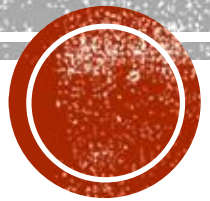
Lecture 2: Cyber Security Foundations and Principles



- Elements
- CIA triad
- AAA elements

WHAT IS CYBERSECURITY ALL ABOUT?

In order to achieve security we need to combine 3 key elements (CYS pillars):

- People
- Policies
- Technologies
- **People** - Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.
- **Policies** - Organizations must have a framework for how they deal with both attempted and successful cyber attacks.
- **Technology** - Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber attacks.

WHAT IS CYBERSECURITY ALL ABOUT?

THREE MAIN ENTITIES MUST BE PROTECTED:

- endpoint devices like: computers, smart devices, and routers;
- networks; and
- the cloud and data centers

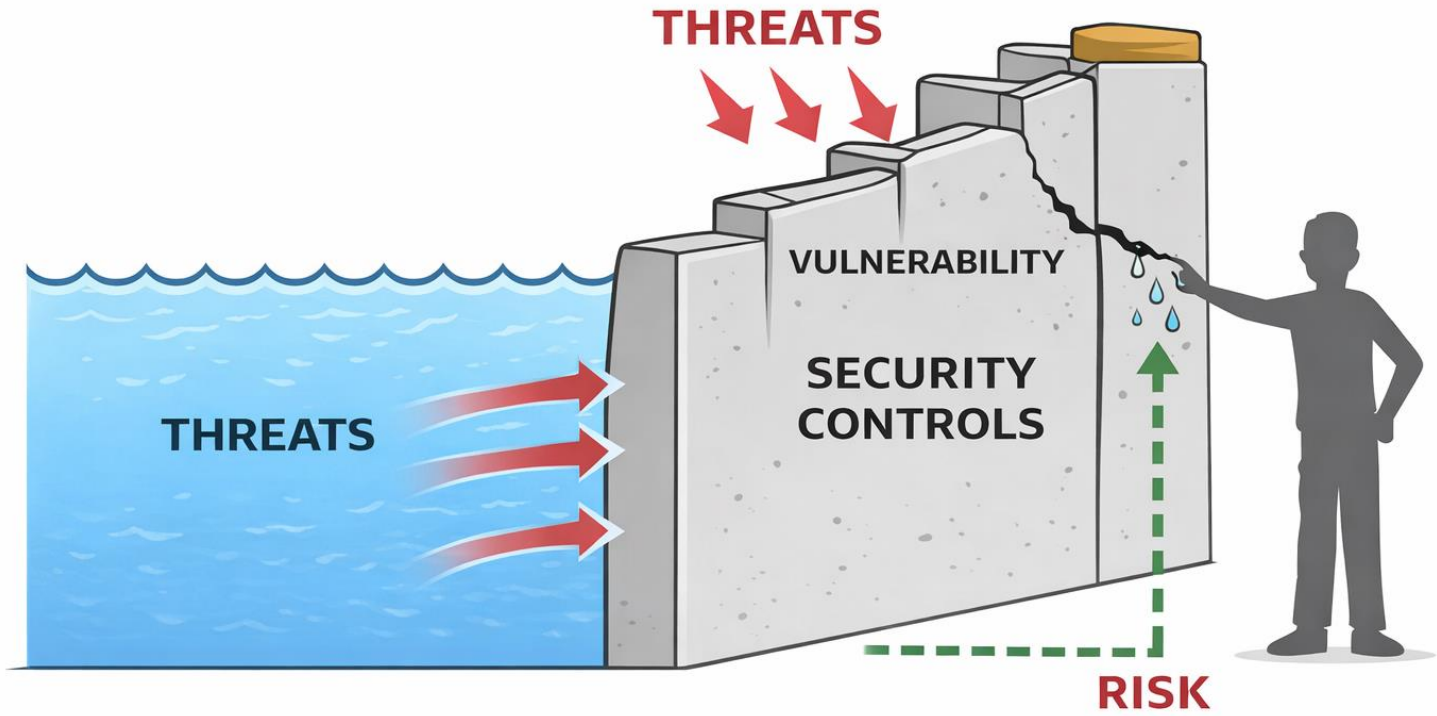
COMMON TECHNOLOGY USED TO PROTECT THESE ENTITIES

- next-generation firewalls,
- DNS filtering,
- malware protection,
- antivirus software, and
- email security solutions.

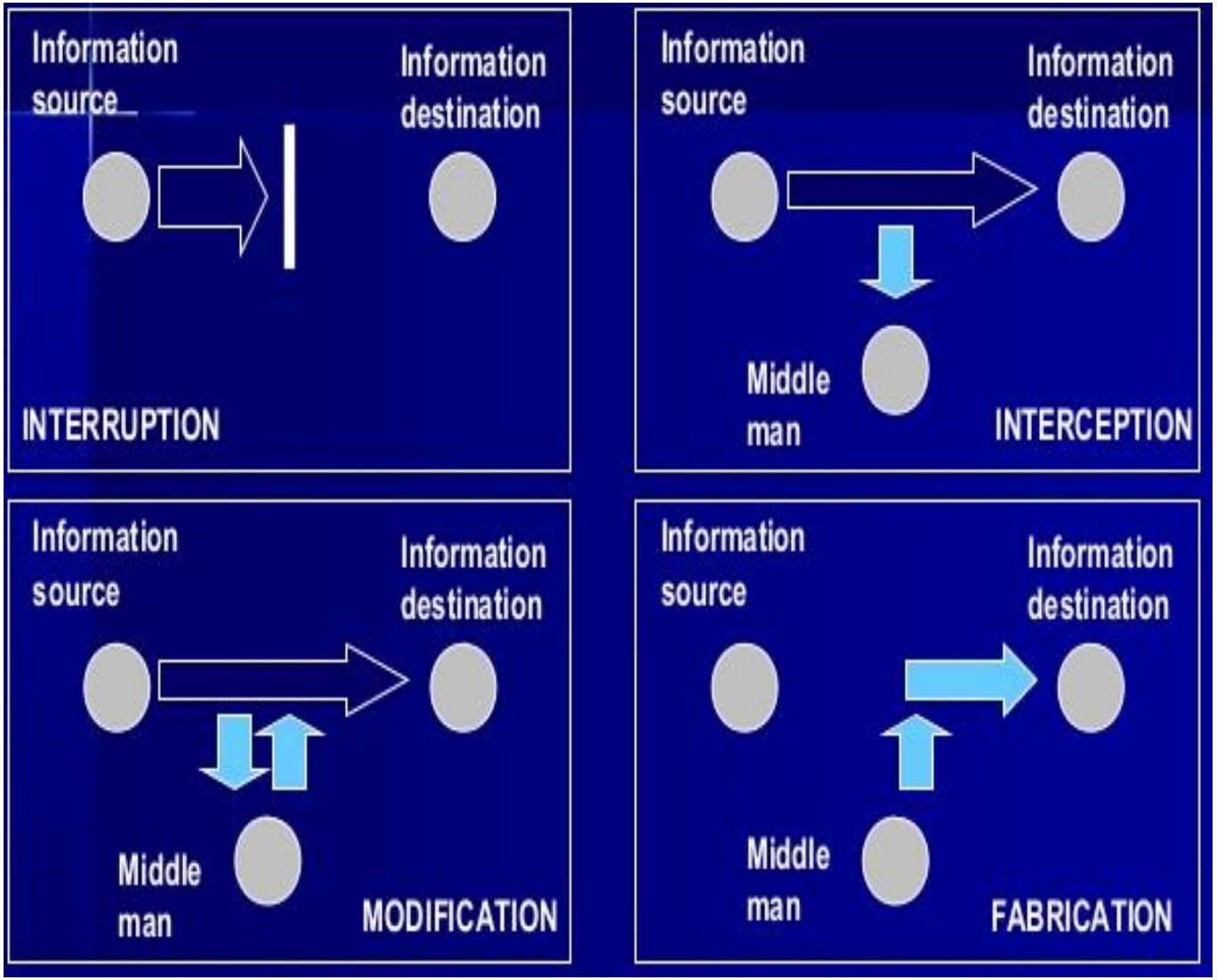
VULNERABILITY, THREAT, COUNTERMEASURE

- **Vulnerability** is a weakness in the security system
  - (i.e., in procedures, design, or implementation), that might be exploited to cause loss or harm.
- **Threat** - is a set of circumstances that has the *potential to cause loss or harm*.
  - a potential violation of security
- **Exploit?**
- A human (criminal) who exploits a vulnerability commits an **attack** on the system.
- How do we address these problems?
  - We use a **control** as a protective measure.
  - That is, a control is an action, device, procedure, or technique that removes or reduces a vulnerability.

Risk is exist when you have a threats with a vulnerabilty in the system or in one of the security control.



THREAT DAMAGE



Threat Damage Types
in Information Security

Interruption

Service stopped

● **Availability**

Examples:

- DoS / DDoS attack
- Server crash
- Network outage

Interception

Data observed

● Confidentiality

Examples:

- Eavesdropping
- Network outage

Modification

Data altered

● **Integrity**

Examples:

- Tampered database records
- Altered transactions
- Website defacement

Fabrication

Fake data sent

● **Integrity + Authenticity**

Examples:

- Spoofed emails
- Fake log entries
- Replay attacks

✓ Interruption → Availability | **Interception** → Confidentiality
Modification & Fabrication → Integrity

Threat Damage in a Communication System

Interruption

Service stopped

● **Availability**

Examples:

- DoS / DDoS attack
- Server crash
- Network outage

Interception

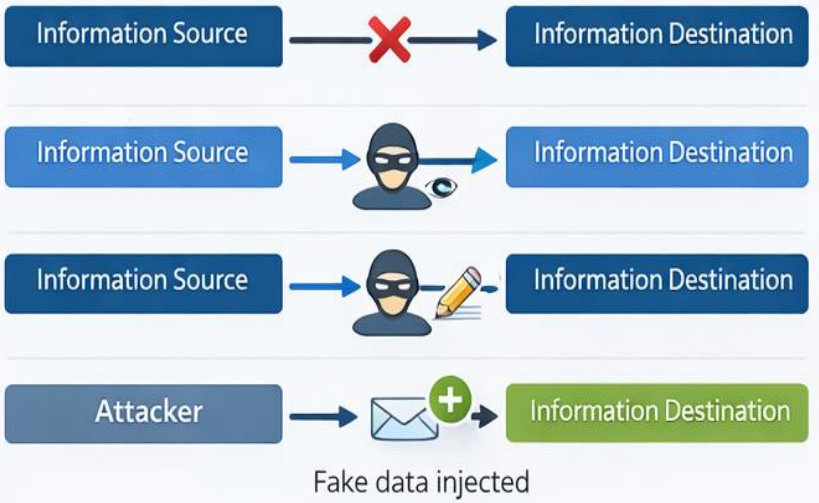
Data observed

● **Confidentiality**

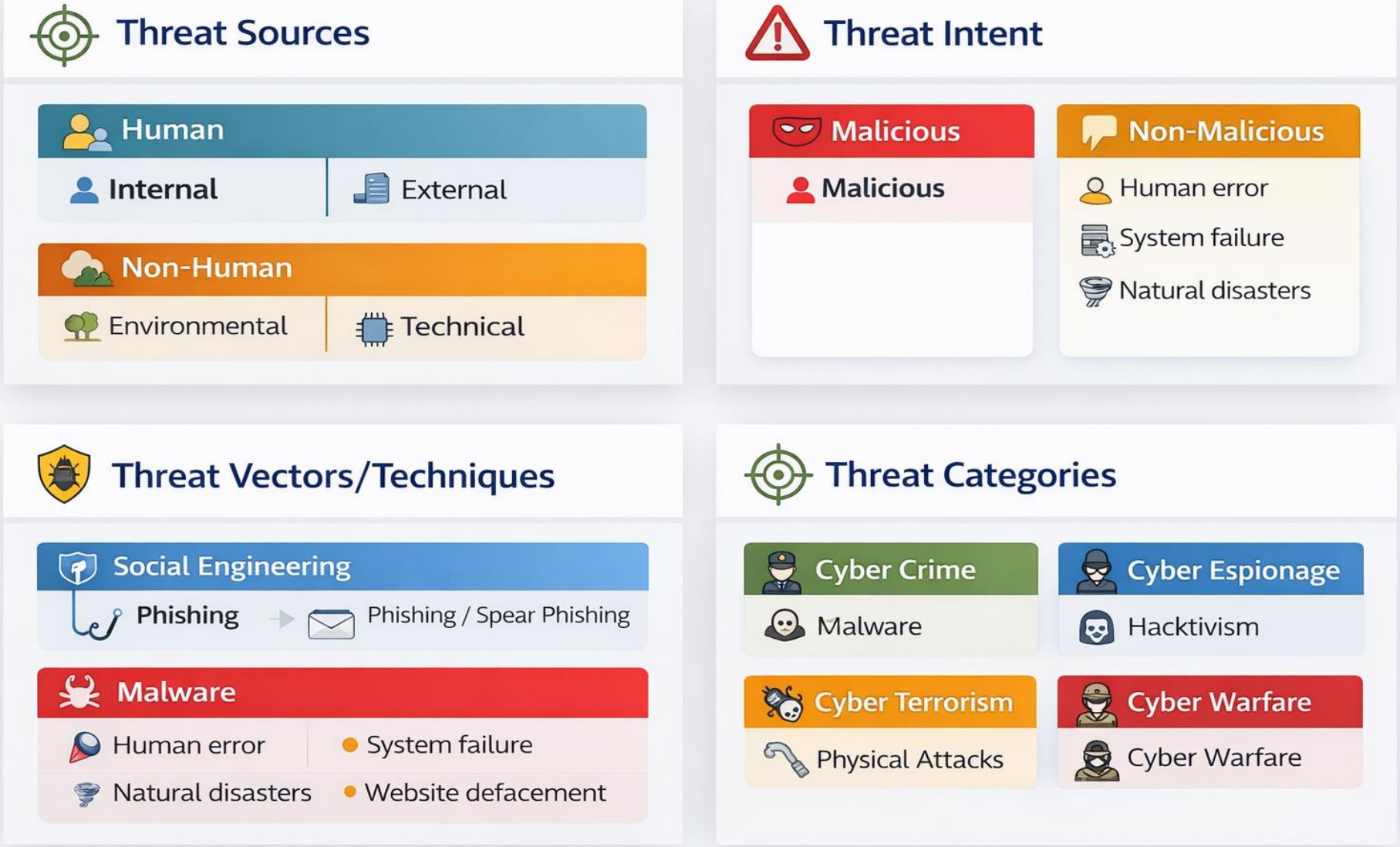
Examples:

- Eavesdropping
- Packet sniffing
- Man-in-the-Middle (MITM)

Threat Damage in a Communication System



THREATS



https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx

Modern Threat Landscape

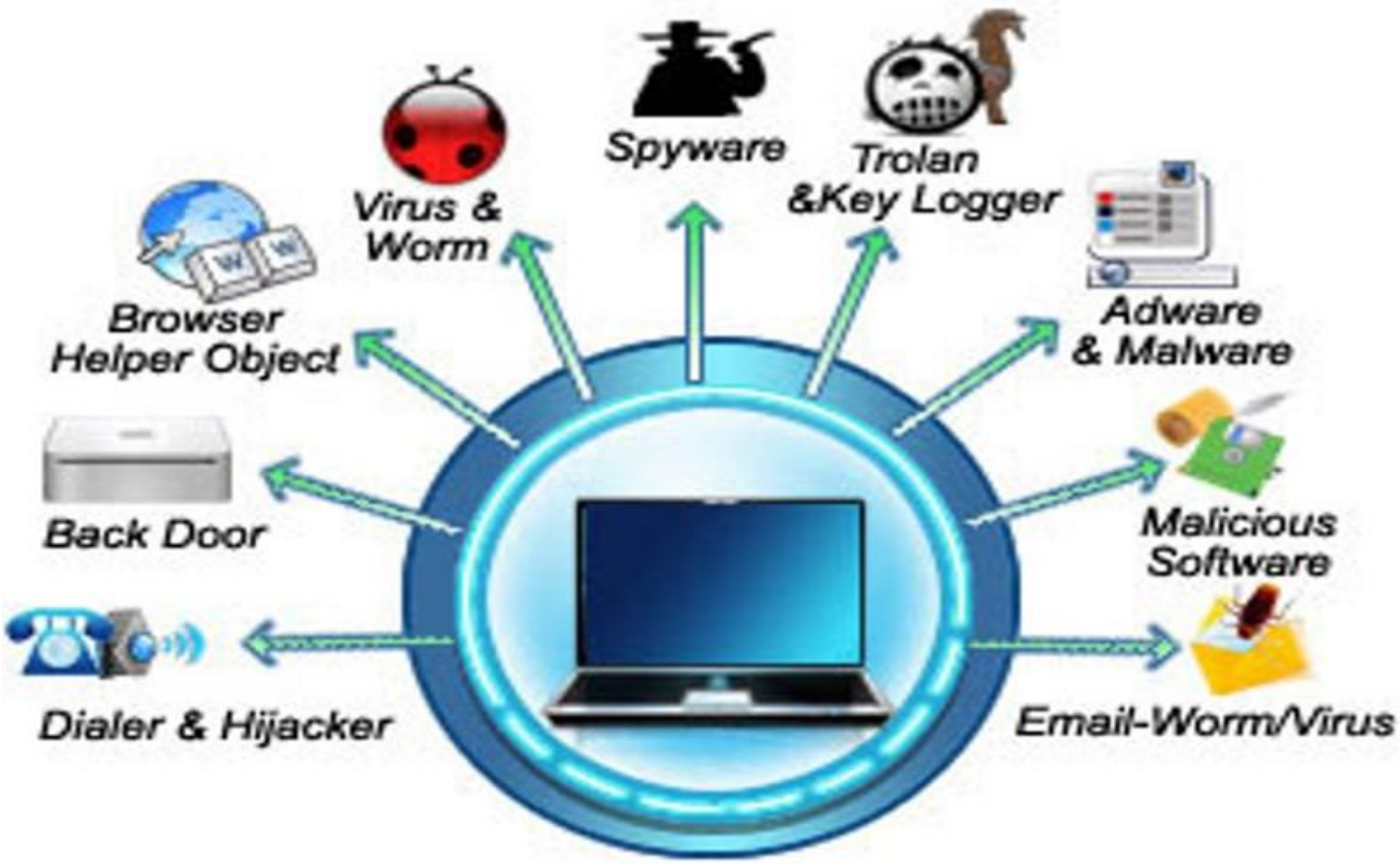
- Supply Chain & Third-Party Threats
  - Compromised vendors, Insecure SaaS providers, or Malicious updates
  - *Supply chain threats are **external human threats with indirect access**.*
- AI-Enabled Threats
  - AI-generated phishing emails, Deepfake voice/video fraud
  - *AI increases scale, speed, and realism of attacks*
- Cloud & API Attacks
  - Cloud misconfiguration, Insecure APIs, or Token theft
- Insider Threat (Intentional vs Unintentional)
  - Malicious Insider or Negligent Insider
- Hybrid Threats
  - Cyber + Physical
  - Cyber + Psychological
  - Ex: Cyber attacks + fake social media campaigns

Threat Vectors/Techniques

- Malware: Malicious Software
- Ransomware: Malware that encrypts files and demands ransom
- Social Engineering: Tricks users into revealing sensitive information
- Supply Chain Attacks: Target trusted vendors, software, or hardware to compromise multiple organizations.
- Advanced Persistent Threats (APTs): Long-term, targeted attacks (often state-sponsored) for espionage or data theft.
- **Zero-Day Exploits**: Exploit unknown or unpatched vulnerabilities in software or hardware.
- **AI-Powered Attacks:** Use of AI to automate attacks, bypass defenses, or create phishing/deepfake campaigns.
- **IoT & OT Attacks:** Target connected devices (IoT) or industrial/operational technology systems.
- **Cloud & API Attacks:** Exploit cloud misconfigurations, insecure APIs, or cloud service vulnerabilities.

TYPES OF MALWARE

Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses and spyware.



Malware Symptoms

- Increased CPU usage
- Slow computer or web browser speeds
- Problems connecting to networks
- Freezing or crashing
- Modified or deleted files
- Appearance of strange files, programs, or desktop icons
- Programs running, turning off, or reconfiguring themselves
- Strange computer behavior
- Emails/messages being sent automatically and without user's knowledge

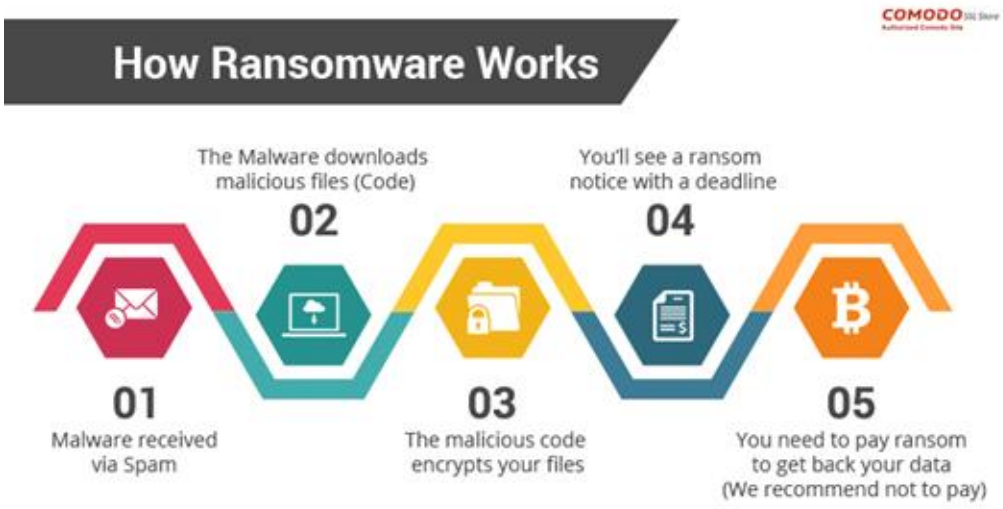
Malware Countermeasures

- Install quality anti-virus software
- Make sure virus definitions of the scanner are regularly updated
- Never open an attachment from an untrusted source
- Taking caution when surfing the internet and downloading files
- Backup data

TYPES OF CYBERSECURITY THREATS

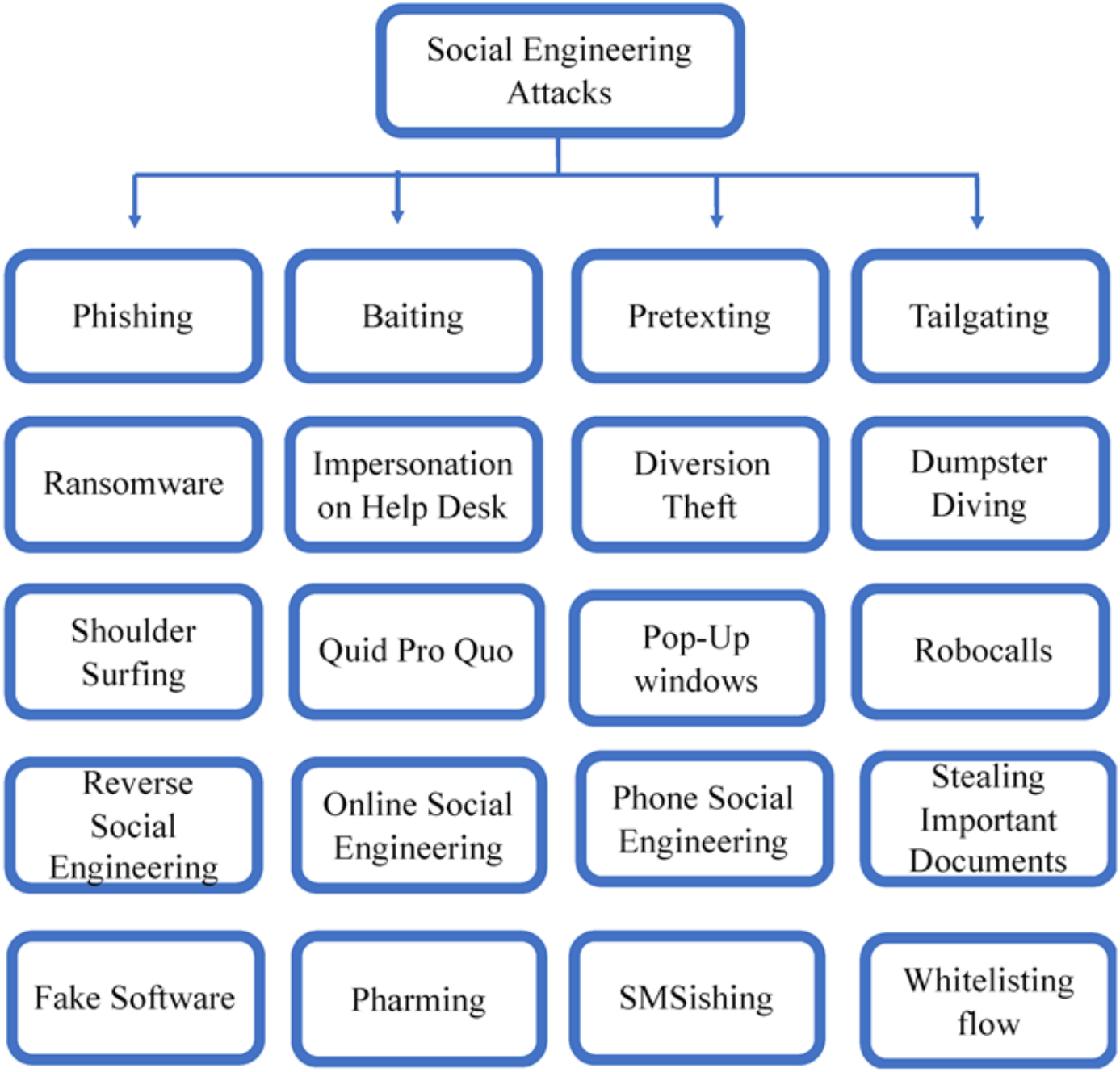
The process of keeping up with new technologies, security trends and threat intelligence is a challenging task.

- **RANSOMWARE (Socially engineered malware)** is a type of malware that involves an attacker locking the victim's computer system files - typically through encryption - and demanding a payment to decrypt and unlock them.
  - WannaCry **ransomware**.
  - Petya and NotPetya **ransomware**.
  - Locky **ransomware**.
  - Cerber **ransomware**.
  - Jigsaw **ransomware**.
  - Bad Rabbit **ransomware**.
  - Ryuk **ransomware**.
  - Dharma (aka CrySIS) **ransomware**.



TYPES OF CYBERSECURITY THREATS

- **SOCIAL ENGINEERING** is an attack that relies on *human interaction to trick users* into breaking security procedures in order to gain sensitive information that is typically protected.
  - **PHISHING** is a form of fraud where fraudulent **emails** are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.
    - Spear phishing/ Whaling: targets a specific individual, group or organization.
    - Angler phishing (latest): targets people on social media sites by taking advantage of the trust that customers have in companies. Attackers trick users into giving up private information by pretending to be customer service
    - Vishing/Smishing: voice phishing & SMS Phishing
  - **PHARMING:** is a cyberattack that redirects users from a legitimate website to a fraudulent one, even when the correct web address (URL) is entered. Unlike phishing, which lures victims into clicking malicious links, pharming is more technical—it poisons DNS or compromises the local system so the victim lands on a fake site without realizing it.
  - **PRETEXTING:** Pretexting is use of a fabricated story, or pretext, to gain a victim's trust and trick or manipulate them into sharing sensitive information, downloading malware, sending money to criminals, or otherwise harming themselves or the organization they work for.
  - **BAITING:** Perpetrator lures the victim with attractive offers or rewards.
  - **TAILGATING:** An unauthorized person wearing a fake ID, follow an authorized person and enters the secure area through a door.


Social Engineering Attacks
Phishing
Baiting
Pretexting
Tailgating
Ransomware
Impersonation on Help Desk
Diversion Theft
Dumpster Diving
Shoulder Surfing
Quid Pro Quo
Pop-Up windows
Robocalls
Reverse Social Engineering
Online Social Engineering
Phone Social Engineering
Stealing Important Documents
Fake Software
Pharming
SMSishing
Whitelisting flow

TYPES OF CYBERSECURITY THREATS

- **Doxing** - the act of publishing private information and identifying information about an individual online with intent to harm.
- **Zero Day Attack** - a form of threat that is unknown to the party or parties responsible for patching or otherwise fixing the flaw. (NO PRIOR KNOWLEDGE)
- **Reverse Social engineering:** an attacker convinces the target that he or she has a problem or might have a certain problem in the future and that he, the attacker, is ready to help solve the problem.

SE Counter Measures

- Password Policies
  - Periodic password change
  - Avoiding guessable passwords
  - Account blocking after failed attempts
  - Length and complexity of passwords
  - Secrecy of passwords
- Physical Security Policies
  - Identification of employees by issuing ID cards
  - Proper Accessing area restrictions
  - shedding of useless documents
  - Security check before employment

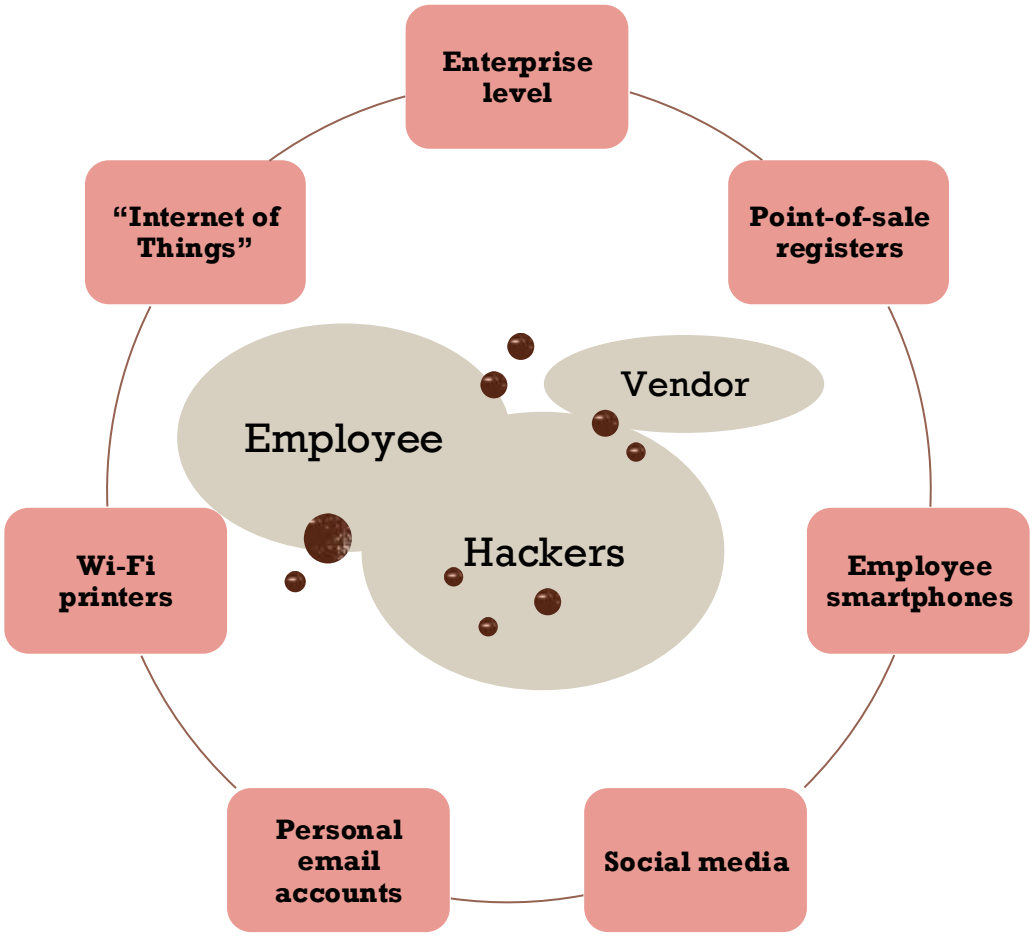
SE Counter Measures

- Effective Training program consisting of all security policies and methods to increase awareness on social engineering
- Operational Guidelines to ensure security of the sensitive information and authorized use of resources
- Classification of Information as top secret, proprietary, for internal use only, for public use
- Access Privileges - administrator, user and guest accounts with proper authorization
- Two factor Authentication

AI-Driven Cyber Threat Vectors

Threat	Description
AI-Generated Malware	• Malware that adapts dynamically to avoid detection. • Can create polymorphic variants automatically.
AI-Enhanced Social Engineering	• Personalized phishing emails, messages, or calls. • Uses AI to analyze targets' behavior and language style.
AI-Driven Reconnaissance	• Automated scanning of networks, websites, and software. • Identifies vulnerabilities and prioritizes high-value targets.
AI Deepfakes & Impersonation	• AI-generated voice, video, or text to impersonate individuals. • Can trick employees, customers, or executives into revealing sensitive info.
AI-Optimized Exploit Kits	• AI selects the most effective attack method per target. • Improves success rates of malware or ransomware campaigns.

WHERE THREATS MAY EXIST

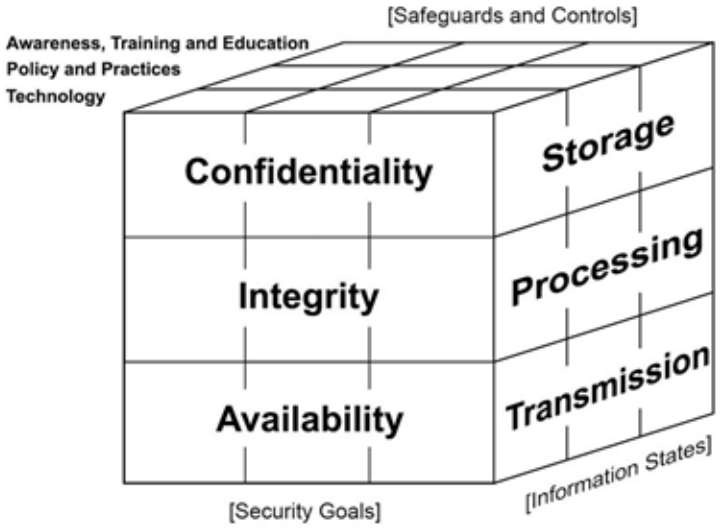


CIA TRIAD

CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY TRIAD

- **Confidentiality** keeping secrets secret
- **Integrity** maintaining the accuracy and consistency of data and not allowing unauthorized people to modify data and systems
- **Availability** making sure data and systems are available when you need them

CIA Triad is a model designed to guide policies for information security within an organization.

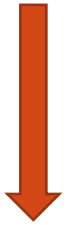


CONFIDENTIALITY

- Confidentiality is the concept of the measures used to ensure the protection of secrecy of data, objects or resources.

- The goal of confidentiality is to prevent or minimize the unauthorized access to data.

- A wide range of security controls can provide protection for confidentiality that include:



Encryption, Access control and Steganography.

ATTACKS FOCUSES ON THE VIOLATION OF CONFIDENTIALITY

Stealing password files: when using public Wi-Fi or inject key logger to your browser

Port scanning: a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number

Shoulder surfing: spying on the user of a cash-dispensing machine (ATM) or other electronic device in order to obtain their personal identification number, password, etc.

ATTACKS FOCUSES ON THE VIOLATION OF CONFIDENTIALITY

- **Eavesdropping:** Eavesdropping is as an electronic attack where digital communications are intercepted by an individual whom they are not intended (Man in the middle)
  - **Sniffing:** interception of data by capturing the network traffic using a sniffer (an application aimed at capturing network packets).
- **Privileges escalation:** is a type of network intrusion that takes advantage of programming errors or design flaws to grant the attacker elevated access to the network and its associated data and applications.
- **Human Errors/mistakes (unintentional)**
- **Intentional damage/harm**
  - .

METHODS USED TO ENSURE CONFIDENTIALITY

- **Data encryption** is a common method of ensuring confidentiality.
- **User IDs and passwords** constitute a standard procedure; two-factor authentication is becoming the norm.
- **Biometric verification** a person can be uniquely identified by evaluating one or more distinguishing biological traits. - fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures.
- **Security tokens** (authentication token) is a small hardware device that the owner carries to authorize access to a network service.

METHODS USED TO ENSURE CONFIDENTIALITY

- **Soft tokens** – is a software-based security token that generates a single-use login PIN.
- **Key fobs** is a small, programmable hardware device that provides access to a physical object that require **two-factor** or **multifactor authentication**.

- **EXTRA MEASURES** might be taken in the case of extremely sensitive documents, precautions such as storing only on:
  - **air gapped computers** - isolating a computer or network and preventing it from establishing an external connection,
  - **disconnected storage devices**.

INTEGRITY

Integrity is **the assurance that the information is reliable and accurate**.

Attacks focus on the violation of integrity: viruses, logic bombs, unauthorized access, errors in coding, system back doors

METHODS USED TO ENSURE INTEGRITY OF DATA

- **File permissions** and **user access controls**.
- **Version control** maybe used to prevent erroneous changes or accidental deletion by authorized users becoming a problem.
- **Checksums/ Hashing**

INTEGRITY

METHODS USED TO ENSURE INTEGRITY OF DATA

➢ **cryptographic checksums** - A cryptographic checksum is a **mathematical value** (called a checksum) that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously changed. Hash value = checksum

HOW TO RESTORE THE AFFECTED DATA?

✓ **Backups** or **redundancies** must be available to restore the affected data to its correct state.

AVAILABILITY

Ensure all information is readily accessible to all authorized users at all times.

Threats to availability includes device failure, software error and environmental issues (heat, flooding, power loss), denial-of-service (DoS) attacks and network intrusions.

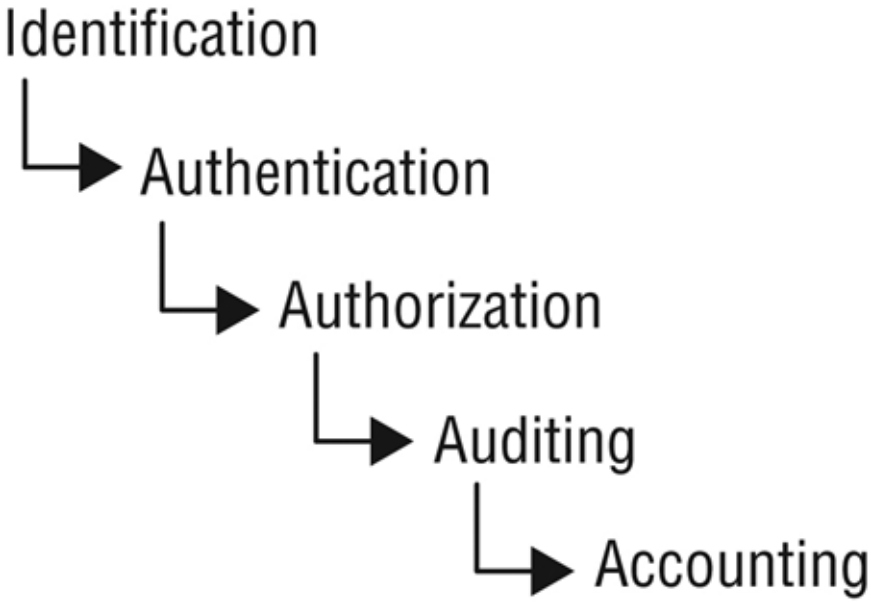
TO PREVENT DATA LOSS

- ✓**A backup copy** may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe.
- ✓Extra security equipment or software such as **firewalls** and **proxy servers** can guard against downtime and unreachable data.
- ✓**Web application firewall (CLOUDFLARE)**

AAA SERVICES

- In addition to the CIA Triad, you need to consider other **security-related concepts and principles when designing a security policy and deploying a security solution.**
- The concept of AAA services - the three A's in this abbreviation refer to authentication, authorization, and accounting/auditing.

- AAA refers to five elements! (It is actually a foundational concept for security)
  - Identification
  - Authentication
  - Authorization
  - Auditing
  - Accounting/ Accountability



ACCESS CONTROL (AAA ELEMENTS)

- ***Identification***: Claiming to be an identity when attempting to access a secured area or system
- ***Authentication***: Proving that you are that identity
- ***Authorization***: Defining the permissions (i.e., allow/grant and/or deny) of a resource and object access for a specific identity
- ***Auditing***: Recording a log of the events and activities related to the system and subjects
- ***Accounting*** (*accountability*): Reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions

PROTECTION MECHANISMS

- Another aspect of understanding and applying concepts of confidentiality, integrity, and availability is the concept of **protection mechanisms or protection controls**.

- **Layering/Defense in Depth**
  - The use of multiple controls in a series.
  - Serial/parallel configuration, mall, bank and airport configuration

- **Abstraction**

Abstraction is used for efficiency.

Similar elements are put into groups, classes, or roles that are assigned security controls, restrictions, or permissions as a collective.

PROTECTION MECHANISMS

- **Data Hiding:**

  Data hiding is the act of intentionally positioning data so that it is not viewable or accessible to an unauthorized subject

- **Encryption**

  Encryption is the art and science of hiding the meaning or intent of a communication from unintended recipients.