Cybersecurity

AL Mansour University College

Digital Media Department

4th Class

Lecturer Mustafa Muhanad

-1-

Introduction to Cyber Security

1.1 Overview of Cyber Security

The internet has made the world smaller in many ways, but it has also opened us up to influences that have never before been so varied and so challenging. As fast as security grew, the hacking world grew faster.

Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks.
It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

cybersecurity categories include:

1. Application Security: Application security protects devices, applications, and software from cyberattacks.
2. Operational Security: It places a great emphasis on securing data assets.
3. Information Security: All about protecting the privacy and integrity of data in transit and storage.
4. Network Security: The process of ensuring security to computer networks from malware or targeted attackers.
5. End-user Education: End-user education aims to teach users about cybersecurity threats and the best security practices to avoid them.

Cybersecurity solutions protect against three types of cyber threats, which are

1. Cyber Attack: Cyberattacks can be classified in a number of ways. For example, cyber-attacks are classified according to their goal or the goal of their implementation; they can also be classified according to the technology or gaps on which they depend; and they can be classified according to their effects.

2. Cyber Crime: Groups or single actors targeting systems, networks, or servers for monetary benefit or for causing disruption.

3. Cyber Terrorism: (also known as digital terrorism) is defined as disruptive attacks by recognized terrorist organizations against computer systems of generating alarm, panic, or physical disruption of the information system.

1. 2 Cybersecurity objectives

The objective of cybersecurity is to protect information from being stolen, compromised, or attacked. Cybersecurity can be measured by at least one of three goals:

1. Protect the confidentiality of data, including the protection of information from any unauthorized disclosure.

2. Preserve the integrity of the data, the accuracy, and the completeness of the information.

3. Promote the availability of data for authorized users. The ability to access information and resources required by the business process.

These goals form the confidentiality, integrity, and availability (CIA) triad, the basis of all security programs. The CIA triad is a security model that is designed to guide policies for information security within the premises of an organization or company. This model is also referred to as the AIC (Availability, Integrity, and Confidentiality) triad to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

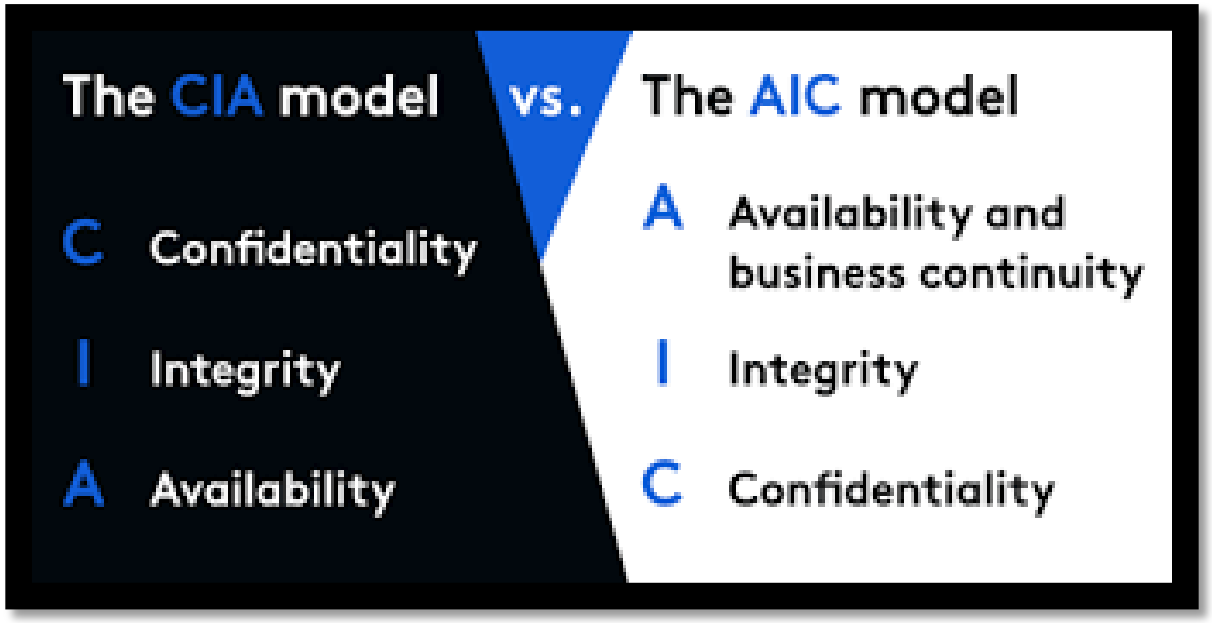

Figure (1.1): AIC or CIA Model

1. 3 Cybersecurity and Network Security

Network Security: Network security is the measure taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data has a degree of protection against many cyber threats.

Cyber Security: Cyber security is the measure to protect our system from cyberattacks and malicious attacks. It is basically to advance the security of the system so that we can prevent unauthorized access to it from an attacker. It protects cyberspace from attacks and damages. Cyberspace can be hampered by inherent vulnerabilities that cannot be removed.

Figure (1.2): relation between Information, Cyber, and Network Security.

What is the difference between Cyber Security and Network Security?

Cyber Security	Network Security
1. Cyber Security is the subset of Information security.	1. Network Security comes under the domain of Cyber Security.
2. Protects data residing in devices and servers.	2. Protects data flowing over Network.
3. Deals with protection from cyber attack	3. Deals with protection for Denial of Service attack.
4. Strikes against Cyber Crime and cyber frauds.	4. Strikes against Trojans.
5. Ensures to protect entire digital data.	5. Ensures to protect transmit data only.
6. Network protection, applications, up-to-date information, comes under Cyber Security.	6. ID and Passwords, internet access, firewalls, backup, comes network security.
7. Cyber Security protects the organization from all kinds of digital attacks from the cyber Realm.	7. Network Security is all about protecting the organization's IT infrastructure from all kinds of online threats.