International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Security and Government Initiatives: An Overview

Sujan Kumar Das

Assistant Teacher,76 Balagachhi Primary School, Murshidabad, West Bengal

ABSTRACT

Thorugh this article we are going to discuss about the introduction of cyber security, Indian cyber act, problems regarding cyber security in India, government initiatives taken on cyber security and some steps to overcome cyber crime in India .

In this era of Technology; with the abundant use of computer and internet; cyber crime has become a major problem. Basically we are living in an age of digital era where we can easily perform our work with the help of computer and internet. With the help of internet, man can successfully do their are assignments related to social networking, online shopping, online studying and online jobs.

To Use the boons of computer and internet, most of the countries of the world have given importance on cyber security to protect themselves from cyber crime which is a major threat to the users. Like all the countries of this world; India too has made satisfactory cyber security acts to withstand cyber- crime.

Keywords: Cyber Crime, Cyber security, Ransomware Attack, Phishing, Government Initiatives, Government Regulating Bodies

INTRODUCTION

Work on digital platform and its importance have given many benefits to the people duringan after the Covid-19 pandemic.It has become very important as India has focussed on the Digital India; an initiative taken by the Govt. of India to avail the benefit of Technology. Govt. of India has given priority to the cyber security to protect trade and Commerce of India and also Govt. of Institutions from the damned hand of Cyber crime. To boost cyber security Govt. of India has setup National critical information infrastructure protection centre (NCIPP) and National Cyber Coordination Centre(NCCC). Besides Govt. of India is continuously conducting many awareness campaigns to protect ourselves from cyber- crime or cyber- threat.Due to increasing use of internet and wireless network cyber system has become very important.

CYBER SECURITY

Cyber security is the exercise of protecting network, computer, data and programme from unauthorized access or illegal attack.Differently we may say that cyber security is the system of defending server, computer electronic system, mobile devices, network data and also software from malignant attack.

Cyber security is called the information & Technology security or Electronic security. There are many domains in cyber security from trade and commerce to mobile computing.

The world “Cyber” is related to computer and computer networking.

NECESSITY OF CYBER SECURITY

It is very important to understand the fundamental aspects of cyber security in India.Theincreasing Use of smartphones, Television and internet of things making various devices has made the necessity of cyber security.Photos of someone , Video or data/ information shared by someone in electronic social media may-be unwantedly used by someone else.Government has stored many secret information regarding its own country and the people living in the country. If these are hacked, the country will become helpless.

Many IT sectors preserve abundant informations in their system. If these information are handed over to the cyber- criminals, the sectors will lose the faith of the common people .For this reason the necessity of cyber security is increasing day by day.

CYBER ATTACKS IN INDIA

1. Recently we have seen the ransomware cyber attack of Delhi AIIMS. As a result the personal data of millions of people is in the risk zone.
2. On February 2022, Air India also caught-in a great cyber attack. As a result the records (passport ,ticket ,credit card information) of 4.5 millions of customers were hacked.
3. In 2021, a high profile India based payment companies also faced the cyber attack.
4. It is also reported by Microsoft that during Covid-19 pandemic, phising and ransomware attack happenes in India.
5. In 2020, 82% of Indian company faced the ransomware attack.
6. On may 2017, Five Mega cities (Kolkata ,Delhi ,Bhubaneswar ,Pune and Mumbai) also faced ransomware attack.
7. In 2017, Food Tech company Zomato also stole the data of 17 million of people.
8. In 2016, Union Bank of India also faced phishing cyber attack.

CHALLENGES TO INDIA'S CYBER SECURITY

1.Not everyone in India can buy expensive smartphone due to the wide range of economic level --- All the users of India cannot use expensive devices for data protection. Whereas in U.S.A. 44% of people uses standard i-Phone, but in India it is not more than 1%. As a result we notice a security gap between the standard i-Phone and less expensive phones.

2. Lacks the required infrastructure --- There is a lack of required infrastructure to improve the cyber security awareness in India. Very often, the infrastructure which is mandatory for national security is purchased from the commercial sectors.

Example: The military has its fire fighting organizations while critical infrastructure is owned by commercial sectors.

3. Lack of awareness --- A good Many number of people of India has no clear idea about the cyber crime and cyber security.

4. **Lack of separation ---** Unlike countries or governments, cyber space has no borders ,making it possible for Cyber attacks to come from anywhere on the armed forces, digital assets of ONGC , banking operation etc.

GOVERNMENT INITIATIVES RELATED TO CYBER SECURITY

Some recent initiatives taken by Government for cyber security are -

1.The Information Technology Act, 2000: India's first ever landmark cyber security law was The Information Technology Act 2000. The IT Act of 2000 enacted by the Parliament of India and administered by the Indian Computer Emergency Response Team (CERT-In) to guide Indian cyber security legislation, Institute data protection policies and govern cyber crime. It also protects e - governance, e -banking, e- commerce and private sectors among many others.

2. Information Technology (Amendment)Act 2008: The Information Technology Amendment Act 2008 (IT Act 2008) was passed in October 2008 and came into effect the following year as a substantial addition to the IT Act of 2000.These amendments helped to improve the original bill, which originally failed to pave the way for further IT-related development. It was hailed as an innovative and long-awaited step towards an improved Cyber security framework in India.

3.Information Technology Rules,2011 : Under the IT Act, another important segment of the cyber security legislation is the Information Technology Rules 2011. The most significant amendments include provisions for the regulation of intermediaries,updated penalties and violation fees for cyber crime, cheating ,slander and non- consensual publishing of private images as well as censoring /restriction of certain speech.

4. Indian SPDI Rules, 2011 for Reasonable Security Practices: The IS/ISO/ IEC 27001 regulation are identified by Indian SPDI rules- 2011 as International standards. As such Indian companies aren't obligated but are highly advised to implement these standard which can help meet the" reasonable security practices "under Indian jurisdiction.The rules can also give individuals the right to correct their information and impose restrictions on disclosure data transfer and security measures.

5.National Cyber Security Policy, 2013: In 2013,the department of Electronics and Information Technology released the national Cyber security 2013 as a security framework for public and private organizations to better protect themselves from cyber attacks.

6.Reserve Bank of India Act 2018: The Reserve Bank of India introduced the RBI act in 2018, which deals cyber security guidelines and framework for urban co-operative banks and payment operators.

7. National Cyber Security Strategy 2020: The national Cyber security strategy of 2020 was the long-awaited follow- up plan by the Indian Government to further improve cyber security efforts. The plan's main goal is to serve as the official guidance for stakeholders ,policy makers, and corporate leaders to prevent cyber incidents , cyber terrorism and espionange in cyber space.

8. IT Rules, 2021: On February 25, 2021, the ministry of Electronics and Information Technology introduced the Information Technology Rules, 2021 as a replacement for IT rules , 2011.The new amendments aim to allow ordinary users of digital platforms to seek compensation for their grievances and demand accountability when their rights are infringed upon, as well as Institute additional due diligence on organizations.

9. KYC(know your customers):KYC is the tracking and monitoring of customer data security for improved safeguarding against fraud and payment credentials theft.

MAIN INDIAN CYBER SECURITY REGULATING BODIES

Government of India has set up some cyber security security Regulating Bodies to ensure cyber crime related laws.

A. Computer Emergency Response Team (CERT- IN) : Made official in 2004, the computer emergency response team is the national nodal agency for collecting , analyzing, forecasting, and disseminating non-critical cyber security incidents.

B. National Critical Information Infrastructure Protection Center (NCIIPC) : The National Critical Information Infrastructure Protection Center (NCIIPC) was established on January 16 ,2014, by the Indian government ,under section 70A of the IT Act ,2000 (amended 2008).

C. Cyber Regulation Appellate Tribunal (CRAT) : Under the IT Act 2000, section 62, the Central Government of India created the Cyber Regulations Appellate Tribunal (CRAT) as a chief governing body and authority for fact- finding, receiving cyber evidence ,and examining witnesses .

D. Securities and Exchange Board (SEBI)of India: Established in 1988, the SEBI (Securities and Exchange Board of India) is the regulatory body for securities and commodity markets in India under the Ministry of Finance .

It acts as an executive government entity with satutory power thanks to SEBI act of January 1992.SEBI ensures that the needs of market intermediaries, investors and issuers of securities are met, including safeguarding their data , customer data and transactions.

E. Insurance Regulatory and Development Authority(IRDAI): The Insurance sector of India is regulated by IRDAI, which issues information security guidelines for insurers and addresses the importance of maintaining Data integrity and confidentiality. With the new information and cyber security for insurers guidelines, the IRDAI **:**

(i) Mandates insurance companies to have a CISO (chief information security officer).
(ii) Puts together an information security committe.
(iii) Creates and implements cyber security assurance programs.
(iv) Maintains risk identification and risk mitigation processes.

F. Telecom Regulatory Authority of India(TRAI) and Department of Telecommunications(DOT):TRAI isaRegulatory Body and DOT is separate executive department of Ministry of Communications in India.

Although TRAI has been granted More regulatory powers, both work together to govern and regulate telephone operators and service providers.TRAI addresses data protection with the following objectives:
(i) Define and understand the scope of "personal data, ownership, and control of data "namely, the data of users of The telecom service providers.
(ii) Understand and identify the " Rights and responsibilities of data controllers".
(iii) Identify and adress critical issue regarding data protection.

HOW TO PROTECT YOURSELF FROM CYBER ATTACK

1.Use strong password and two factor authentication.
2.Keep your software and operating system up to date .
3.Use a reputable anti-virus and Firewall program.
4. Be careful about what you click on and download.
5. Don't use public Wi-Fi without a VPN .
6.Backup your data regularly.

CONCLUSION

For the last few decades, India has also witnessed cyber attack like other countries of the world. Growing economy and 1.3 billion people of India are the point of attraction to the cyber criminals. But with the progress of Technology,cyber world has given us many gifts. In this era of Science and Technology, no development is possible without computer, Network device and smartphone.Necessity of Cyber act has become compulsory with the use of internet.Like the two sides of a coin use of Technology has also both good and bad sides. Interdependency on technology has decreased the wastage of time, labour and also various problems of our society providing us speed in our work. During the first decade of 21st century, Govt. of India has introduced thIinformation Technology Act, which that investigates rectifies and Punishes the criminals who are engaged in digital crime ,cyber crime, data theft and so on. Government has now set up many cyber security regulating bodies and trying to aware people about the cyber crime .We hope that right implementation of cyber act will positively and safely Secure our digital data.

REFERENCES

1. Cyber Security (Principles, Theory and Practiess) MAYANK BHUSHAN, RAJKUMAR SINGH RATHORE, AATIF JAMSHED.
2. Dr. SANTOSH KUMAR.Cyber Laws and Crimes- WHITESMANN PUBLISHING CO.
3. Introduction to Cyber Security (Guide to the world of cyber security) ANAND SHINDE.

Web sources

1. https://www.techtarget.com/searchsecurity/definition/cybersecurity
2. https://digitalskills.engin.umich.edu/cybersecurity/introduction-to-cybersecurity
3. https://en.m.wikipedia.org/wiki/Computer_security