Cyber Security

Cyber-attack cases have increased significantly; with it, the initiatives have also evolved. Everyone must know the Basics of Cyber Security in India to protect themselves.

- In the 1990s, cyber security initiatives like Anti-virus and firewalls were developed to deal with the virus.
- To deal with Worms in 2020, intrusion detection and prevention initiatives took place
- To resolve Botnets (the 2000s – Present) issues, DLP, Application-aware Firewalls, and SIM were developed
- For APT Insiders (Present), the Network Flow Analysis initiative is taken

Cyber Security: Components

Let’s take a look at the components of Cyber Security.

- **Application Security:** It is the measures taken during the development of an application to protect it from cyber threats.
- **Network Security:** It includes security measures to protect the network's reliability, usability, safety, and integrity.
- **Information Security:** Protecting information from unauthorized access to protect the privacy and avoid theft.
- **Disaster Recovery Planning:** This process includes performing risk assessment, developing recovery plans for attacks, and establishing priorities.

Cyber Security in India

The digital revolution arrived in India a long time ago. Still, it is now that the nation and its citizens have started truly utilizing the transformation through small changes like going cashless, shopping online, etc. However, as mentioned before, with increased technological conveniences, India also faced increased online fraud and cyber security threats.

Hence, in 2013, India introduced the National Cyber Security Policy to build safe and robust cyberspace.

- The policy is an umbrella framework guiding home users, business enterprises, and government and non-governmental entities on appropriate cyber security measures.
- During COVID-19, policies like this have become increasingly important. According to the Data Security Council of India (DSCI), the cybersecurity industry doubled during the pandemic due to rapid digitalization.
- The revenue of the cyber security service industry went from $4.3 billion in 2019 to $8.4 billion in 2021.

How Does Cyber Security Work?

It is recommended to use a top-down approach to cyber security. In this digital era, cyber incidents are truly inevitable. Hence, companies need to protect their holdings and reputation under such circumstances.

The top-down strategy can be developed keeping in mind some important cybersecurity domains. Some of them are:

- **Information Security:** It is a data protection measure to safeguard sensitive information from unauthorized access, theft, and abuse.
- **Cloud Security:** A computing system that encrypts data in storage or moving within the cloud. It also protects the cloud data from unauthorized access.
- **Application Security:** Each organization uses its own set of required applications; hence application security protects the application from off-premises and unauthorized access.

Challenges of Cyber Security

Cyber Security in India faces a lot of challenges which are as follows

- Usage of mobile and internet by people has increased
- Lack of solid security infrastructure in some devices
- Lack of awareness of Cyber Security in India
- Increasing use of cyberspace by terrorists
- Vulnerabilities in cyberspace
- In many cases, the attack technology overpowers defense technology

Cyber Security in India

Here are a few recent initiatives taken by the Government for Cyber Security in India.

Government Initiatives for Cyber Security in India	Motives
Cyber Surakshit Bharat Initiative	Was Launched in 2018 to spread awareness about cybercrimes and build capacity for safety measures for CISOs (Chief Information Security Officers) and frontline IT staff across the govt departments.
National Cyber Security Coordination Centre (NCCC)	It was Launched in 2019 to scan the internet traffic and communication metadata coming into the country to curb real-time cyber threats.
Cyber Swachhta Kendra	This platform was introduced in 2017 for internet users to clear their devices and computer to wipe out malware and viruses
Information Security Education and Awareness Project (ISEA)	Training of 1.14 Lakh people through 52 institutions under this project to raise awareness and provide education, research, and training in the field of Cyber Security
International cooperation	India has joined with several countries like Japan, United States, Singapore to strengthen the cyber ecosystem. It would help India to become better at dealing with cyber threats.

Cyber Laws in India

There are various Cyber Laws in India to protect and prevent such crimes.

Information Technology Act, 2000

- Came into existence in October 2020, also known as the Indian Cyber Act. it provides legal recognition to all e-transactions.
- Information Technology Act 2000 regulates the use of computer systems, computers and computer networks, data, and information in electronic format.
- This Act lists the following as offenses- hacking with a computer system, tampering with computer documents, cheating using computer resources, and an act of cyber terrorism, among others.

National Cyber Policy 2013

The strategies under National Cyber Policy 2013 are as follows.

- To create a secure cyber ecosystem and mechanisms for the security threats and the responses through national processes and systems.

- To secure e-governance by using Public Key Infrastructure and global best practices.
- Protection of critical information infrastructure with the NCIIPC (National Critical Information Infrastructure Protection Centre)
- Human Resource development through training and education programs
- Development of Cyber Security technologies.

National Cyber Security Strategy 2020

The Indian government has planned to implement National Cyber Security Strategy 2020 to secure cyberspace in India.

Cyber Surakshit Bharat Initiative

MeitY collaborated with National e-Governance Division (NeGD) and developed this initiative in 2008 to establish a cyber-resilient IT setup.

Cyber Attacks

A malicious act that aims to destroy data, steal data, or otherwise interfere with digital life is referred to as a cyber security threat. Additionally, it alludes to the potential for a successful cyber attack with the intent of stealing sensitive data, damaging a computer network, or gaining unauthorized access to a computer asset.

Financial systems, air traffic control, and telecommunications are among the industries classified as Critical Information Infrastructure (CII) particularly vulnerable to cyberattacks. It entails stealing intellectual property and money, manipulating and erasing data, etc.

Several prevalent cyber threats include the following types of cyber attacks that have evolved over the years.

- **Malware:** Refers to any kind of software designed only to cause damage to a computer network, computer, or server. Worms, viruses, spyware, and trojans are varieties of malware.
- **Phishing:** This method of gathering personal information using deceptive e-mails and websites.
- **DOS, DDOS:** the attackers make the network or machine unavailable by disrupting the services of the host network.

- **SQL Injection:** Many services that store data of services and websites use SQL to manage their databases. SQL injection attack target such servers by using malicious code to get confidential information.
- **Cyber Espionage:** An important organization's or government's privacy is at risk due to the illegal use of computer networks to capture confidential information.
- **Cyber Warfare:** Attacking information systems using computer technology, especially for military purposes.
- **Social Engineering:** It relies on human interaction to trick users into breaking security procedures to gain the vital information that is protected.