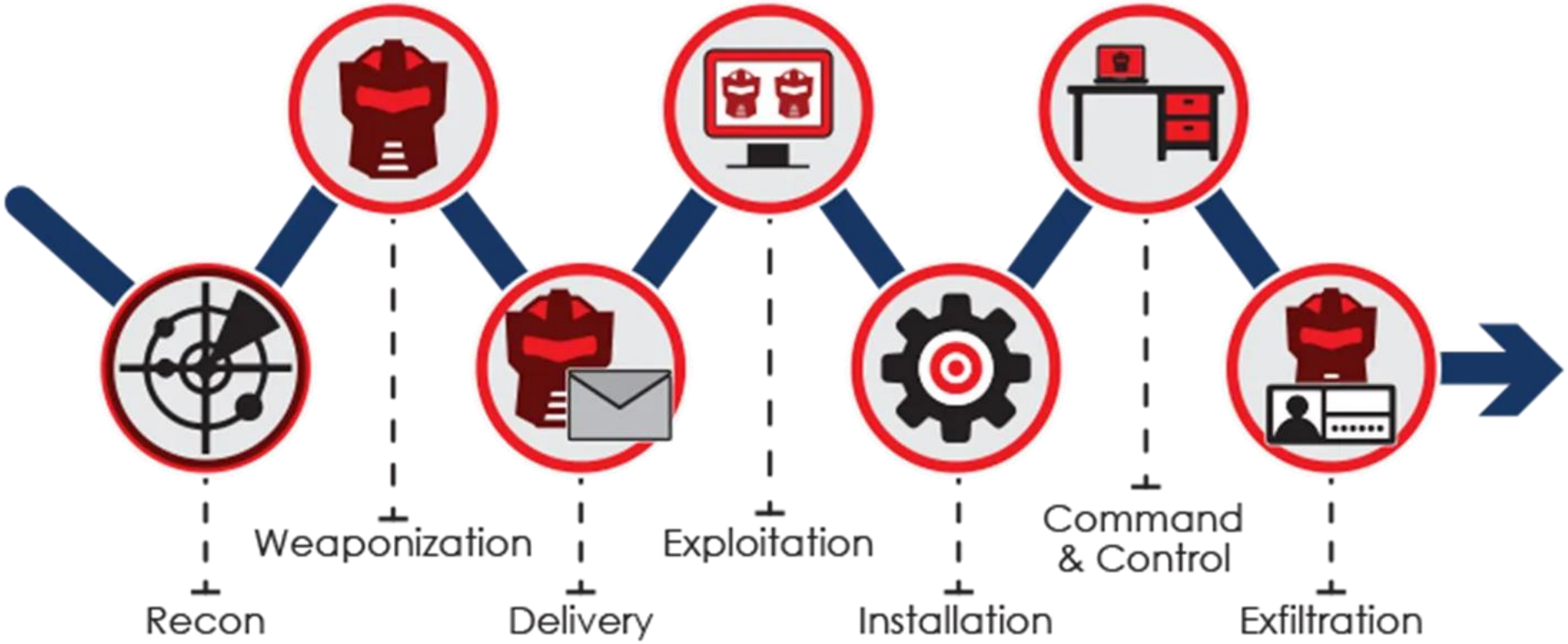
is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.



Security Policy

is a set of rules and policy that specify how an organization or a security system provides the security services to protect sensitive and critical system resources

Cyber Kill Chain



Security concepts and relationships

Security taxonomy

- Action: A step taken by a user or process in order to achieve a result
- Target: A computer or network logical entity or physical entity
- Event: An action directed at a target that is intended to result in a change of state, or status, of the target
- Tool: A means of exploiting a computer or network vulnerability
- Vulnerability: A flaw or weakness in a system that can be exploited by an attacker
- Unauthorized result: An unauthorized consequence of an event
- Attack: A series of steps taken by an attacker to achieve an unauthorized result
- Attacker: An individual who attempts one or more attacks in order to achieve an objective
- Objectives: The purpose or end goal of an incident

Security taxonomy

- Incident: An event that actually compromises the integrity, confidentiality, or availability of an information asset.
- Advanced Persistent Threat (APT): A prolonged and targeted cyberattack in which an intruder gains access to a network and remains undetected for an extended period.
- Tactics, Techniques, and Procedures (TTP): The behavior and methods used by cyber attackers, detailing how specific attacks are carried out.
- Indicators of Compromise (IOC): Artifacts observed on a network or in an operating system that with high confidence indicate a computer intrusion.
- Root Cause Analysis (RCA): The process of discovering the underlying causes of a security incident or problem to prevent future occurrences.
- Zero Day Vulnerability: A flaw in software that is exploited by attackers before it is known to the developer, or before the developer has had a chance to fix it.
- Zero Trust: Zero trust is a security model that operates on the principle of "never trust, always verify." It requires strict identity verification and context assessment before granting access to resources, regardless of a user's or device's network location.

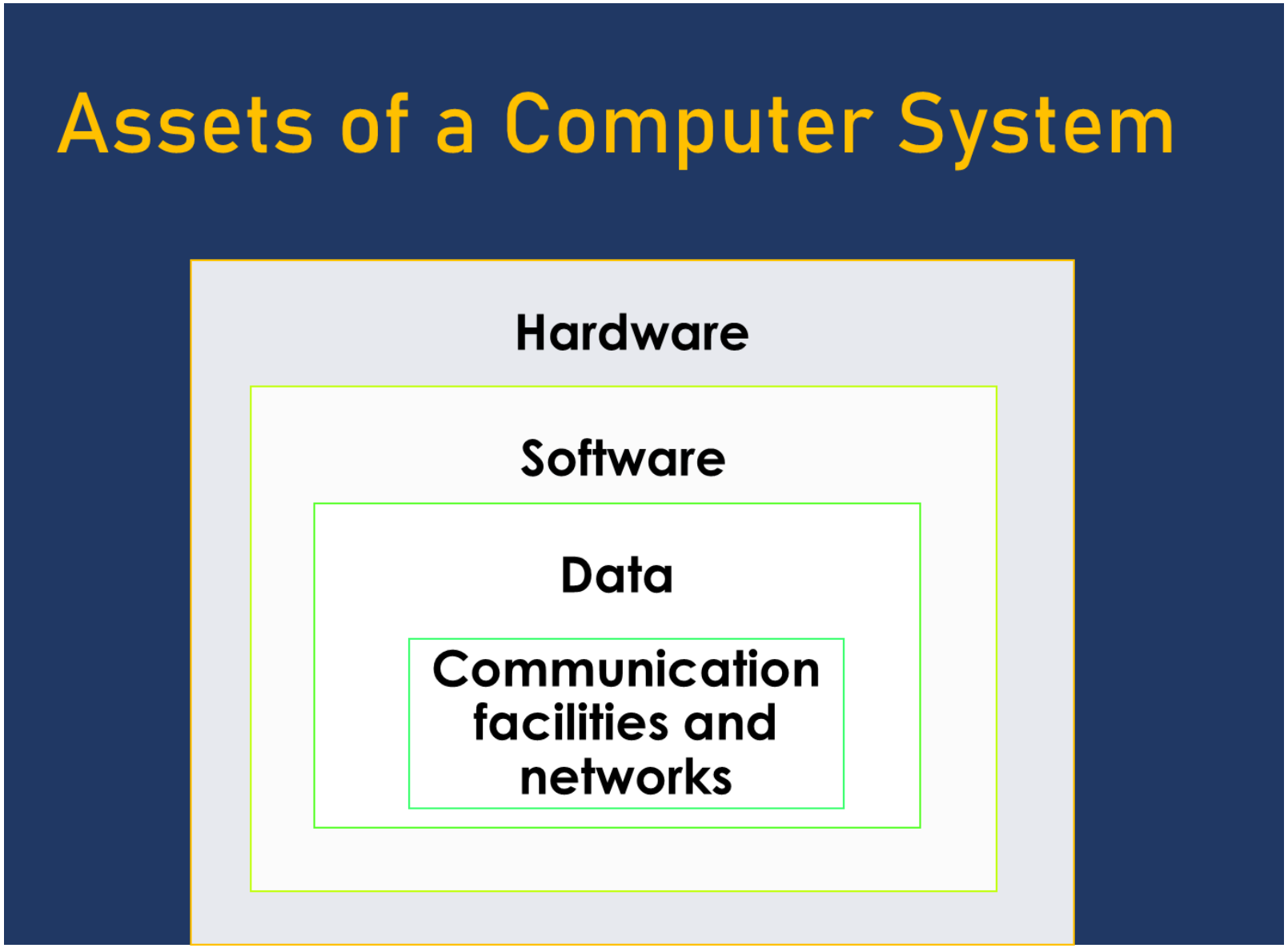
Security taxonomy

Code obfuscation: Code obfuscation is the process of modifying software code to make it difficult to understand and reverse engineer. It involves altering the code's structure, formatting, and data without changing its functionality, aiming to protect intellectual property and increase security against unauthorized access and modification. It is commonly used in both web and mobile applications. Code obfuscation can add complexity, increasing the codebase size.

Endpoint Detection and Response (EDR): EDR systems are vital in modern cybersecurity, focusing on continuous monitoring, detection, and response to threats at endpoint levels. EDR systems track and store endpoint activities to identify suspicious behaviors through various detection methods like signature-based, behavioral, and anomaly detection. Upon identifying potential threats, EDR solutions alert security teams and provide robust response capabilities, including isolating endpoints and terminating malicious processes.

Security Terminology

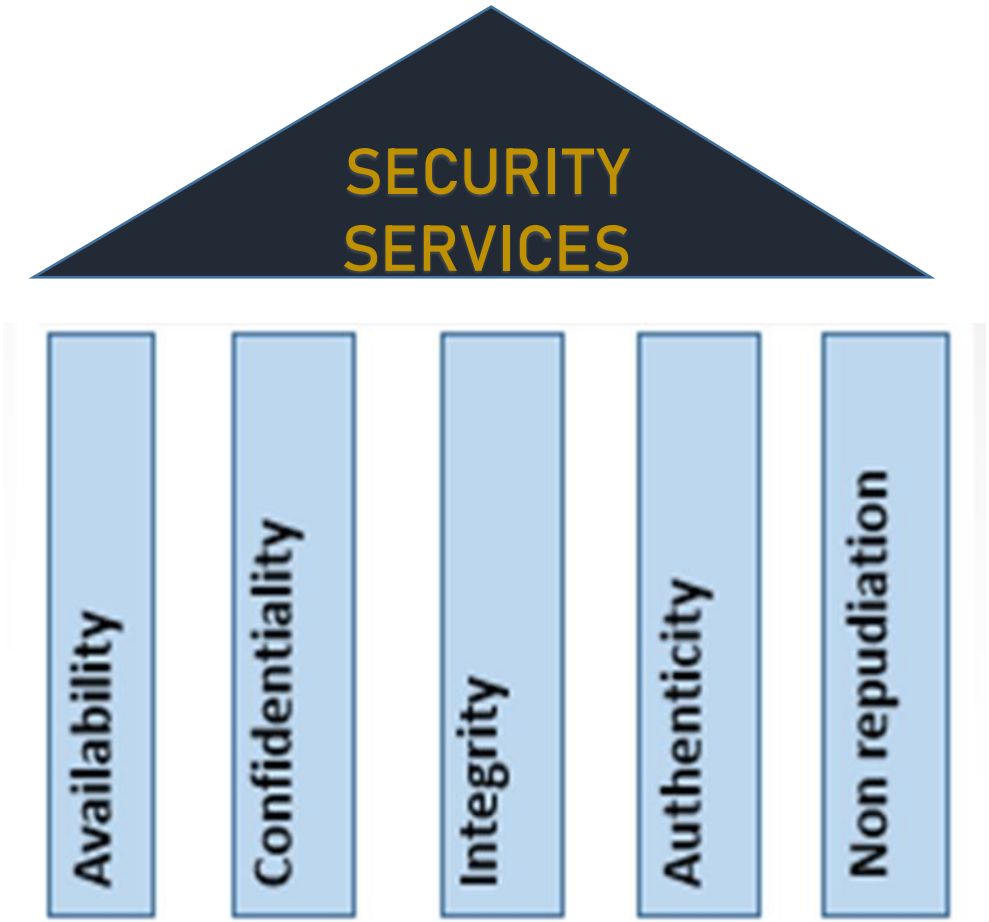
Assets of a Computer System

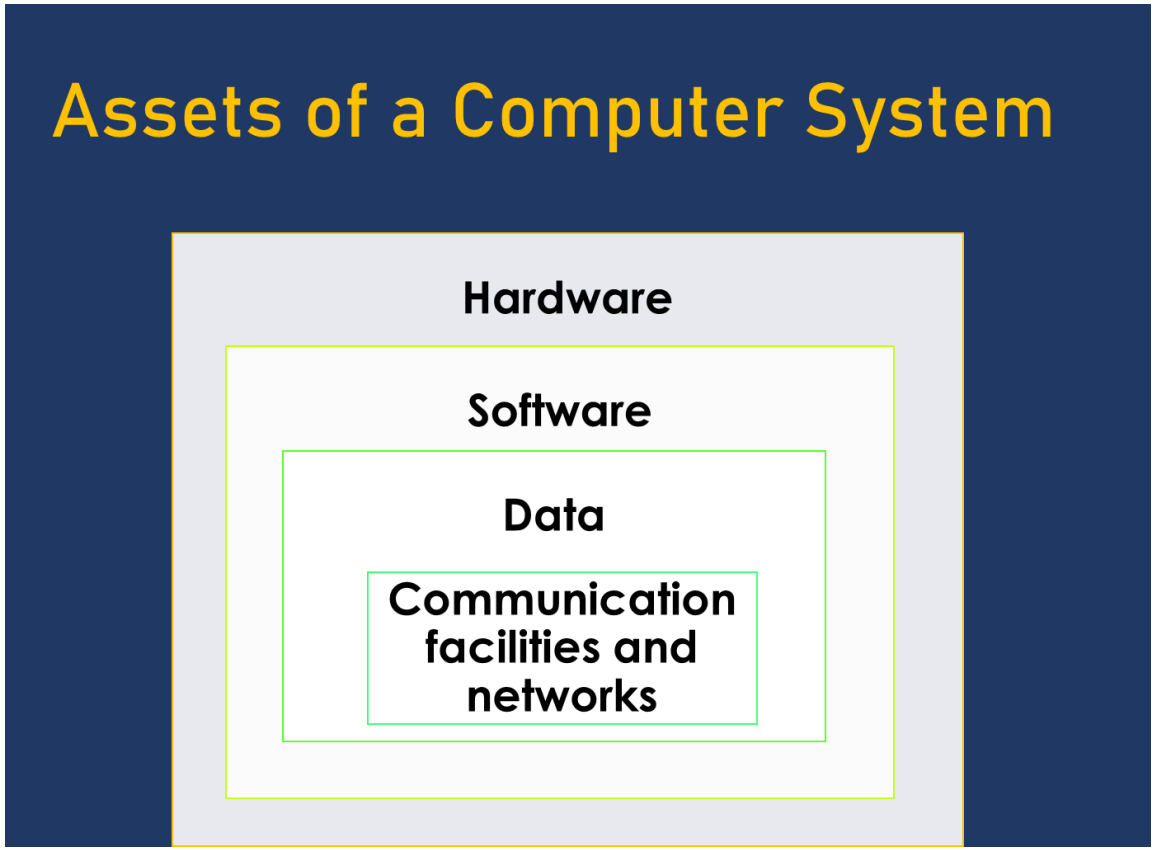


Examples of CIA Triad, Assets and Threats

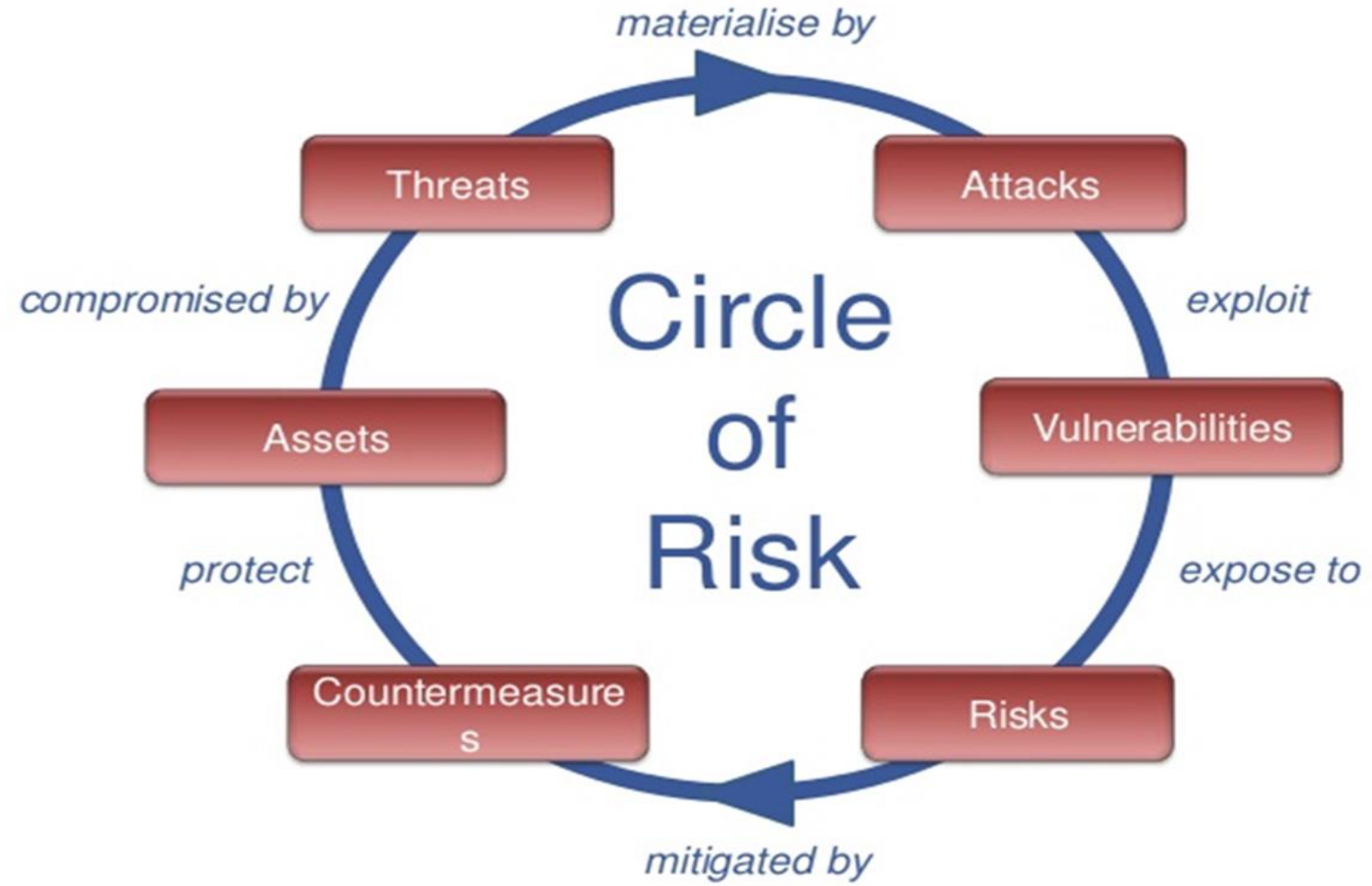
	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Summary


SECURITY SERVICES
Availability
Confidentiality
Integrity
Authenticity
Non repudiation


Assets of a Computer System
Hardware
Software
Data
Communication facilities and networks

Summary


materialise by
Threats
Attacks
compromised by
exploit
Circle of Risk
Assets
Vulnerabilities
protect
expose to
Countermeasures
Risks
mitigated by

THANK YOU

Assignment – About You

- **Tasks**

1. Individual-based assignment
2. Prepare a ONE (1) page pdf
3. Submit via ULEARN

- **Contents**
  1. Your picture
  2. Your biodata
  3. Your expectations towards this course
  4. Any other interesting facts about you!

- **Submission**
  - Due : Monday 09/09/2024
  - Via : ULearn (TFB2043:Information Assurance and Security - September 2024: ASSIGNMENT - ABOUT YOU | ULearn (utp.edu.my))

- **Formatting**
  - UP to your creativity