Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 01, No. 02, Oct -Nov 2021
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs12.1.7

Cyber Security Is More than Just a Question of Information Technology

Peer Amir Ahmad*

**Department of Political science and Public Administration Research Scholar of Annamalai University Tamil Nadu, India*

*Corresponding Email: *rahieamir786@gmail.com*

Received: 08 July 2021 **Accepted:** 20 September 2021 **Published:** 10 October 2021

Abstract: However, a growing cybercrime threat has been a significant issue for most countries even though information technology plays a vital role in economic and social growth Indian cybercrime has followed a pattern that is similar to the rest of the world in many ways. Regardless of whether the risks originate from inside or outside a company, cyber security measures are designed to protect networked systems and applications. A computer network, hardware, and software are all necessary components of information technology (IT). More specifically, cyber security focuses on securing computers, digital devices, and personal information from illegal access. A company that provides a variety of services linked to the protection of an organization's IT computer systems. To secure your company's sensitive data from illegal electronic access, you need information security, and to protect your company's sensitive data from unauthorised electronic access, you need cyber security. The subject of whether or not cyber security is more than just a matter of information technology is being asked all across the world. Thus, the study's goal is to examine the idea that cyber security is more than just a matter of information technology.

Keywords: Cyber, Technology, Security, Threats, Attacks etc.

1. INTRODUCTION

As society uses computers more, cybercrime has increased. The internet has made man dependant on it for everything. The internet has made man's life easier. The internet allows for online social networking, shopping, education, and employment. Cybercrime differs from other crimes. Cybercrime has no borders and no culprits. It affects the government, industry, and citizens.

The use of ICT in India is boosting cybercrime (ICT). While both IT and cyber security aim to secure people, devices, and data, they focus on distinct concerns and use different approaches. IT stores and shares digital data via computer networks, hardware, and software. Cyber security focuses on preventing illegal access to computer systems, digital

Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 01, No. 02, Oct -Nov 2021
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs12.1.7

devices, and data. Both fields have specialised duties. Working in IT or cyber security means defending people and data against cyber assaults. It is possible to hack into someone's account and steal their data or install malicious software. IT focuses on systems that store and transfer digital data. In contrast, cyber security protects the electronic data contained in those systems.

Cyber security typically targets digital data and infrastructure. Internet connections and local area networks are examples of infrastructure. In short, cyber security prevents hackers from digitally accessing sensitive data on networks, computers, or applications. Job titles in IT and cyber security vary depending on education, experience, and duties. Protecting digital assets and monitoring computer systems and networks requires IT security professionals. They may also protect the data as well as the physical equipment storing it. Information security is concerned with protecting data and systems from illegal access. Some professionals classify cyber security as information security. Professionals in cyber security, information security, and information technology frequently overlap.

Data integrity and security are the focus of information security (InfoSec). In short, information security covers all data types. Create and enforce user, network, and data security policies. Employees in information security educate network users about security issues and requirements. So they can prevent or eradicate future threats. Most people associate cyber security with IT. However, most cyber security occupations protect digital data. Some companies may call these people cyber security specialists or managers. Other cyber security job titles include engineer and administrator. When it comes to projects, IT is often more focused on developing and operating computer networks. Cyber security protects the data within those systems.

Many of the aims of cyber security and IT are similar. These objectives protect digital data and infrastructure from hackers. We rely on technology to conduct our work successfully and efficiently. Cyber security abilities involve handling internet dangers and analysing, storing, and regulating user access. Soft skills include collaboration and critical thinking.

2. RESEARCH OBJECTIVES

- To analyse and shed detailed light on cyber security is a matter of concern for India and study demonstrate on challenges and possible Suggestions.

Methodology

When it comes to supporting its claims, the article is both descriptive and analytical in nature. It makes extensive use of secondary sources to do so, including newspaper articles, magazine articles, and investigation reports, among other things.

Scope of Study

Today's world is more dependent on technology than ever. The benefits of this trend range from near-instant Internet connectivity to modern comforts like smart home automation and

Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 01, No. 02, Oct -Nov 2021
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs12.1.7

the Internet of Things. It's hard to comprehend that behind every device and platform are potential hazards. Despite society's positive opinion of contemporary technology, cyber security concerns are a serious hazard. The increase of cybercrime exposes weaknesses in gadgets and services we rely on. In light of this issue, we must define cyber security and learn about it. Where are we now in terms of cyber security?

3. DISCUSSION

India's need for cyber defence:
Every year, cyber intrusions cost the country a fortune. This is a major factor for cyber security. India has already lost a lot of money, and it will continue to lose money if we do not have effective cyber security regulations. Cyber-attacks are on the rise. So many cyber-attacks. It is critical that we secure our cyberspace. India's digital security has just been exposed. Recent events have shown that cyber security is lacking, and unless we act immediately, this will continue. Destabilizing cyber-attacks can expose governments to hostile attacks, especially in war-torn areas. Cyber strikes can destabilise combat zones. Economic, political, and military costs can result from weak cyber security policy. Cyber education and awareness must grow. Cyber security issues can be avoided by increasing cyber security education and awareness. Attacks can result in loss of life, enormous financial loss, destruction of vital data and information, or even serious harm to the government itself. India must have strong cyber security rules and regulations. Cyber-attacks can be tremendously costly to the country's economy. If the country cannot address these concerns, the economy will suffer and recovery would be difficult. If India wants to reduce cyber-attacks, it must take its cyber security rules and regulations seriously.

There are some Preventive Measures against Cyber Crime like Don’t post any of your personal information online where it can be seen by the public. Disclosing one’s identifying in public is as bad as this. Whenever possible, don't share your personal photos online, especially with strangers or someone you've just met in a chat room. To avoid credit card fraud, never enter your credit card number on an unencrypted page.

Cybercrime is a broad term used to describe illicit activity involving computers or computer networks. Violations of the law, such as child pornography and child kidnapping via chat rooms. It also includes conventional crimes involving computers or networks. Cybercrime is on the rise, and it's trendy to make fake phone calls or steal from others. In the early 1970s, thieves frequently used the phone. They were dubbed Phreaks Cybercrime emerged in the 1980s. Personal data were copied or altered on another's computer. First convicted of cybercrime in 1981 by Captain Zap, Lan Murphy. It was hacked to keep subscribers' free calls during peak hours.

India needs strong cyber security rules. Global cyber security concerns India faces escalating cyber security challenges and must own up to them. According to a recent Economic Times investigation, cyber-attacks cost the government Rs. 1.25L. Cybercriminals prefer India, according to Kaspersky. From February to March 2020, cyber-attacks increased

Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 01, No. 02, Oct -Nov 2021
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs12.1.7

by 3.5 million. Assaults against India totalled 4.6 million in The RBI recently banned MasterCard for not storing payment system data. A cyber-security policy is the greatest way to combat the internet's hazards.

India is the world's second largest Internet market, with 570 million users. By 2023, 660 million people will be online in China. The NCRB documented 29,258 cybercrimes in India in 2019. Telangana had 1209 cybercrimes in 2013. By far the most common cybercrime victim is India. Last year, the central government created cybercrime.gov.in. Cybercrime cost Indian customers nearly $18 billion in 2017. In 2018, the country reported over 27,000 cybercrimes, a 123 percent rise from two years earlier. Cyber stalking, disseminating obscene content, defamation, and hacking are prevalent cybercrimes. Cyber Squatting, Cyber Vandalism, Hacking Computer Systems, Transmitting Virus, Cyber Trespass, Internet Time Thefts, Cyber Warfare, etc. Violations that necessitate.

During 2016-2018, India ranked second in terms of cyber-attacks. India saw a 25% increase in cyber-attacks against IoT deployments. Most IoT attacks this year were in India. India has been cyber-attacked twice in a row! Out of 16 Indian cities, New Delhi and Bengaluru had the highest cyber-attacks. In 2018, 55% of cyber breaches cost companies above $500,000. Data breaches in India have surged 8.9% since 2017. A data breach costs INR 4,652 ($66). India is now the fourth most targeted country globally. Chennai has the most cyber-attacks, according to India Today (49 percent in Q1 2019). No study or warning has changed business cyber security policies. Despite frequent cyber-attacks, many in India are ignorant of lucrative cyber security options. Cyber-attacks recently cost renowned Indian companies millions of rupees.

In 2018, a cyber-attack hit Pune's Cosmos Bank. With impunity, hackers raided the Pune-based Cosmos Cooperative Bank Ltd. Some visa and rupee card numbers were stolen from the bank's ATM server. Money was lost, and hacker gangs from 28 nations hurried to retrieve it.

In mid-2018, Canara bank ATM servers were attacked. Several accounts lost roughly Rs. 20 lakh. Sources said hackers had over 300 ATM users' details, with 50 victims. Skimming devices were used to steal debit card data. It was between Rs 10,000 and 40,000.

There were 1.1 billion Aadhaar card holders in India in January 2018. UIDAI says official Indian government websites posted Aadhaar details online. Cardholders' personal data, including Aadhaar, PAN and cell phone numbers, was included. Unknown marketers were selling Aadhaar data for Rs. 500 via WhatsApp. To get Aadhaar car prints, add Rs 300.

An attack on Indian healthcare websites in 2019 Security experts say hackers broke into a famous Indian healthcare website. An attacker stole 68 lakh patient and doctor data.

A total of Rs 4 crore was transferred from various accounts in August 2018. They emptied many bank accounts. Both attackers deactivated people's SIM cards and utilised stolen SIM card information to undertake online banking activities. They also sought to

Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 01, No. 02, Oct -Nov 2021
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs12.1.7

access company accounts. In the light of recent cyber-attacks in India, all individuals and businesses should take note. Using cyber security measures and following security standards is a must.

India faces cyber security challenges

There are not as many high-end phones in India as there used to be. Apple has more than 46% of the US market. In India, on the other hand, only about 2% of mobile phone users have iPhones with better security. There are too many high-end iPhones and low-cost phones for regulators to set legal and technical standards for protecting data.

This is how it works: The private sector owns important infrastructure, and the military has its own fire departments. However, there isn't a national security architecture that all of these agencies work together to look at threats and respond effectively. The Prime Minister's Office has set up a job for this, but India doesn't have the right structure in place. People can attack the military, ONGC's digital assets and other things in cyberspace from any place because there are no borders. This could lead to national security breaches that could cost money, property, or even lives. To deal with possible threats to the country's most important resources, a well-equipped multi-agency group is needed. People and businesses don't know what to do about cyber security because there isn't a national plan in place. Netizens at home can only be safe from cyber-attacks if there is a legal framework that guides and supervises them.

Suggestions

Employees in India need to be educated on the latest cyber threats through awareness training. In addition, be sure to keep all of your software and systems up to date with the most recent security fixes. India Secure your email domain from email-based cyber assaults by implementing email authentication methods such as DMARC, DKIM, and SPF. Patch and eradicate any existing vulnerabilities in the network or online application via frequent Vulnerability Assessment and Penetration Testing. There must be a Limit the authority of employees to install software and their access to sensitive or confidential data. There must be the use of extremely strong passwords for all accounts, and they must be updated at regular intervals. Also, refrain from disclosing your passwords in the course of your workday. In order for India to adapt to the changing conditions, it is necessary to examine the validity of the IT Act and modify it to fit the current situation.

4. CONCLUSION

There is now a digital age, and cyberspace has spread across the whole world. As a result, cybercrime is on the rise all over the world, especially in India. The most difficult thing about dealing with cybercrime is that it changes all the time because of new technology. As a result, new ways to do cybercrime come up. As a result, cybercrime should be treated as seriously as other forms of crime such as theft, rape, and murder. In India, cyber security is important in a variety of fields. Whether its cyber technology, commerce, legislation, or global internet management, countries like India will need to create much greater levels of national capacity and skill to secure composite national security.

Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 01, No. 02, Oct -Nov 2021
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs12.1.7

Young India should be more aware of this perspective and give this sector the respect it deserves. Secure ICT protects confidential data from unauthorised access, use, modification, loss, or disclosure. Access to confidential information must be constantly managed. Secure data communication Data should be stored and discarded securely. With its vast IT workforce, the government must emphasise on strategic goals. Government incentives to business would stimulate investment in a national cyber security agency. In the future, increased cyber security will help Indian businesses compete globally and contribute to a more secure digital India.

Acknowledgement
I would like to express my heartfelt gratitude to everyone who gave me the opportunity to complete this paper. A special thanks to my friend **Dr. Showkat Ahmad from Handwara Kashmir,** whose dedication, dynamic ideas and consolation aided me in planning my article in a period bond way. Furthermore, I would like to express my gratitude to all of the researchers who had effectively summarised their papers on a similar topic. Their citations and references helped me a great deal in finishing my article in a fruitful way.

Conflict of interest
No Potential conflict was reported by the Author

Funding
Nil

5. REFERENCES

1. Agarwal, V. K., Garg, S. K., Kapil, M., & Sinha, D. (2014). Cybercrime investigations in India: rendering knowledge from the past to address the future. In ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II (pp. 593-600). Springer, Cham.
2. Bhatt, S. C., & Pant, D. (2011). Cyber Crime in India. International Journal of Advanced Research in Computer Science, 2(5).
3. Chaturvedi, M. M., Gupta, M. P., & Bhattacharya, J. (2008). Cyber security infrastructure in India: a study. Emerging Technologies in E-Government ‘, CSI Publication.
4. Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020, March). A technical review report on cybercrimes in India. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 269-275). IEEE.
5. Ghate, S., & Agrawal, P. K. (2017). A literature review on cyber security in Indian context. J. Comput. Inf. Technol, 8(5), 30-36.
6. Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).
7. Gunjan, V. K., Kumar, A., & Avdhanam, S. (2013, September). A survey of cybercrime in India. In 2013 15th International Conference on Advanced Computing Technologies (ICACT) (pp. 1-6). IEEE.

Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 01, No. 02, Oct -Nov 2021
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs12.1.7

8. Kandpal, V., & Singh, R. K. (2013). Latest face of cybercrime and its prevention in India. International Journal of Basic and Applied Sciences, 2(4), 150-156.
9. Kesharwani, S., Sarkar, M. P., & Oberoi, S. (2019). Cyber security in India: threats and challenges. Cybernetics, 1(2), 32-34.
10. Kshetri, N. (2016). Cybercrime and cyber security in India: causes, consequences and implications for the future. Crime, Law and Social Change, 66(3), 313-338.
11. Kshetri, N. (2016). Cybercrime and cyber security in India: causes, consequences and implications for the future. Crime, Law and Social Change, 66(3), 313-338.
12. Kumar, P. V. (2016, March). Growing cybercrimes in India: A survey. In 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE) (pp. 246-251). IEEE.
13. Kumar, V. A., Pandey, K. K., & Punia, D. K. (2014). Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. Energy policy, 65, 126-133.
14. Mishra, S., Dhir, S., & Hooda, M. (2016). A Study on Cyber Security, Its Issues and Cyber Crime Rates in India. In Innovations in Computer Science and Engineering (pp. 249-253). Springer, Singapore.
15. Shah, P., & Agrawal, A. (2020). Cyber security behaviour of smartphone users in India: an empirical analysis. Information & Computer Security.
16. Shrivastava, G., Sharma, K., Khari, M., & Zohora, S. E. (2018). Role of cyber security and cyber forensics in India. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 143-161). IGI Global.
17. Shukla, S. K., & Agrawal, M. (Eds.). (2020). Cyber Security in India: Education, Research and Training (Vol. 4). Springer Nature.
18. Singh, N., & Rishi, A. (2015). Pyramid: A case study of cyber security in India. South Asian Journal of Business and Management Cases, 4(1), 135-142.
19. Speer, D. L. (2000). Redefining borders: The challenges of cybercrime. Crime, law and social change, 34(3), 259-273.
20. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178-188.