**Al- Mustaqbal University**

**College of Sciences**

**Department of Cybersecurity**

**Principles of Cyber Security**

**First stage**

**Lecture 1**

 **2025-2024 Lectuer : Muntather AL-Mousawi**

**Overview**

introduces security fundamentals. It begins by examining the current challenges in computer security and why it is so difficult to achieve. It then describes information security in more detail to illustrate why it is important.

**Lecture Objectives**

1. Explain the challenges of securing information

2. Define information security and explain why it is important

3. Identify the types of threat actors that are common today

**OB.1: Challenges of Securing Information**

1. Explain that there is no simple solution to securing information. This can be seen through the different types of attacks that users face today, as well as the difficulties in defending against these attacks.

**1.1 Today’s Security Attacks**

* 1. 1. Describe some recent security attacks, such as the following: a. A reporter drove a Jeep Cherokee while two security researchers 10 miles away remotely connected to it and started manipulating its controls.
	2. b. United Airlines passenger who tampered with the Seat Electronic Box to connect to other system on the plane.
	3. c. Half a billion Yahoo accounts were compromised by attacker who gained unauthorized access to its web servers.
	4. 2. Mention that security statistics bear witness to the continual success of attackers: a. From 2005-2017 over 907 million electronic data records in the U.S. had been breached.

**(1)**

**1.2 Reasons for Successful Attacks**

* 1. 1. Discuss the following reasons behind successful attacks: a. Widespread vulnerabilities
	2. b. Configuration issues
	3. c. Poorly designed software
	4. d. Hardware limitations
	5. e. Enterprise-based issues

**1.3 Difficulties in Defending against Attacks**

* 1. 1. Describe the following difficulties in defending against attacks: a. Universally connected devices
	2. b. Increased speed of attacks
	3. c. Greater sophistication of attacks
	4. d. Availability and simplicity of attack tools
	5. e. Faster detection of vulnerabilities
	6. f. Delays in security updating
	7. g. Weak security update distribution
	8. h. Distributed attacks
	9. i. Use of personal devices
	10. j. User confusion

**(2)**

**OB.2 What Is Information Security?**

1. Mention that knowing why information security is important today and who the attackers are is beneficial. Point out that knowing the terminology used can be helpful when creating defenses for computers.

**2.1 Understanding Security**

* + 1. Explain that security can be considered as a state of freedom from a danger or risk. This state or condition of freedom exists because protective measures are established and maintained.

**2.2 Defining Information Security**

1. Define information security as the tasks of guarding information that is in a digital format. It ensures that protective measures are properly implemented. Information security cannot completely prevent attacks or guarantee that a system is totally secure.

* 1. 2. Explain that information security is intended to protect information that has value to people and organizations. That value comes from the characteristics of the information:
	2. a. Confidentiality
	3. b. Integrity
	4. c. Availability

3. Explain that information security is achieved through a combination of three protections.

4. Emphasize that information security is that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures.

**(3)**

**2.3 Information Security Terminology**

* 1. 1. Define the following information security terms: a. Asset
	2. b. Threat
	3. c. Threat actor
	4. d. Vulnerability
	5. e. Attack vector
	6. f. Attack surface
	7. g. Risk

2. Discuss and define the different options available when dealing with risks.

a. Acceptance

b. Transference

c. Risk avoidance

d. Mitigation

**(4)**

**Quick Quiz 1**

1. Which protection ensures that only authorized parties can view the information?

a. Confidentiality

b. Integrity

c. Accounting

d. Availability

* 1. 2. Which of the following terms best describes ensuring that data is accessible to authorized users? a. Integrity
	2. b. Accounting
	3. c. Availability
	4. d. BYOD

3. A(n) \_\_\_\_ is defined as something that has a value.

4. A situation that involves exposure to some type of danger is known as which of the following?

a. vector

b. risk

c. threat

d. asset

5. Addressing a risk by making it less serious is known as which of the following?

a. acceptance b. transference

c. avoidance d. mitigation

**(5)**

**2.4 Understanding the Importance of Information Security**

1. Mention that the main goals of information security are to prevent data theft, thwart identity theft, avoid the legal consequences of not securing information, maintain productivity, and foil cyberterrorism.

2. Explain that security is often associated with theft prevention. The theft of data is one of the largest causes of financial loss due to an attack. Individuals are often victims of data thievery.

3. Mention that identity theft involves using someone’s personal information to establish bank or credit card accounts that are then left unpaid, leaving the victim with the debts and ruining their credit rating.

* 1. 4. Explain that a number of federal and state laws have been enacted to protect the privacy of electronic data, including the following: a. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
	2. b. The Sarbanes-Oxley Act of 2002 (Sarbox)
	3. c. The Gramm-Leach-Bliley Act (GLBA)
	4. d. Payment Card Industry Data Security Standard (PCI DSS)
	5. e. State notification and security laws

5. Explain that cleaning up after an attack diverts resources such as time and money away from normal activities

6. Define cyberterrorism as attacks by terrorist groups using computer technology and the Internet. Utility, telecommunications, and financial services companies are considered prime targets of cyberterrorists.

**(6)**

**OB.3 Identify the types of threat actors that are common today**

**3.1 Who Are the Threat Actors?**

1. Explain that the term threat actor, in a generic sense, is used to describe individuals who launch attacks against other users and their computers.

2. Explain that threat actors of today have a more focused goal of financial gain: to exploit vulnerabilities that can generate income.

* 1. 3. Point out that the characteristic features of different groups of threat actors can vary widely: a. Sophisticated
	2. b. Funding and resources
	3. c. External or internal to the enterprise
	4. d. Intent and motivation

4. Today threat actors are recognized in more distinct categories, such as script kiddies, hactivists, nation state actors, insiders, and others.

**Other Threat Actors**

**Common Types of Attackers and Their Characteristics**

**(7)**

**1. Script Kiddies**

**Characteristics: Unskilled individuals using pre-written tools or scripts to exploit vulnerabilities.**

**Motivations: Thrill, notoriety, or curiosity rather than financial or strategic goals.**

**Methods: Basic attacks like Denial of Service (DoS), website defacement, or simple phishing.**

**Threat Level: Generally low due to lack of sophistication but can cause widespread nuisance.**

**2. Hacktivists**

**Characteristics: Politically or ideologically motivated attackers who aim to promote a cause.**

**Motivations: Social justice, activism, or political statements.**

**Methods: Website defacements, DDoS attacks, or data leaks targeting specific organizations or governments.**

**Threat Level: Moderate, as their attacks can be disruptive and damaging to reputation.**

**3. Cybercriminals**

**Characteristics: Organized groups or individuals seeking financial gain.**

**Motivations: Profit through fraud, identity theft, ransomware, or selling stolen data.**

**Methods: Advanced phishing schemes, ransomware attacks, or exploiting vulnerabilities in systems.**

**Threat Level: High, due to their organized and sophisticated techniques.**

**(8)**

**4. Insiders**

**Characteristics: Individuals with legitimate access to an organization's resources but misuse it maliciously or accidentally.**

**Motivations: Revenge, financial gain, ideological reasons, or negligence.**

**Methods: Data theft, sabotage, or leaking confidential information.**

**Threat Level: High, as they have trusted access and knowledge of internal systems.**

**5. State-Sponsored Actors (Nation-States)**

**Characteristics: Highly skilled attackers funded and supported by governments.**

**Motivations: Espionage, political disruption, or cyber warfare.**

**Methods: Advanced Persistent Threats (APTs), zero-day exploits, and targeting critical infrastructure.**

**Threat Level: Extremely high, given their access to significant resources and expertise.**

**6. Terrorists**

**Characteristics: Groups using cyberattacks to instill fear or disrupt critical infrastructure.**

**Motivations: Ideological or religious reasons.**

**Methods: Cyber-attacks on power grids, transportation systems, or financial institutions.**

**Threat Level: High in critical sectors but less common than other attacker types.**

**(9)**