CHAPTER 1

INTRODUCTION TO CYBER SECURITY

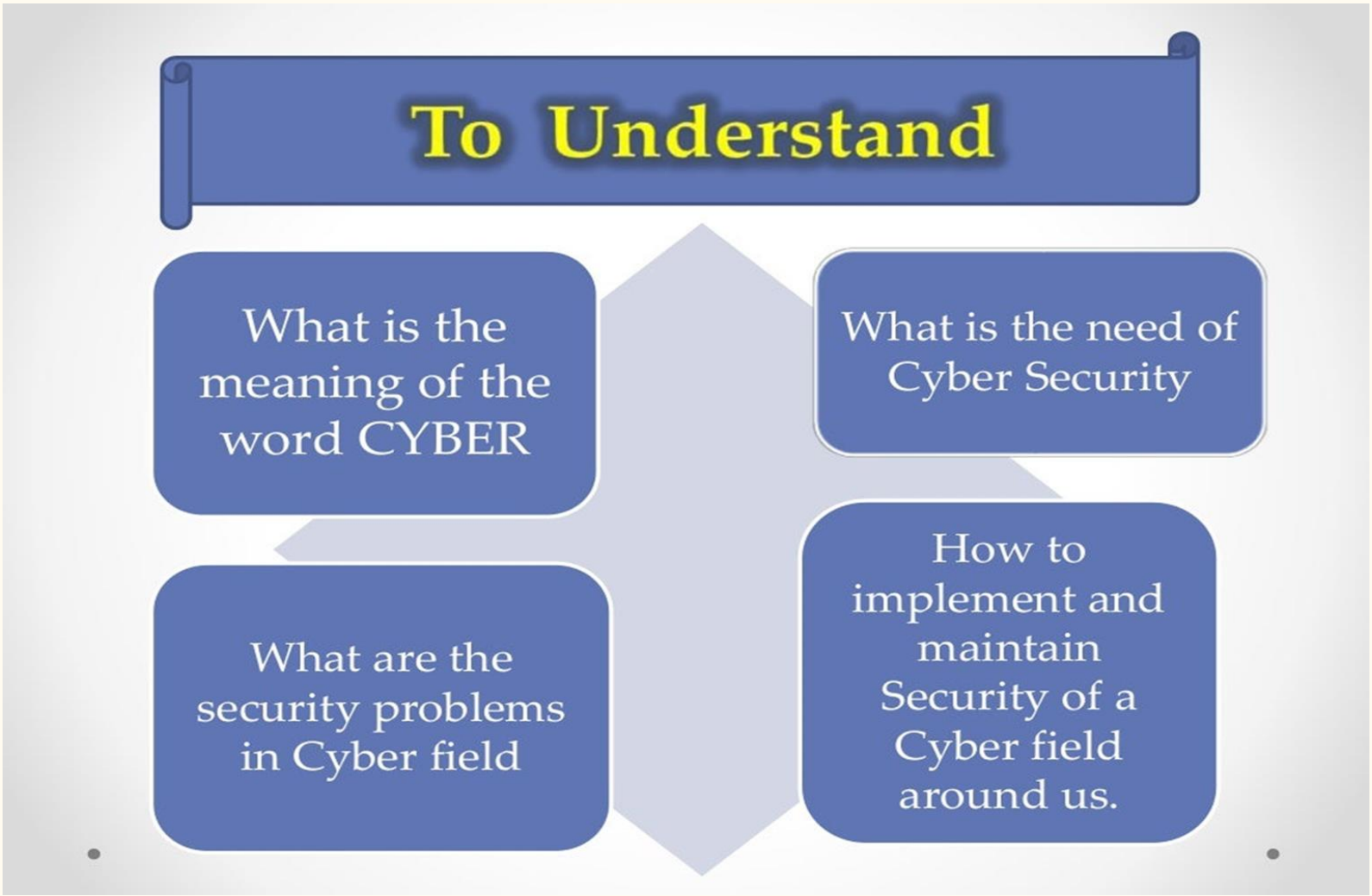
INTRODUCTION

- Internet also has it's own disadvantages - Cyber crime- illegal activity committed on the internet.

- Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals.

- Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks.

- 3 core Principles of Cyber Security:
  - Confidentiality
  - Integrity
  - Availability
- Confidentiality: Sensitive / Confidential - remain & shared - appropriate users.
- Integrity: Integrity in information and not be altered .
- Availability: Information & Systems - available who need it.


To Understand
What is the meaning of the word CYBER
What is the need of Cyber Security
What are the security problems in Cyber field
How to implement and maintain Security of a Cyber field around us.

WHAT IS CYBER?

The meaning of CYBER is of, relating to, or involving computers or computer networks (such as the Internet).

Anything relating to computing, such as the internet, falls under the cyber category.

It's worth noting cyber carries a connotation of a relationship with modern computing and technology.

Need of Cyber Security

Financial services, payments, health services, etc are all connected to digital mediums; and due to Covid-19, this is expected to increase.

There has been a rapid increase in the use of the online environment where millions of users have access to internet resources and are providing contents on a daily basis. To ensure critical infrastructure system do not collapse under any situation.

Why Cyber Security is important?

- There Are Different Types Of Cyber Attacks (Cryptojacking)
- Increase In Cybercrimes
- Tech Users Are Vulnerable
- Cloud Storage Needs Protection
- It Could Save Millions Of Dollars
- Viruses Can Harm You Or Business
- The Dark Web

Ultimately Cyber Security enables **Credibility**

Cyber attacks often make online platforms, like websites, unpleasant or inaccessible. That could result in a bad reputation, which might be difficult to undo. Cyber security is, hence, important for the protection of your platform from such risks. It could also help protect customers from potential hackers.

Types of Cyber attacks

1. DoS and DDoS Attacks
2. MITM Attacks
3. Phishing Attacks
4. Ransomware
5. Password Attacks

And many more attacks....Refer OWASP TOP TEN (2021)

MAJOR CYBER ATTACKS

- **Anthem**

Hackers breached a database that contained 80 million records of current, former customers and employees. The information accessed included names, Social Security numbers, birthdays, addresses, email and employment information, including income.

- **Ashley Madison**

Credit card details – of over 11 million users was leaked.

MEASURES TO PREVENT CYBER ATTACKS

- A cyber countermeasure is defined as an action, process, technology, device, or system that serves to prevent or mitigate the effects of a cyber attack against a computer, server, network or associated device.

1. Use Complex Passwords
2. Limit Access to Critical Data
3. Secure Your Wi-Fi Network
4. Introduce Encryption Software
5. Take Regular Back-up
6. Secure Laptops and Smartphones
7. Impart Cyber Security Policies to Employees

- **TalkTalk**

The mobile phone provider was the target of a bunch of teenage hackers who stole the details of over 20,000 customers.

The company was left with a bill of £35 million, having had millions wiped off its share price, and is facing law suits from customers and investors.

- **EBay**

eBay exposed that the hacking managed to take personal record of 233 million customers.

Data such as phone numbers, usernames, physical addresses, passwords were compromised.

Internet Governance

Internet governance refers to the rules, policies, standards and practices that coordinate and shape global cyberspace.

Internet governance is the complementary development and application by governments, the private sector, civil society and the technical community, in their respective roles, of shared principles, norms, rules, decision-making procedures, and activities that shape the evolution and use of the Internet

Governing Bodies

Internet Society (ISOC): Responsible for development of standards and protocols related to internet

Internet Architecture Board (IAB): Advisory group of ISOC

Internet Engineering Task Force (IETF): Evolution of Internet. Open to all individuals

Internet Engineering Steering Group (IESG): Reviews

Internet Research Task Force (IRTF): Future of Internet

Internet Assigned Number Authority (IANA): IP addresses

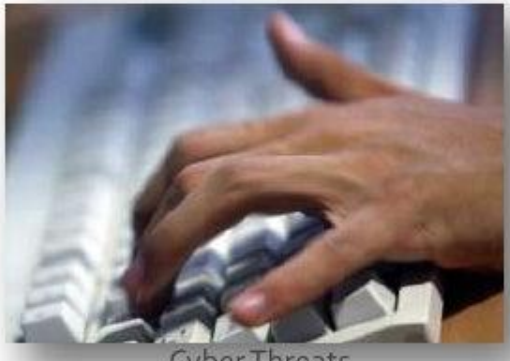
Internet Network Information Center (INIC): Domain Names

World Wide Web Consortium (W3C): For handling websites

Cyberterrorism

"The use of computer networks to shut down critical infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."

(Source: Center for Strategic and International Studies)



Cyber Threats

Cyberwarfare

- Information war

"The use of computers and other devices to attack an enemy's information systems as opposed to an enemy's armies or factories."

(Source: American Heritage New Dictionary)

Types of Cyber Attacks

- **Trojan Horse**: A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.

- **Virus:** A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to affect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.

Types of Cyber Attacks

- **Phishing**: Using emails and websites designed to look like those of legitimate businesses/government agencies to deceive internet users into disclosing personal data, e.g. bank and financial account information and passwords.
- **DoS (Denial of Service)**: A method of attack from a single source that denise system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems of use the internet.

Types of Cyber Attacks

- **Distributed Denial of Service (DDoS)**: A variant of the DoS attack that uses *a coordinated attack from a distributed system of computers* rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.

Examples of Cyber Attacks

Titan Rain (2003+)

- Series of coordinated attacks on US computers
- Thought to be Chinese in origin
- NASA, Lockheed Martin, and other vital organizations penetrated

Examples of Cyber Attacks

Estonia, April 2007

- DDoS attack against Estonian banks, media and government
- Coincided with major civil unrest by Russian nationals

Examples of Cyber Attacks

GhostNet

- Chinese cyberespionage network
- At least 103 countries penetrated
- Searches computers and emails, then turns on webcams and microphones to record any conversations within range

Cyber Espionage

- Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

Examples of Cyber espionage:

- The act of spying.
- The use of spies by a government to learn the military secrets of other nations.
- The use of spies in industry or commerce to learn the secrets of other companies.
- The practice of spying or of using spies to obtain secret information, especially regarding a government or business.

What is a Comprehensive IT Security Policy?

- To ensure that you are effectively protecting your data, you need something that works to prevent breaches, detect potential threats, analyze suspicious activity, and provide remediation in the event that something does occur. **That's where IT security policy comes into play.**

- Guides your organization, ensuring that your data and network is guarded from potential security threats.

- Having IT security policy in place, therefore, should tell your employees what's expected of them, and helps to educate them on safe and secure procedures they should be following.

- Such a policy should encompass a variety of activities, like how your organization's workstations will be configured, how your employees will log in, building access procedures to be aware of, and how your employees should be trained – after all, security breaches at the end-user level can often be prevented if the end-users are aware of safe practices.

Need of Security policies

- It increases efficiency.
- It upholds discipline and accountability
- It can make or break a business deal
- It helps to educate employees on security literacy
- **Virus and Spyware Protection policy**, **Firewall Policy**, **Intrusion Prevention policy** etc are some examples of security policies

Need for a Nodal Authority

The **Indian Computer Emergency Response Team** (**CERT-IN** or **ICERT**) is an office within the Ministry of Electronics and Information Technology of the Government of India. It is the nodal agency to deal with cyber security threats like hacking and phishing.

It strengthens security-related defence of the Indian Internet domain.

Functions of CERT-In

In December 2013, CERT-In reported there was a rise in the cyber attacks on Government organisations like banking and finance, oil and gas and emergency services. It issued a list of security guidelines to all critical departments.

It liaisons with Office of National Cyber Security Coordinator, National Security Council and National Information Board in terms of the nation's cyber security and threats.

As a nodal entity, India’s Computer Emergency Response Team (CERT-in) plays a crucial role under the Ministry of Electronics and Information Technology(MeitY).

Need for an International convention on Cyberspace.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation.