Module 1: Cybersecurity Overview

Topic 1: Cybersecurity Overview

What is Cybersecurity?

- Technology has its drawbacks aside from its many positives

- The number of cyber crimes has increased, and international companies are sometimes exposed to such crimes, such as Facebook, YouTube and many others.

- Such services to be available to clients, it has to communicate with clients. Such communication could be harmful to the harmful to server/client.

- Our goal to make sure that all communications

  (1) Is secured (Encrypted)
  (2) Did not change (Integrity)
  (3) Not harmful/malicious

What is Cybersecurity?

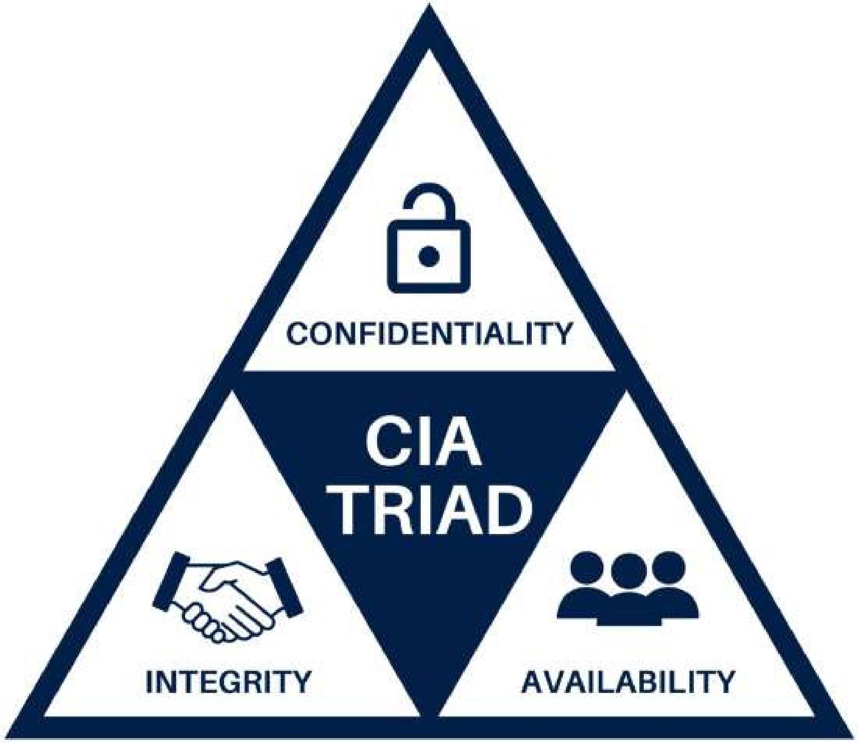
Hence it appeared urgent need to protect corporate security.

What is Cybersecurity?

- Cybersecurity is an operation of protecting computer, server, mobiles, networks, data or any device that communicates with another devices using any connectivity methods such WiFi/ Bluetooth.

- Cybersecurity operation does not only to prevent risk but also to mitigate the risk if possible.

Cybersecurity Fundamentals



Cybersecurity Fundamentals

Confidentiality

- Confidentiality means secrecy of data, keep the data private & safe

- Only authorized persons can view the data

- Raised concept “Need to know” & “Need to have”

Cybersecurity Fundamentals

To ensure and apply Confidentiality, we can apply:

- Data Encryption
- Strong authentication techniques (strong passwords, 2 Factor authentication)
- Biometric authentication
- Physical locks, doors, vaults

Cybersecurity Fundamentals

Integrity

- Integrity means protect data from being modified by unauthorized parties
- Protect data from being changed
- Protect data in case data in motion or data at rest

Cybersecurity Fundamentals

To ensure and apply Integrity, we can apply:

- Data hashing
- Data Backups
- Enforce File permissions
- Monitor file changes
- Use Power supplies

Cybersecurity Fundamentals

Availability

Availability means ability to access system or data anytime whenever needed

- Data is always available and accessible

The opposite of Availability is one of the most cybersecurity attacks which is Denial of service

Cybersecurity Fundamentals

To ensure and apply Availability, we can apply:

- Data redundancy
- Data backups
- Backup power supplies
- Disaster recovery & Business continuity plans

Types of Cyber Attacks

Cyber Attacks can be categorized based on:

- Source of Attack

  Internal Attacker / External attacker

- Attacked system

  System (Server,OS) or Web service or Mobile service or IOT or etc.

- Way of attack

  Direct (Active) attack or Indirect (passive) attack

Types of Cyber Attacks

Examples on Cyberattacks:

Malware/virus	System attack
Backdoors	System attack
SQL injection	Web attack
Brute force	Web attack
Root/ Jailbreak	Mobile attack
Phishing	System, Web, Mobile attack
Denial of Service	System, Web, Mobile attack
Man in the middle	System, web, mobile attack

Cybercrime

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

Cybercrime is carried out by individuals or organizations.

Some cybercriminals are organized, use advanced techniques and are highly technically skilled.

Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money.

Cybercrime

Email and internet fraud (like spam and phishing).

Identity fraud (where personal information is stolen and used).

Theft and sale of corporate data.

Ransomware attacks (encrypts a victim's files, then demands a ransom from the victim to restore access to the data upon payment).

Crypto jacking (where hackers mine cryptocurrency using resources they do not own).

Cybercrime

General Data Protection Regulation (GDPR- EU) & Sarbanes Oxley (USA)

Law No. 175 of 2018 Regarding Anti-Cyber and Information Technology Crimes (Egypt).

According to article 14, individuals who gain access to or hack a website, private account, or

prohibited information system, whether intentionally or unintentionally, may be penalized with

imprisonment of no less than a year and/or a fine of 50,000–100,000 EGP.

If the hacking leads to the damage, erasure, altering, copying, or redistribution of data or information, the term of imprisonment would be for no less than two years.

The Future of Cybersecurity

Currently, the need for better cyber security methods has reached all-time high importance because of ever-increasing cyber threats.

The evolution of cyber threats and their scale of destruction in recent years has brought about a change in the perception of cyber security and proven the need for an active and dynamic cyber security infrastructure.

The Future of Cybersecurity

Although there is no way to know precisely what the future of cybersecurity holds, it will likely be full of innovation and improvements.

As technology advances, so does the need for better cybersecurity solutions. The demand for Cyber Security professionals has increased significantly in the last few years making a career in cybersecurity very promising.