UNIVERSITY OF FRONTIER TECHNOLOGY, BANGLADESH

Topic: Introduction to Cyber Security

Presented By:

Rakib Hossen
Assistant Professor
Dept. of Cyber Security Engineering (CySE), UFTB

Today’s Cyber Attacks

Cyber security?

- In present-day society, our daily lives are **increasingly reliant on the use of technology.**
- This dependence brings numerous advantages, including **quick access to online information** and the convenience offered by smart home automation and concepts like the **Internet of Things (IoT).**
- Despite the generally optimistic view of **technological progress**, **cyber security threats** posed by **modern technology are indeed a tangible danger.**
- **Cyber Security** is a way to **protect electronic devices and services connected** to the internet from potential threats.

What is security?

- In general, **security** is “the quality or state of being secure—to be free from danger.”
- A successful **organization** should have the following **multiple layers** of security:-
  - ❑ Physical security
  - ❑ Personnel security
  - ❑ Operations security
  - ❑ Communications security
  - ❑ Network security
  - ❑ Information security

What is Cyber security

- We can divide cybersecurity into two parts:
  - ❑ **Cyber:** refers to the **technology** that includes **systems, networks, programs, and data.**
  - ❑ **Security**: means the **protection of systems, networks, applications, and information**.

- Also called **electronic information** security or **information technology security.**

What is Cyber security

- Cyber security is a discipline that covers **how to defend devices and services from electronic attacks** by nefarious actors such as hackers, spammers, and cybercriminals.

- Cybersecurity involves shielding against **fraudulent tactics, such as phishing, unauthorized data access, identity theft, and malicious ransomware attacks.**

- Definition by Cisco Systems Inc.: "The practice of protecting systems, networks, and programs from digital attacks. These cyberattacks typically aim to gain unauthorized access, manipulate or destroy sensitive information, extort money from users, or disrupt normal business operations."

What is Cyber security

- Cyber security is the **protection of internet-connected** systems such as **hardware, software and data** from **cyber threats**

- Cyber security is the practice of **protecting systems, networks, and programs** from **cyber attacks and unauthorized access**

- The technique of **protecting internet-connected systems** such as **computers, servers, mobile devices, electronic systems, networks, and data** from **malicious attacks** is known as cyber security
- Broadly the term "Cyber Security" is used to **describe protection against various forms of cybercrimes, including identity theft and international digital warfare.**

Why Cyber Security?

Protection of business

Stops the system from crashing

Increase Productivity

Inspire customer satisfaction

Protection of Customers or Clients

History of Cyber security

- **1968**, Maurice Wilkes discusses password security in Time-Sharing Computer Systems.

- **1975**, The Federal Information Processing Standards (FIPS) examines Digital Encryption Standard (DES) in the Federal Register.

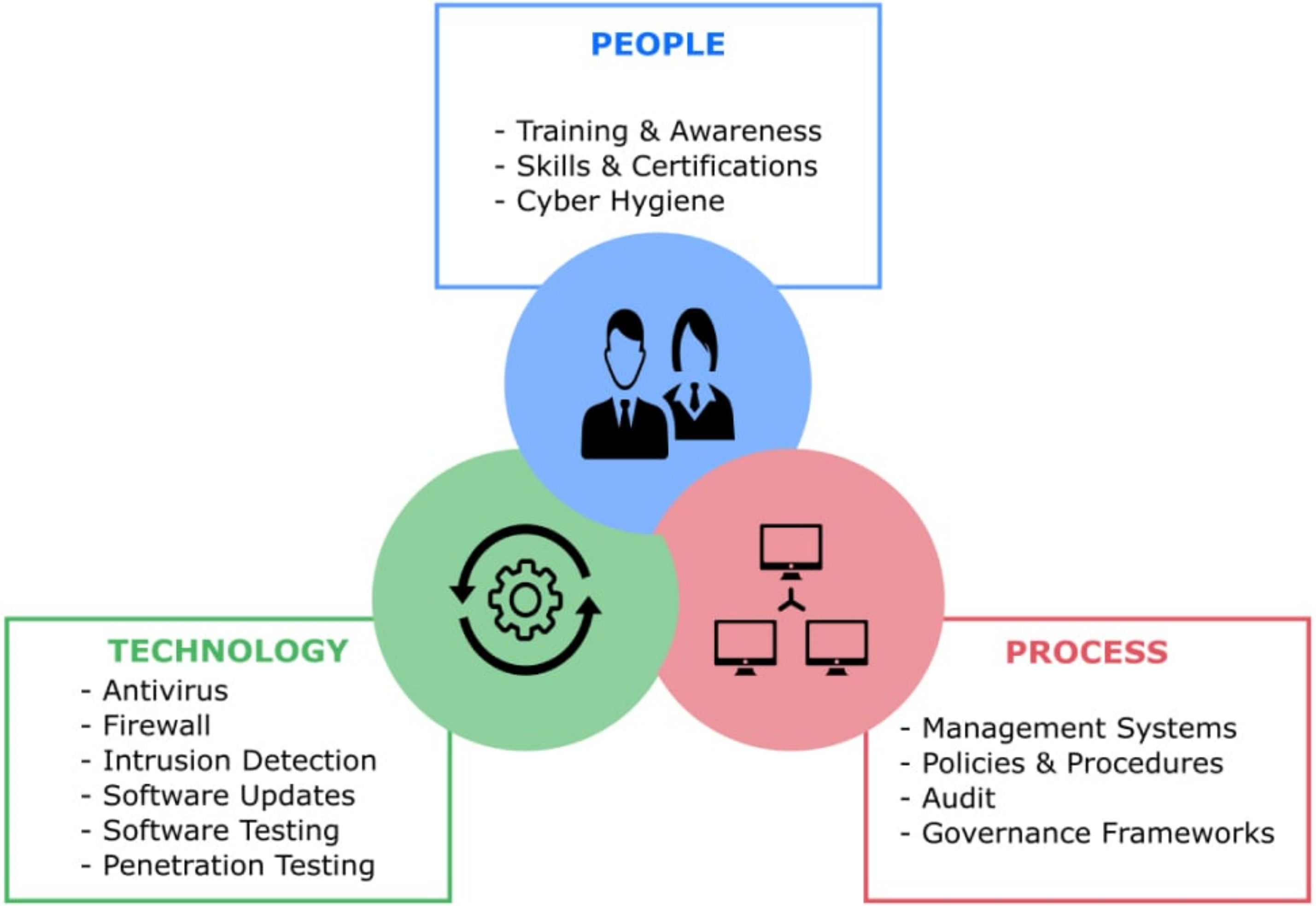
- **1979**, Dennis Ritchie publishes “On the Security of UNIX” and “Protection of Data File Contents,” discussing secure user IDs and secure group IDs, and the problems inherent in the systems.

- **Today**, the Internet brings millions of unsecured computer networks into continuous communication with each other.

Scale of Cyber Security Threats

- It is projected that cybercrime will result in an **annual cost of 10.5 trillion USD worldwide by 2025**, accordingly to Cybercrime Magazine.
  https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
- The global expenses associated with cybercrime are anticipated to increase by **approximately 15 percent each year over the next four years.**
  https://www.thenationalnews.com/business/technology/2021/12/29/top-10-cyber-crime-trends-to-watch-out-for-in-2022/
- Various factors, including the pandemic, the prevalence of cryptocurrency, and the growing trend of remote work, are converging to create a fertile ground for criminals to exploit.

Three Pillars of Cyber security



PEOPLE

- Training & Awareness
- Skills & Certifications
- Cyber Hygiene

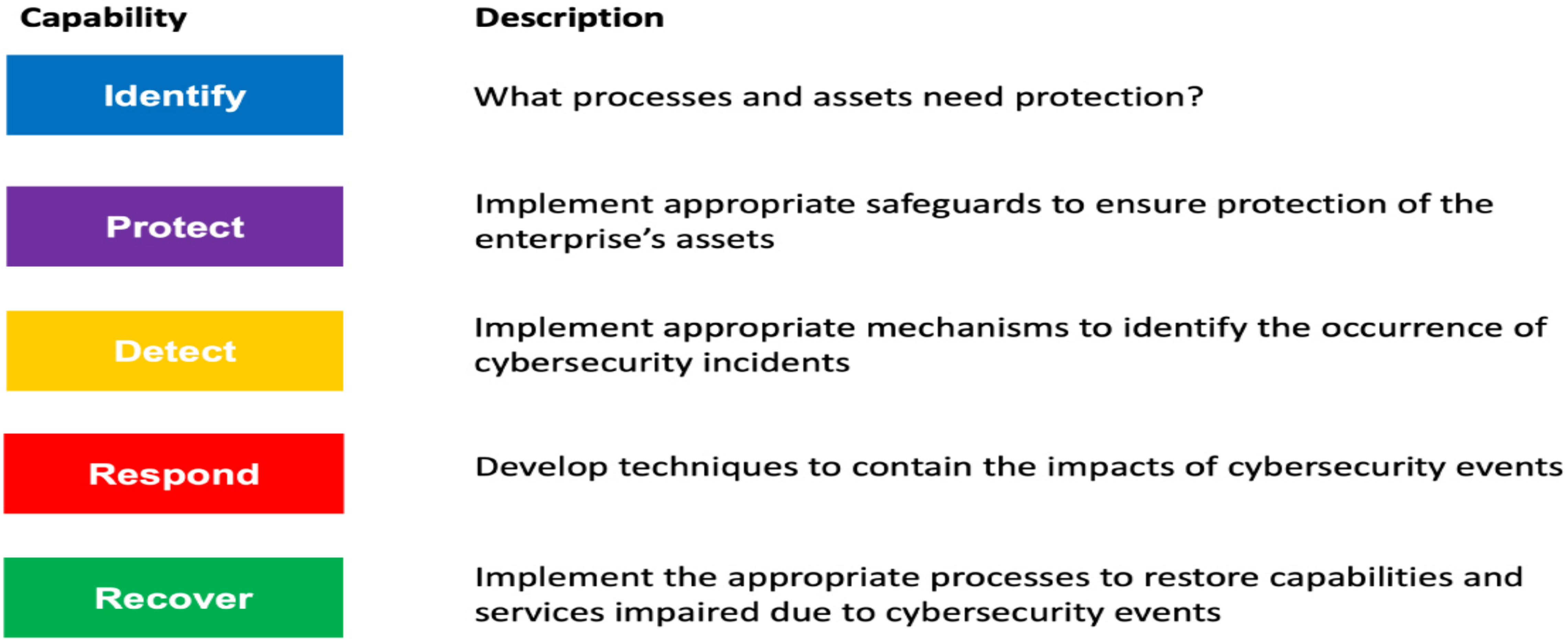
TECHNOLOGY

- Antivirus
- Firewall
- Intrusion Detection
- Software Updates
- Software Testing
- Penetration Testing

PROCESS

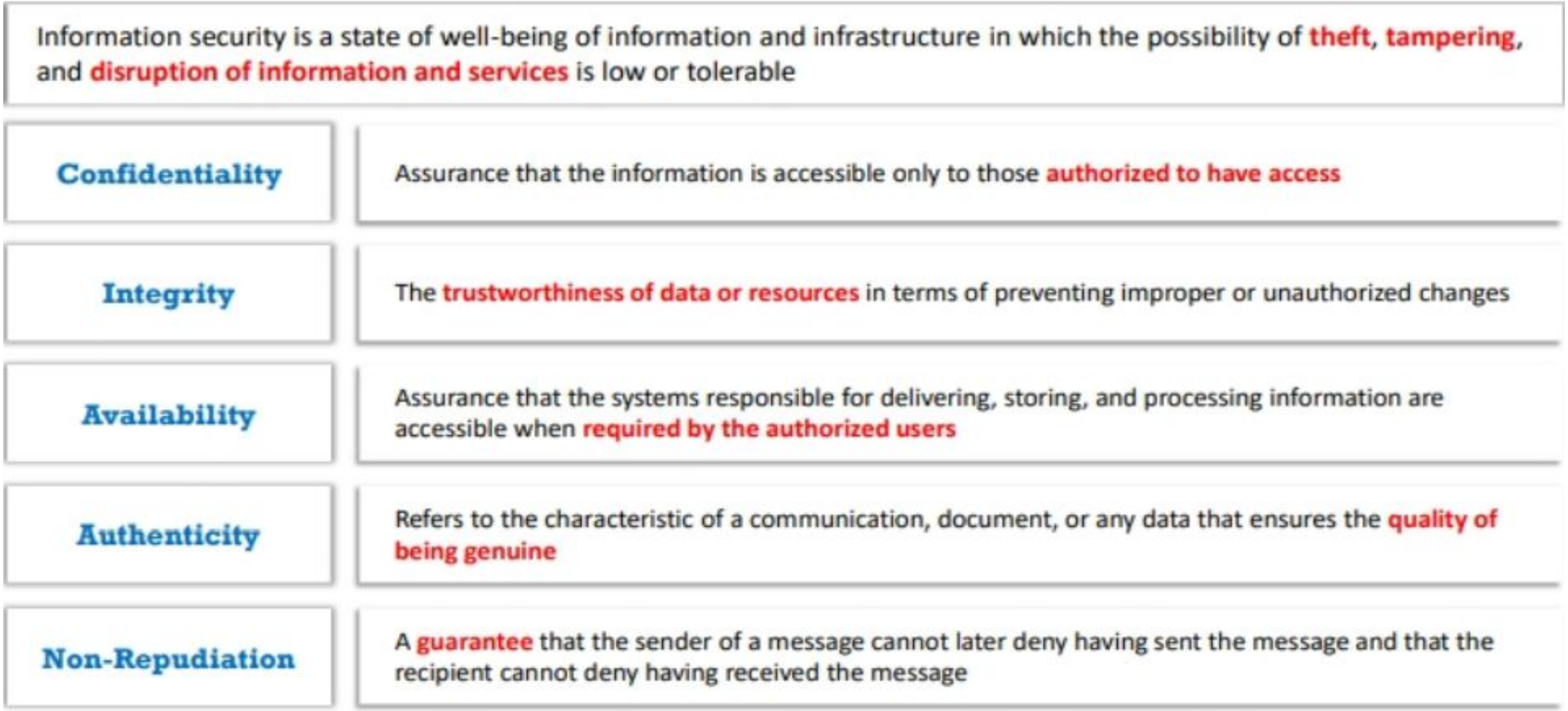
- Management Systems
- Policies & Procedures
- Audit
- Governance Frameworks

The Cyber security Process



Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise’s assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

Five major Elements of Cyber Security



Information security is a state of well-being of information and infrastructure in which the possibility of theft, tampering, and disruption of information and services is low or tolerable

Confidentiality

Assurance that the information is accessible only to those authorized to have access

Integrity

The trustworthiness of data or resources in terms of preventing improper or unauthorized changes

Availability

Assurance that the systems responsible for delivering, storing, and processing information are accessible when required by the authorized users

Authenticity

Refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine

Non-Repudiation

A guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message

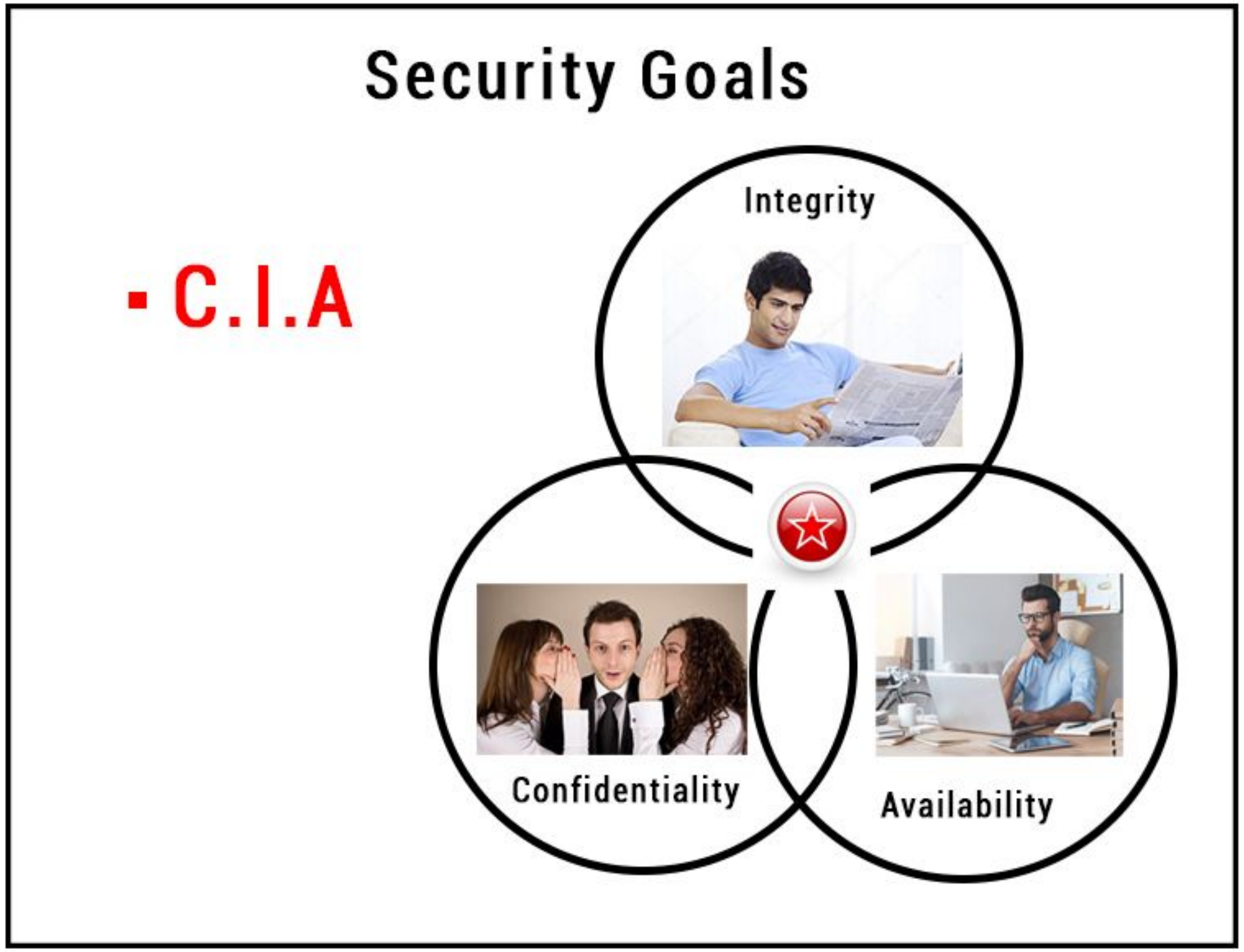
Cyber Security Goals

The objective of Cyber Security is to **protect information from being stolen, compromised or attacked**. Cyber Security can be measured by at least one of three goals-

❑ Protect the confidentiality of data.

❑ Preserve the integrity of data.

❑ Promote the availability of data for authorized users.



Why Does Cyber security Matter?

- Protecting sensitive information
- Defending against cyber threats
- Maintaining the security of critical infrastructure
- Ensuring business continuity
- Enhancing network security
- Collaborating with security analysts
- Adhering to regulatory compliance
- Addressing insider threats
- Evaluating and implementing Cyber Security solutions

Principles of Cyber Security (CIA Triad)

- Cyber Security's main objective is to ensure data protection.
- The security community provides a triangle of three related principles to protect the data from cyber-attacks. This principle is called the CIA triad.

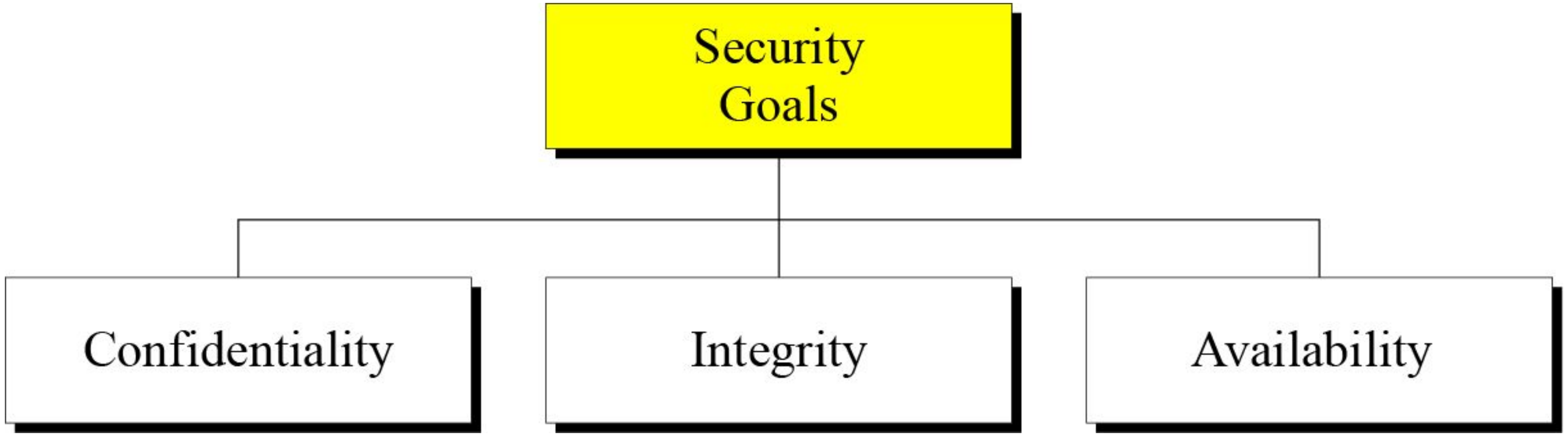
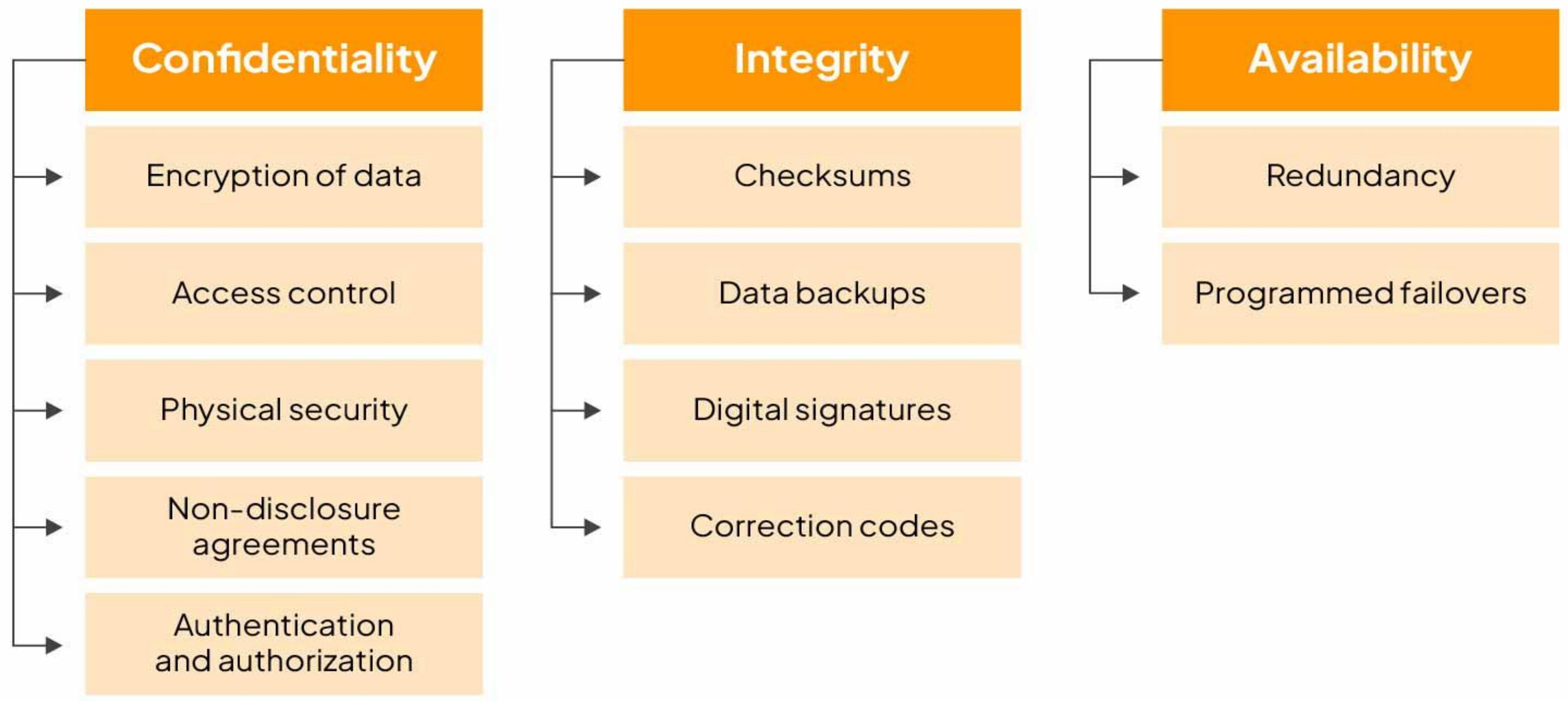


Figure 1.1 Taxonomy of security goals

What are the key goals of Cyber security?



Confidentiality

- Encryption of data
- Access control
- Physical security
- Non-disclosure agreements
- Authentication and authorization

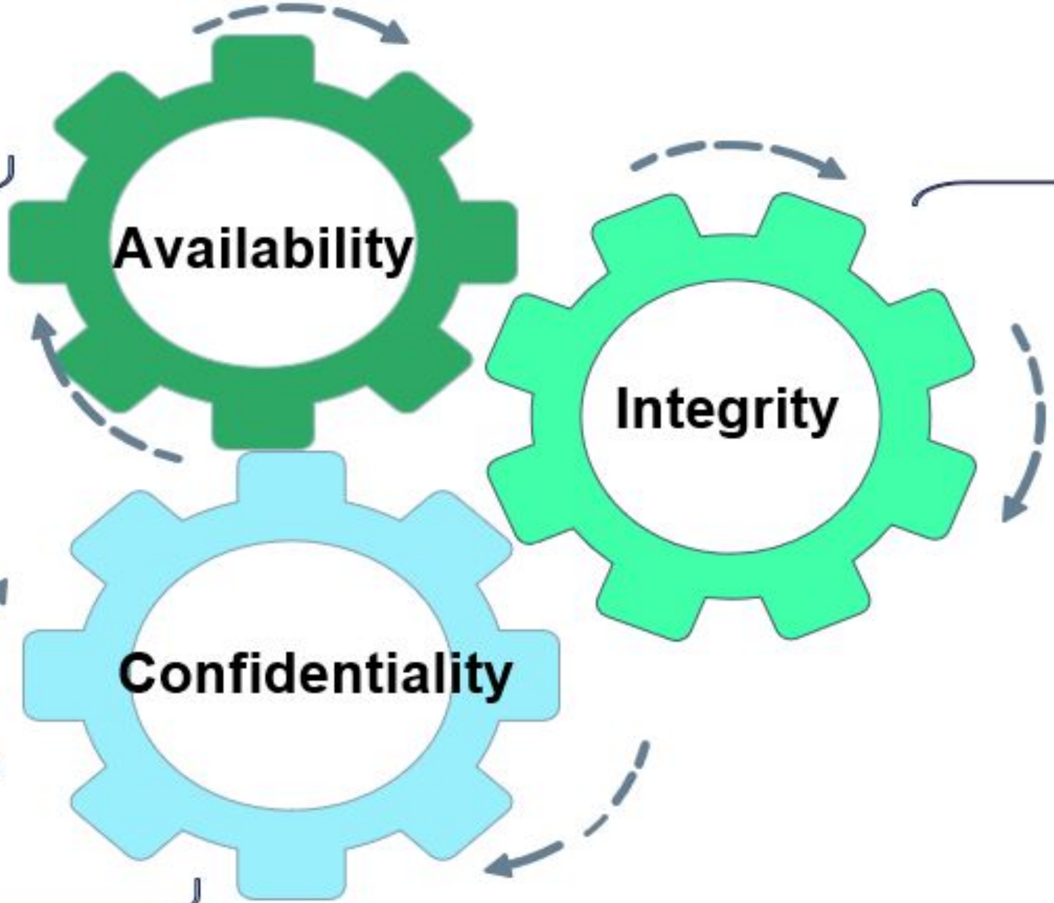
Integrity

- Checksums
- Data backups
- Digital signatures
- Correction codes

Availability

- Redundancy
- Programmed failovers

CIA Triad(Con..)



The principle of availability asserts that system functions and data must be available on demand. asserts

The principle of integrity asserts that information and functions can be added, altered, or removed only by authorized users. Example: Correct data entered by a user in the database

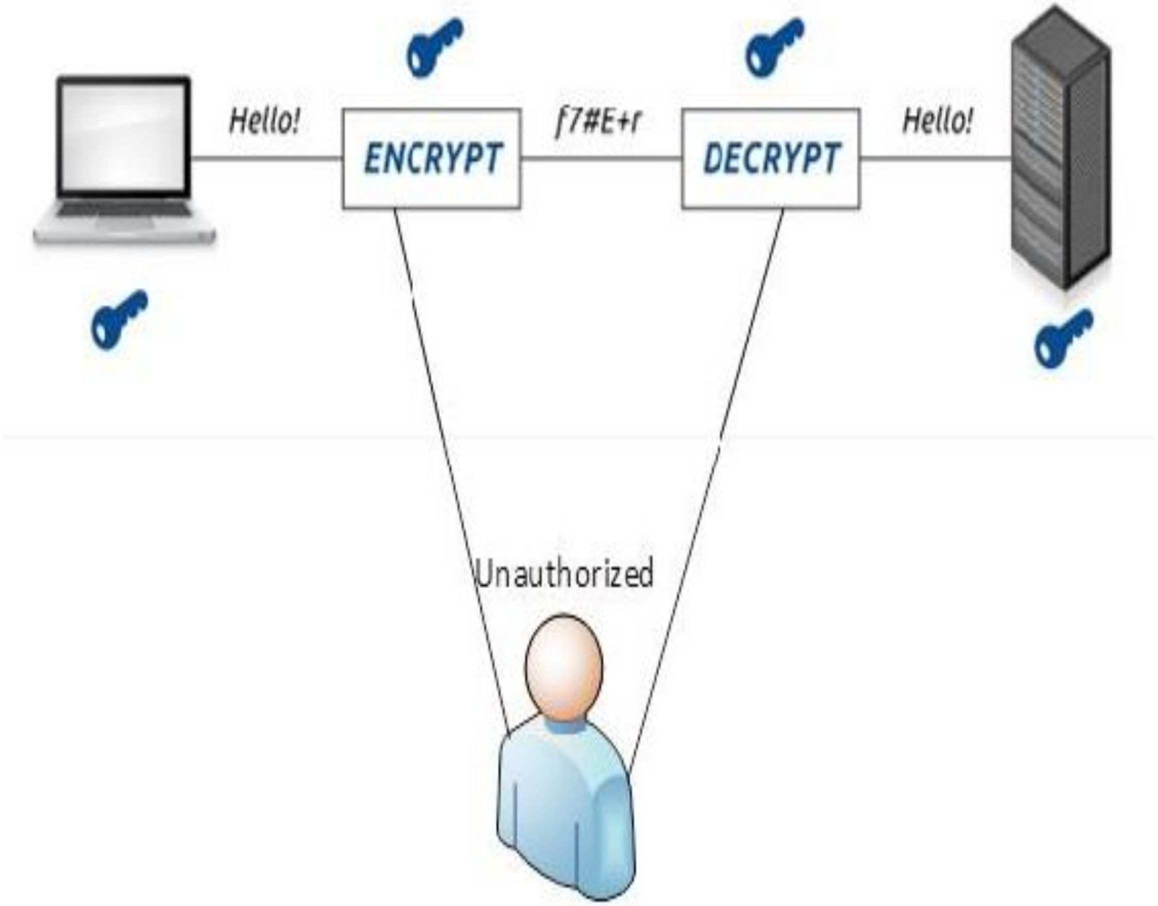
The principle of confidentiality asserts that the information and functions can be accessed only by authorized users.

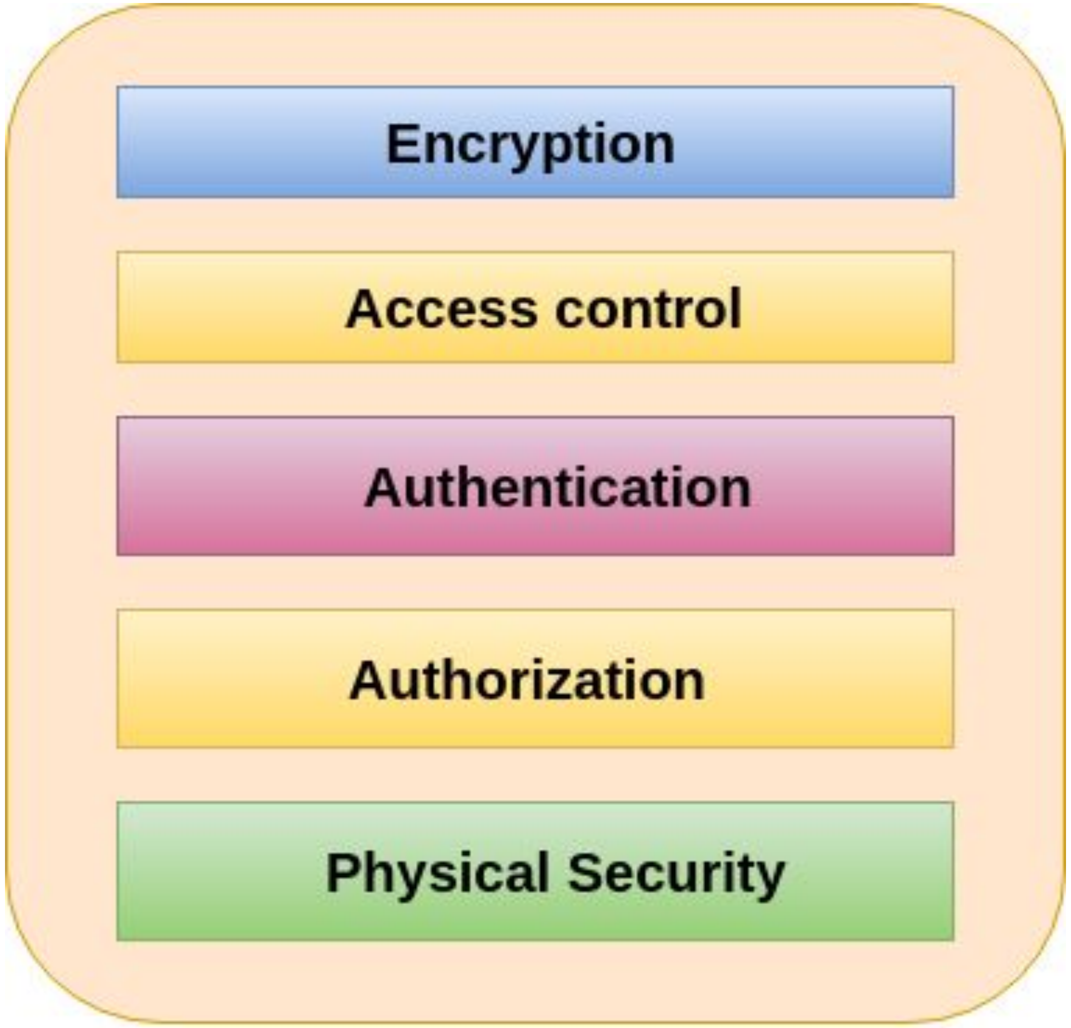
Example: Military Secrets

Confidentiality

- ❑ Confidentiality is probably the most common aspect of **information security.**
- ❑ It also equivalent to **privacy and avoids the unauthorized disclosure of information**
- ❑ We need to **protect our confidential information**.
- ❑ It involves the **protection of data, providing access** for those who are allowed to see it while **disallowing others from learning anything about its content.**
- ❑ It **prevents essential information** from reaching the wrong people while making sure that the right people can get it.
- ❑ **Data encryption** is a good example to ensure confidentiality.

Tools for Confidentiality





Encryption

Access control

Authentication

Authorization

Physical Security

Confidentiality Tools

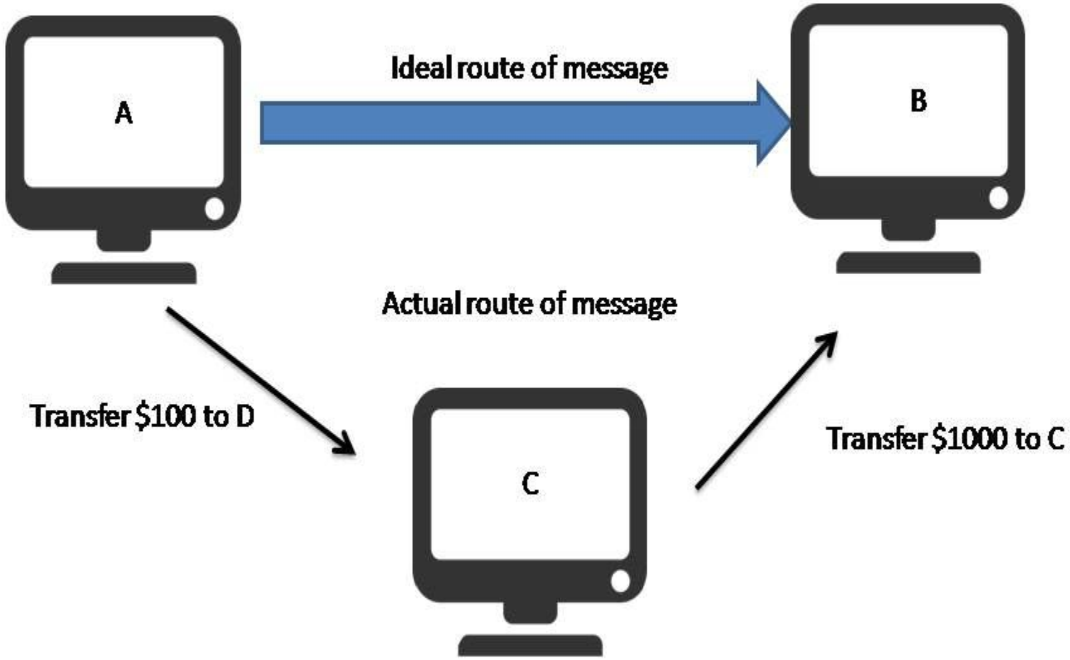
Integrity

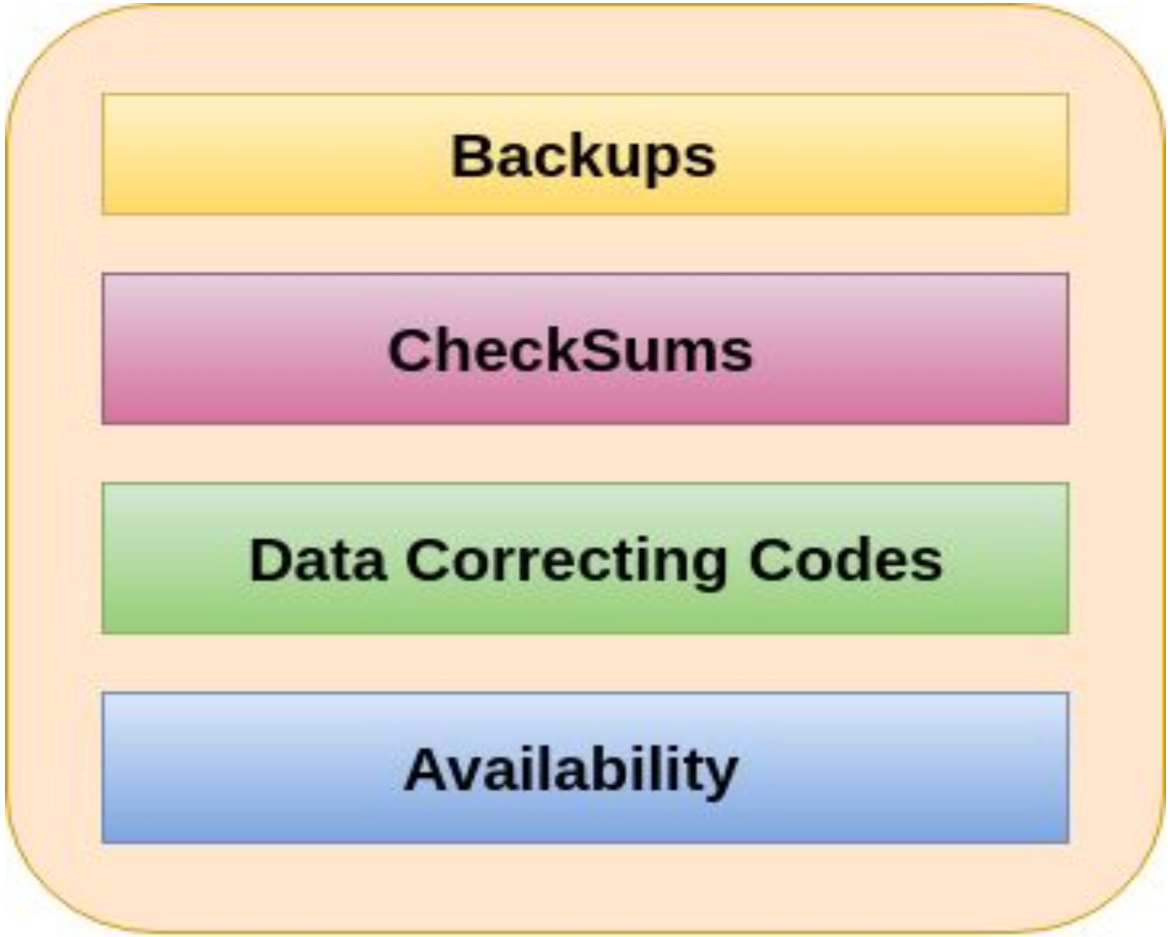
- Information needs to be **changed constantly**. Integrity means that changes need to be done only by **authorized entities** and through authorized mechanisms.

- Integrity refers to the methods for **ensuring that data is real**, **accurate and safeguarded** from **unauthorized user modification.**

- It is the property that information has not be altered in an unauthorized way, and that source of the information is genuine.

Tools for Integrity





Backups

CheckSums

Data Correcting Codes

Availability

Integrity Tools

Availability

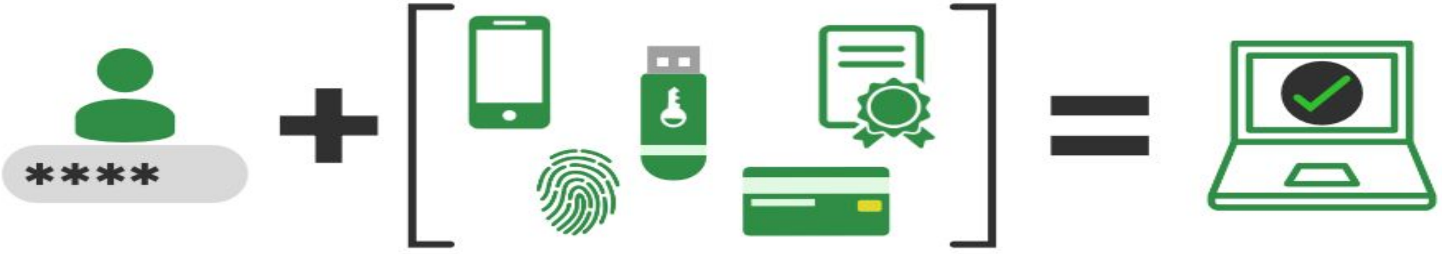
- The information **created and stored** by an organization needs to be **available to authorized entities.**
- Information needs to be **constantly changed**, which means it must be **accessible to authorized entities.**

Tools for Availability

- **Physical Protections**
- **Computational Redundancies**

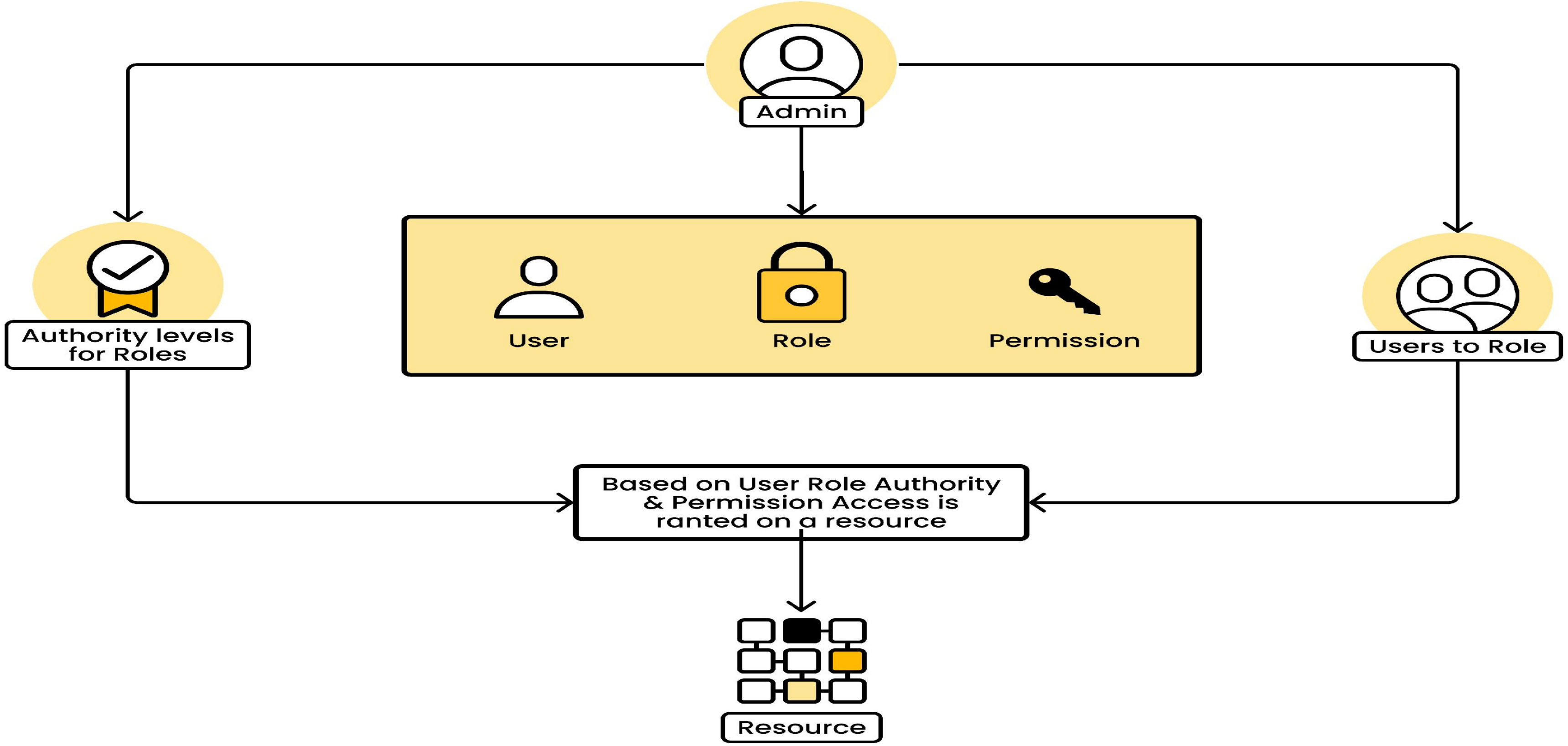
Authentication

Verifying the identity of users or systems to **ensure** they are who they claim to be.



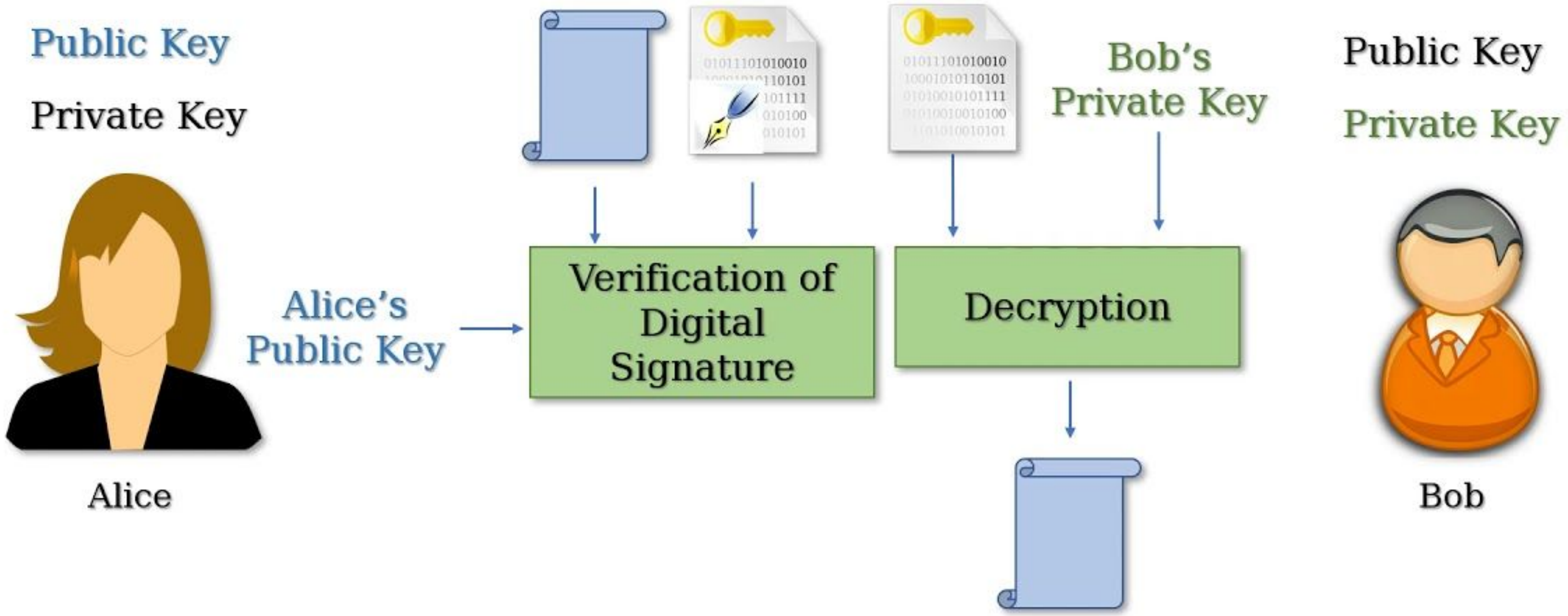
Authorization

Granting or denying access to **resources** based on a user's permissions or privileges limits what actions they can perform.


Admin
Authority levels for Roles
User
Role
Permission
Users to Role
Based on User Role Authority & Permission Access is ranted on a resource
Resource

Non Repudiation

Providing proof that a **specific action or transaction** occurred, makes it **difficult for individuals** to deny their involvement.

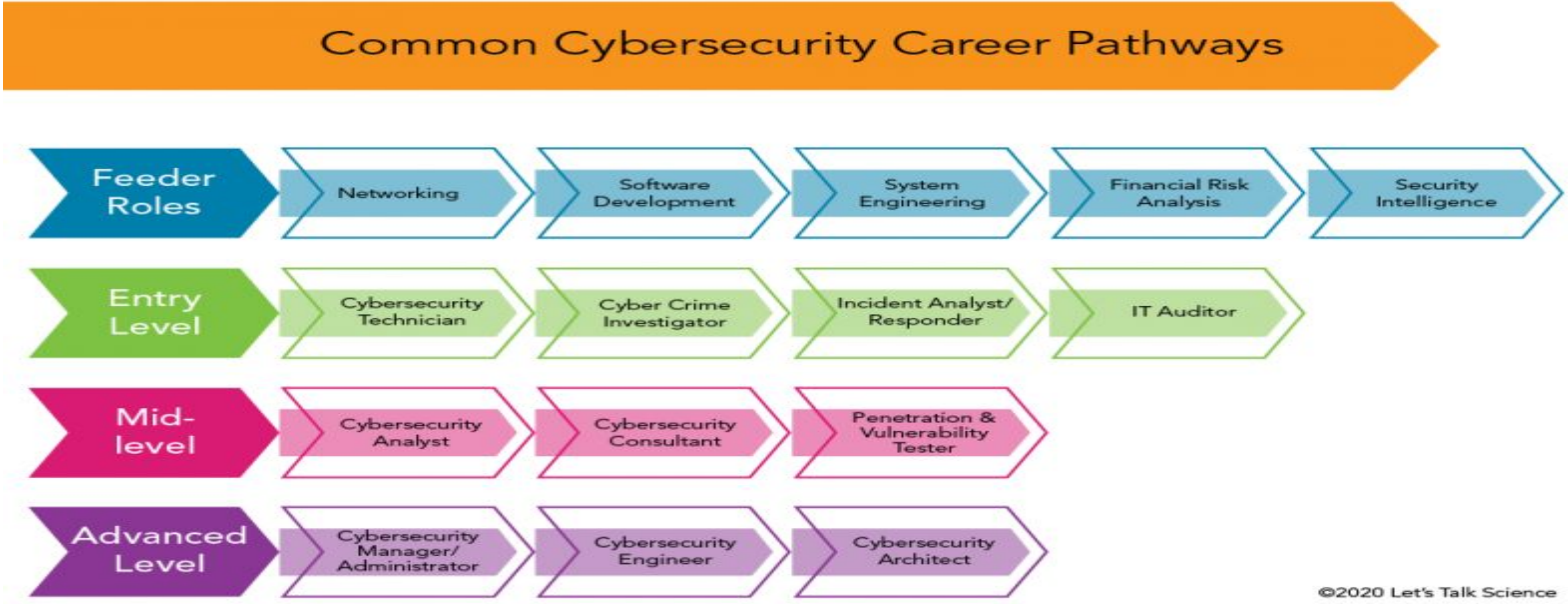


What are the benefits of cyber security?

The benefits of implementing and maintaining cyber security practices include:

- Business protection against cyber-attacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.
- Business continuity.
- Regulatory Compliance.
- Improved confidence in the company’s reputation and trust for developers, partners, customers, stakeholders, and employees.

What are the career opportunities in cyber security?



Common Cybersecurity Career Pathways

Feeder Roles: Networking; Software Development; System Engineering; Financial Risk Analysis; Security Intelligence

Entry Level: Cybersecurity Technician; Cyber Crime Investigator; Incident Analyst/ Responder; IT Auditor

Mid-level: Cybersecurity Analyst; Cybersecurity Consultant; Penetration & Vulnerability Tester

Advanced Level: Cybersecurity Manager/ Administrator; Cybersecurity Engineer; Cybersecurity Architect

©2020 Let's Talk Science

Types of Cyber Security

- **Network Security:** secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse.
- **Application Security**: Protecting the software and devices from unwanted threats.
- **Information or Data Security:** maintain the integrity and privacy of data, both in storage and in transit.
- **Identity management:** It deals with the procedure for determining the level of access that each individual has within an organization.
- **Operational Security:** It involves processing and making decisions on handling and securing data assets.
- **Mobile Security:** securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats.
- **Cloud Security:** protecting the information stored in the digital environment or cloud architectures for the organization.

What is Cyber Crime?

- Cybercrime means the use of a **computer as an instrument** to further illegal ends, such as **committing fraud, trafficking** in child **pornography and intellectual property, stealing identities, or violating privacy.**

It Includes:

- ✔ Illegal access
- ✔ Illegal Interception
- ✔ System Interference
- ✔ Data Interference
- ✔ Misuse of devices
- ✔ Fraud

Types of Cyber Crime?

Computer-Assisted Crimes

Fraud, Denial of services (DOS)

Computer Incidental to Crime

Customer Traffickers

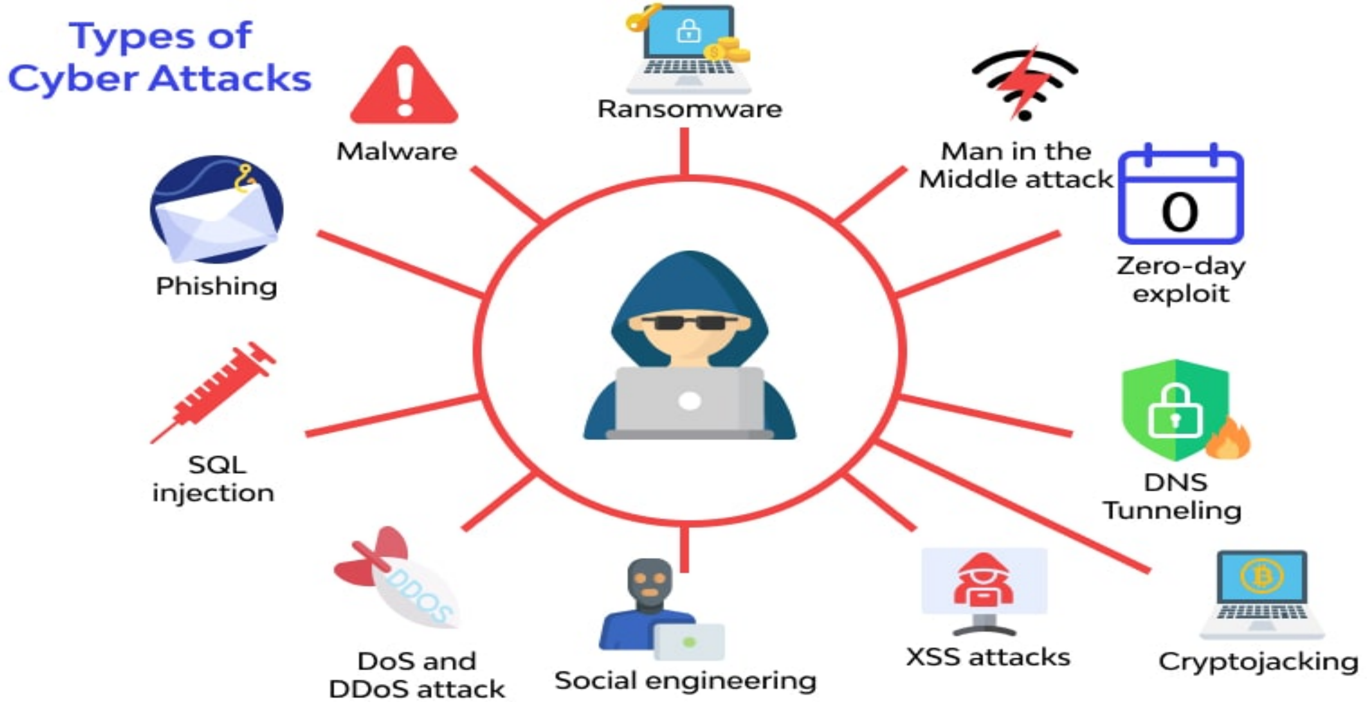
Computer as the target of crimes

Sniffing Viruses

What is Cyber Attack?

- A threat in cybersecurity is a **malicious activity** by an individual or organization to **corrupt or steal data, gain access** to a network, or disrupt digital life.

- Common Cy

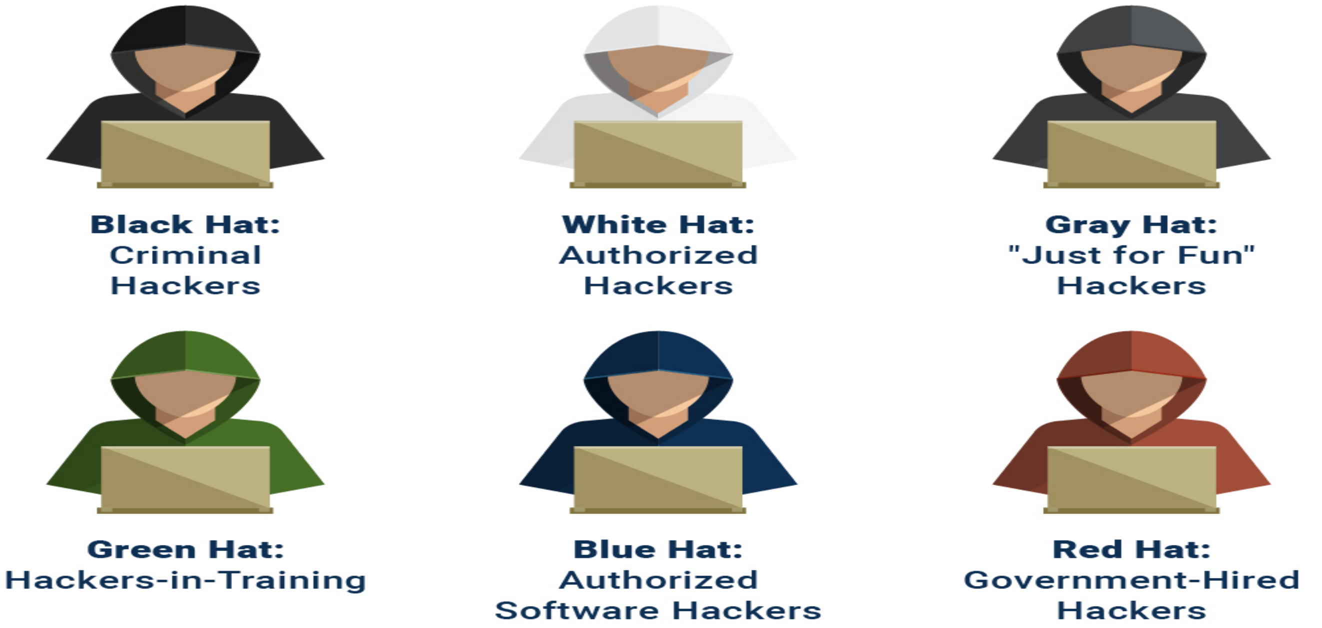


Hacker

- A hacker is a person who **breaks into a computer system**.

- The reasons for hacking can be many: **installing malware, stealing or destroying data, disrupting service, and more.**

- Hacking can also be done for **ethical reasons**, such as trying to find **software vulnerabilities**. so they can be fixed. Some common types of hacker are:


Black Hat: Criminal Hackers
White Hat: Authorized Hackers
Gray Hat: "Just for Fun" Hackers
Green Hat: Hackers-in-Training
Blue Hat: Authorized Software Hackers
Red Hat: Government-Hired Hackers

How to ensure Cyber Security

1. **User education:** Human error is the leading cause of data breaches. Therefore, you must equip staff with the knowledge to deal with the threats they face.

2. **Application security:** Web application vulnerabilities are a common point of intrusion for cybercriminals.

3. **Network security:** Network security is the process of protecting the usability and integrity of your network and data. This is achieved by conducting a network penetration test, which assesses your network for vulnerabilities and security issues.

4. **Leadership commitment:** Leadership commitment is key to cyber resilience. Without it, it is tough to establish or enforce effective processes.

5. **Password management:** Almost half of the UK population uses 'password', '123456' or 'qwerty' as their password. You should implement a password management policy to guide staff to create strong passwords and keep them secure.

Thank You