Chapter-#01

Cyber Security

Cyber Security

- Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber attackers. It is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc.
- It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification, or unauthorized access. Therefore, it may also be referred to as **information technology security.**
- Cyber-attack is now an international concern. It has given many concerns that could endanger the global economy. As the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to take steps to protect their sensitive business and personal information.
- It will cover the most popular concept of Cyber Security, such as what is Cyber Security, Cyber Security goals, types of cyber-attacks, types of cyber attackers, policies, digital signature, Cyber Security tools, security risk analysis, challenges, etc.

Cyber Security

- ## What is Cyber Security?
- 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. We can divide cyber security into two parts one is cyber, and the other is security. Cyber refers to the technology that includes systems, networks, programs, and data. And security is concerned with the protection of systems, networks, applications, and information. In some cases, it is also called **electronic information security** or **information technology security**.
- ## Some other definitions of cyber security are:
- *"Cyber Security is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access."*
- *"Cyber Security is the set of principles and practices designed to protect our computing resources and online information against threats."*

Types of Cyber Security

- Every organization's assets are the combinations of a variety of different systems. These systems have a strong cyber security posture that requires coordinated efforts across all of its systems. Therefore, we can categorize cyber security in the following sub-domains:
- **Network Security:** It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse. This security helps an organization to protect its assets against external and internal threats.
- **Application Security:** It involves protecting the software and devices from unwanted threats. This protection can be done by constantly updating the apps to ensure they are secure from attacks. Successful security begins in the design stage, writing source code, validation, threat modelling, etc., before a program or device is deployed.
- **Information or Data Security:** It involves implementing a strong data storage mechanism to 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.

Types of Cyber Security

- **Operational Security:** It involves processing and making decisions on handling and securing data assets.
- **Mobile Security:** It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats. These threats are unauthorized access, device loss or theft, malware, etc.
- **Cloud Security:** It involves in protecting the information stored in the digital environment or cloud architectures for the organization. It uses various cloud service providers such as AWS, Azure, Google, etc., to ensure security against multiple threats.
- **Disaster Recovery and Business Continuity Planning:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.
- **User Education:** It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data. Its policies dictate resuming the lost operations after any disaster happens to the same operating capacity as before the event.

Importance of Cyber Security

- Today we live in a digital era where all aspects of our lives depend on the network, computer and other electronic devices, and software applications. All critical infrastructure such as the banking system, healthcare, financial institutions, governments, and manufacturing industries use **devices connected to the Internet** as a core part of their operations. Some of their information, such as intellectual property, financial data, and personal data, can be sensitive for unauthorized access or exposure that could have **negative consequences**. This information gives intruders and threat actors to infiltrate them for financial gain, extortion, political or social motives, or just vandalism.

- Cyber-attack is now an international concern that hacks the system, and other security attacks could endanger the global economy. Therefore, it is essential to have an excellent cyber security strategy to protect sensitive information from high-profile security breaches. Furthermore, as the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to use strong cyber security measures and processes to protect their sensitive business and personal information.

History of Cyber Security

- The origin of cyber security began with a research project. It only came into existence because of the development of viruses.
- How did we get here?
- In 1969, **Leonard Kleinrock,** professor of UCLA and student, **Charley Kline,** sent the first electronic message from the UCLA SDS Sigma 7 Host computer to Bill Duvall, a programmer, at the Stanford Research Institute. This is a well-known story and a moment in the history of a digital world. The sent message from the UCLA was the word "login." The system crashed after they typed the first two letters "lo." Since then, this story has been a belief that the programmers typed the beginning message **"lo and behold."** While factually believed that **"login"** was the intended message. Those two letters of messages were changed the way we communicate with one another.
- In 1970's, **Robert (Bob) Thomas** who was a researcher for BBN Technologies in Cambridge, Massachusetts created the first computer worm (virus). He realized that it was possible for a computer program to move across a network, leaving a small trail (series of signs) wherever it went. He named the program **Creeper**, and designed it to travel between Tenex terminals on the early ARPANET, printing the message *"I'M THE CREEPER: CATCH ME IF YOU CAN."*

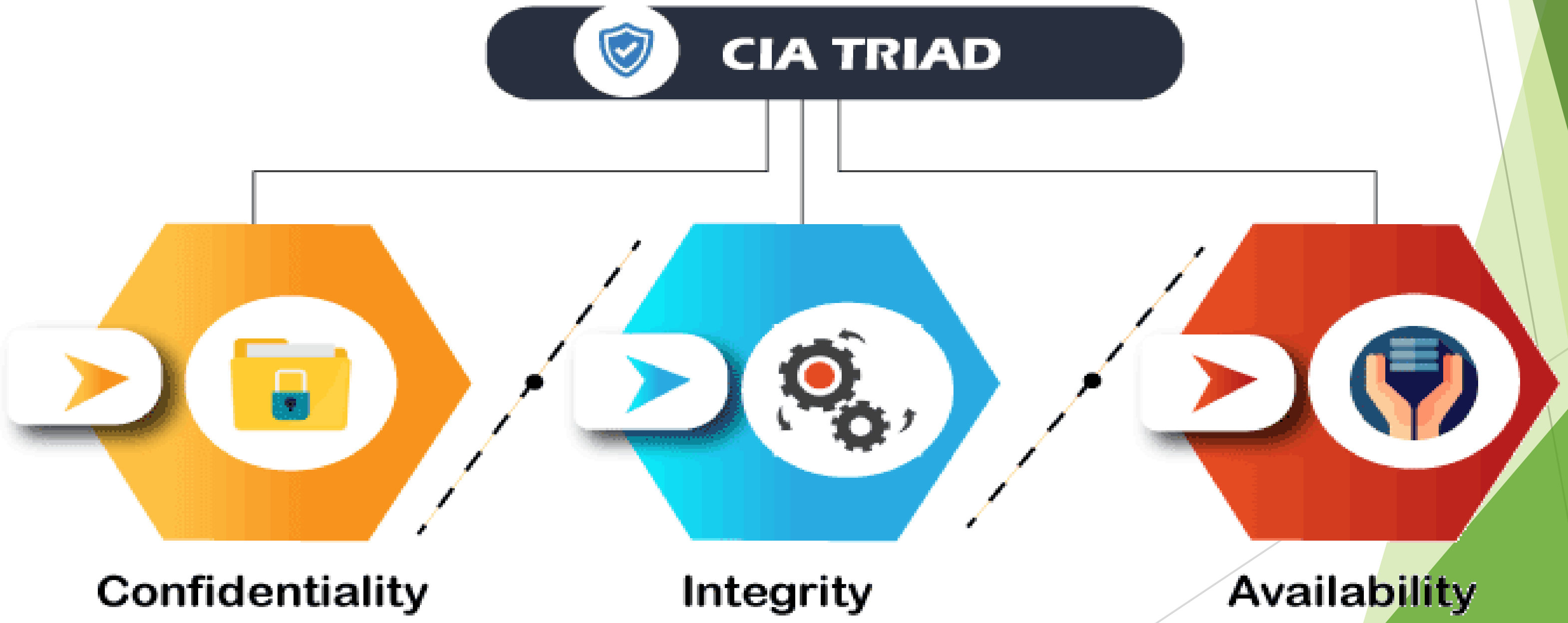
History of Cyber Security

- An American computer programmer named **Ray Tomlinson**, the inventor of email, was also working for BBN Technologies at the time. He saw this idea and liked it. He tinkered (an act of attempting to repair something) with the program and made it self-replicating "the first computer worm." He named the program **Reaper,** the **first antivirus software** which would found copies of The Creeper and delete it.
- **Where are we now?**
- After Creeper and Reaper, cyber-crimes became more powerful. As computer software and hardware developed, security breaches also increase. With every new development came an aspect of vulnerability, or a way for hackers to work around methods of protection. **In 1986**, the Russians were the first who implement the cyber power as a weapon. **Marcus Hess**, a German citizen, hacked into 400 military computers, including processors at the Pentagon. He intended to sell secrets to the KGB, but an American astronomer, Clifford Stoll, caught him before that could happen.

Cyber Security Goals

- 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.** The CIA model is designed to guide policies for an organization's information security infrastructure. When any security breaches are found, one or more of these principles has been violated.

- We can break the **CIA model into three parts:** Confidentiality, Integrity, and Availability. It is actually a security model that helps people to think about various parts of IT security. Let us discuss each part in detail.



Cyber Security Goals

- **Confidentiality**
- Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. **Data encryption** is an excellent example of ensuring confidentiality.
- **Integrity**
- This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.
- **Availability**
- This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.