Cyber Security

drishtiias.com/printpdf/cyber-security

According to EY's latest Global Information Security Survey (GISS) 2018-19 – India edition, one of the highest number of cyber threats have been detected in India, and the country ranks second in terms of targeted attacks. Although Banking and Telecom are the most attacked sectors but Manufacturing, Healthcare, and Retail have also faced a significant number of cyber attacks.

- **Cyber Security** is protecting cyber space including critical information infrastructure from attack, damage, misuse and economic espionage.
- **Cyber Space:** A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
- **Critical Information Infrastructure:** According to Section 70(1) of the **Information Technology Act,** CII is defined as a "computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety".
- **Cyber Attack:** It is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization.

Motives behind Cyber Attacks

- To seek commercial gain by hacking banks and financial institutions.
- To attack critical assets of a nation.
- To penetrate into both corporate and military data servers to obtain plans and intelligence.
- To hack sites to virally communicate a message for some specific campaign related to politics and society.

Types of Cyber Attacks

- **Malware,** short for malicious software refers to any kind of software that is designed to cause damage to a single computer, server, or computer network. Ransomware, Spy ware, Worms, viruses, and Trojans are all varieties of malware.
- **Phishing:** It is the method of trying to gather personal information using deceptive e-mails and websites.
- **Denial of Service attacks:** A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
- **Man-in-the-middle (MitM) attacks,** also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.
- **SQL Injection:**
  - SQL (pronounced “sequel”) stands for Structured Query Language, a programming language used to communicate with databases.
  - Many of the servers that store critical data for websites and services use SQL to manage the data in their databases.
  - A SQL injection attack specifically targets such kind of servers, using malicious code to get the server to divulge information it normally wouldn’t.
- **Cross-Site Scripting (XSS):**
  - Similar to an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked.
  - Instead the malicious code the attacker has injected, only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.
- **Social engineering** is an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.

Latest Cases

- **WannaCry**: It was a ransomware attack that spread rapidly in May, 2017. The ransomware locked users’ devices and prevented them from accessing data and software until a certain ransom was paid to the criminals. Top five cities in India (Kolkata, Delhi, Bhubaneswar, Pune and Mumbai) got impacted due to it.
- **Mirai Botnet:** Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots or zombies. This network of bots, called a botnet, is often used to launch Distributed Denial of Service (DDoS) attacks. In September 2016, Mirai malware launched a DDoS attack on the website of a well-known security expert.

Components of Cyber Security

- **Application Security:** It encompasses measures or counter-measures that are taken during an application's development process to protect it from threats that can come through flaws in the app design, development, deployment, upgrade or maintenance.
- **Information security:** It is related to the protection of information from an unauthorized access to avoid identity theft and to protect privacy.
- **Network Security:** It includes activities to protect the usability, reliability, integrity and safety of the network.
- **Disaster Recovery Planning:** It is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of an attack.

Need for Cyber Security

- **For Individuals:** Photos, videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.
- **For Business Organizations:** Companies have a lot of data and information on their systems. A cyber attack may lead to loss of competitive information (such as patents or original work), loss of employees/customers private data resulting into complete loss of public trust on the integrity of the organization.
- **For Government:** A local, state or central government maintains huge amount of confidential data related to country (geographical, military strategic assets etc.) and citizens. Unauthorized access to the data can lead to serious threats on a country.

International Mechanisms:

- The **International Telecommunication Union (ITU)** is a specialized agency within the United Nations which plays a leading role in the standardization and development of telecommunications and cyber security issues.
- **Budapest Convention on Cybercrime:** It is an international treaty that seeks to address Internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It came into force on 1 July 2004. **India is not a signatory to this convention.**
- **Internet Governance Forum (IGF):** It brings together all stakeholders i.e. government, private sector and civil society on the Internet governance debate. It was first convened in October–November 2006.

- **Internet Corporation for Assigned Names and Numbers (ICANN):** It is a non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. It has its headquarters in Los Angeles, U.S.A.

Laws related to Cyber Security in India

Information Technology Act, 2000

- The act regulates use of computers, computer systems, computer networks and also data and information in electronic format.
- The act lists down among other things, following as offences:
    - Tampering with computer source documents.
    - Hacking with computer system
    - Act of cyber terrorism i.e. accessing a protected system with the intention of threatening the unity, integrity, sovereignty or security of country.
    - Cheating using computer resource etc.

Strategies under National Cyber Policy, 2013

- Creating a secure cyber ecosystem.
- Creating mechanisms for security threats and responses to the same through national systems and processes.

    National Computer Emergency Response Team (CERT-in) functions as the nodal agency for coordination of all cyber security efforts, emergency responses, and crisis management.
- Securing e-governance by implementing global best practices, and wider use of Public Key Infrastructure.
- Protection and resilience of critical information infrastructure with the **National Critical Information Infrastructure Protection Centre** (NCIIPC) operating as the nodal agency.

    NCIIPC has been created under Information Technology Act, 2000 to secure India’s critical information infrastructure. It is based in New Delhi.
- Promoting cutting edge research and development of cyber security technology.
- Human Resource Development through education and training programs to build capacity.

Challenges

- Increased use of mobile technology and internet by people.
- Proliferation of Internet of Things (IoT) and lack of proper security infrastructure in some devices.

- Cyberspace has inherent vulnerabilities that cannot be removed.
- Internet technology makes it relatively easy to misdirect attribution to other parties.
- It is generally seen that attack technology outpaces defence technology.
- Lack of awareness on Cyber security.
- Lack of Cyber security specialists.
- Increased use of cyberspace by terrorists.

Recent Steps taken by Government

- **Cyber Surakshit Bharat Initiative:** It was launched in 2018 with an aim to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
- **National Cyber security Coordination Centre (NCCC):** In 2017, the NCCC was developed. Its mandate is to scan internet traffic and communication metadata (which are little snippets of information hidden inside each communication) coming into the country to detect real-time cyber threats.
- **Cyber Swachhta Kendra:** In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.
- Training of 1.14 Lakh persons through 52 institutions under the **Information Security Education and Awareness Project (ISEA)** – a project to raise awareness and to provide research, education and training in the field of Information Security.
- **International cooperation:** Looking forward to becoming a secure cyber ecosystem, India has joined hands with several developed countries like the United States, Singapore, Japan, etc. These agreements will help India to challenge even more sophisticated cyber threats.

Way Forward

- Real-time intelligence is required for preventing and containing cyber attacks.
- Periodical ‘Backup of Data’ is a solution to ransomware.
- Using Artificial Intelligence (AI) for predicting and accurately identifying attacks.
- Using the knowledge gained from actual attacks that have already taken place in building effective and pragmatic defence.
- Increased awareness about cyber threats for which digital literacy is required first.
- India needs to secure its computing environment and IoT with current tools, patches, updates and best known methods in a timely manner.
- The need of the hour for Indian government is to develop core skills in cyber security, data integrity and data security fields while also setting stringent cyber security standards to protect banks and financial institutions.