NASSCOM® FOUNDATION

Directorate General of Training

Powered by Microsoft

Session1-Explain Cyber

Session1-Explain Cyber Security

Describe Information Security and its Basic Principles

What is Information Security?

- Information security covers tools and processes that organizations use to protect information.
- Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction.

Information security principles

- Every element of the information security program must be designed to implement one or more of the following information security principles.

Basic principles of information security

Confidentiality

- Confidentiality measures are designed to prevent unauthorized disclosure of information.
- The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions
- Most systems implement confidentiality through data encryption

Integrity

- Consistency includes protection against unauthorized changes to data.
- The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

Availability

- Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time).
- The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers.

Cyber security

What is Cyber Security?

- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
- The term cyber security refers to both personal and business devices, mobile computing that are connected to the internet.

Information Security and Cyber Security

- Information security differs from cybersecurity in both scope and purpose.
- Cybersecurity primarily addresses technology-related threats, with practices and tools that can prevent or mitigate them.
- The two terms are often used interchangeably, but more accurately, cybersecurity is a subcategory of information security.

Purpose and Importance of Cyber Security

- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems
- To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment
- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.
- To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, etc through effective predictive, preventive, protective, response and recovery actions.
- To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC)
- To develop suitable indigenous security technologies through frontier technology research, solution-oriented research, proof of concept, pilot development, transition, diffusion and

commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

- To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.
- Create workforce of 500,000 professionals skilled in cyber security India in 5years through capacity building, skill development and training.
- To provide fiscal benefits to businesses for adoption of standard security practices and processes.
- To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.
- To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.
- To create a culture of cyber security India and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.
- To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.
- To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

Benefits of having cyber security

- Cyber security helps companies from unauthorized users accessing their network or data. It helps them protect both their end users and their employees.
- Cyber security will help you to keep information, data, and devices private and safe.
- Companies need cyber security to keep their data, finances, and intellectual property safe.
- Individuals need it for similar reasons, although intellectual property is less of a factor, and there is a higher risk of losing important files, such as family photos.

- In the case of public services or governmental organizations, cyber security helps ensure that the community can continue to rely on their services.

List Types of Cyber Security Threats & Their Sources

A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information.

- Malware Attacks
- Emotet
- Denial-of-Service
- Man-in-the-Middle
- Phishing
- SQL Injection
- Password Attacks

Malware Attacks

- Malware is malicious software such as spyware, ransomware, viruses and worms.
- Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software.

The malware once activated, can:

- Block access to key network components (ransomware)
- Install additional harmful software
- Covertly obtain information by transmitting data from the hard drive (spyware)
- Disrupt individual parts, making the system inoperable

Emotet

- The Cybersecurity and Infrastructure Security Agency (CISA) describes Emotet as "an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans.
- Emotet continues to be among the most costly and destructive malware."

Denial of service (DoS)

- A denial of service (DoS) is a type of cyber attack that floods a computer or network so it can't respond to requests.
- A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network.
- Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS.
- Several other techniques may be used, and some cyber attackers use the time that a network is disabled to launch other attacks.

Man-in-the-middle (MITM)

- A man-in-the-middle (MITM) attack occurs when hackers insert themselves into a two-party transaction.
- MITM attacks often occur when a visitor uses an unsecured public Wi-Fi network.
- Attackers insert themselves between the visitor and the network, and then use malware to install

software and use data maliciously.

Phishing attacks

- Phishing attacks use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number.
- "The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine".

Structured Query Language (SQL) injection

- A Structured Query Language (SQL) injection is a type of cyber attack that results from inserting malicious code into a server that uses SQL.
- When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website search box.

Password Attacks

- With the right password, a cyber attacker has access to a wealth of information.
- Social engineering is a type of password attack that Data Insider defines as “a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices.”
- Other types of password attacks include accessing a password database or outright guessing.

Common Sources of Cyber Threats against organizations

- Nation states
- Terrorist organizations
- Criminal groups
- Hackers
- Malicious insiders

Recap:

- Information security covers tools and processes that organizations use to protect information.
- The basic principles of information security are Confidentiality, Integrity, Availability
- Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
- A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information.