NJESR/ March-2023/Volume-5/Issue-3 E-ISSN-2582-5836
DOI-10.53571/NJESR.2023.5.3.25-31

Cyber Security Challenges for India

Dr.M.Ramana
Assistant Professor
Osmania University
Hyderabad
Telanagana

(Received:15Feburary2023/Revised:26Feburary2023/Accepted:10March2023/Published:18March2023)

Abstract

The present work is an attempt to propose the cyber security challenges that the country India is facing currently. India is currently the second largest nation in terms of the number of internet users next to China. Also, the country has been ranked 4th next to the USA, UK, and China concerning the number of research publications in the field of cyber securities (Rai et al, 2019, Statista, 2020). Nevertheless, India has seen 52, 974 cases in 2021 which is 5% more than the year 2020 which has seen 50,035 cases that were filed as cybercrimes (NCRB, 2022). These figures are mounting each year. This must be given careful consideration since India has been suggested to be lacking strong defensive mechanisms to face cyber-crimes compared to the technically sound western nations and Asian giant China. There must be some contextual reasons and concerns that are affecting India to put up a strong and effective fight against national cybercrimes. Thus, the present study is aiming to identify the cyber security challenges that India is facing currently and the reasons for India being not so effective at controlling the rate of cyber-crimes in the nation, to assist the key stakeholders involved with cyber security and cyber forensics in India.

Introduction

Web technologies and trends and updates in the world of web-based technologies have revolutionized human lives. Today the world wide web has become a prominent medium of operations for organizations from different backgrounds. The Internet way of doing things not only can be seen among organizations for organizational purposes, but it is also found among individuals for various purposes. A vast amount of research relating to web technologies and IOT are being conducted all over the world to identify new ways to exploit them to create opportunities and wealth for promoting individual and organizational growth. Nevertheless, these

organizations and people's dependence on the internet and web technologies have opened doors to new means of artifice. Cyber crimes are becoming more threatening each year and new trends and upgraded ways of cyber fraud are being instigated every day. No country is free from these cyber-attacks and statistics of cybercrime are extremely intimidating. It has been suggested that cyber-attacks have risen by over 125% in 2022 compared to 2021 (AAG, 2022) and cyber-crimes have cost over 6 trillion dollars in 2022 and are expected to reach 10 trillion by 2025 (Purpplesec, 2022). For these reasons, nations all over the world are taking precautions to ensure the employment of the right security mechanisms to be able to defend their people and businesses from these cyber crimes. Technologically advanced nations such as the USA and UK are ranked among the top in terms of cyber-attacks along with India which is considered to be a developing nation with regards to web-based technologies. This indeed suggests the vulnerability of India being a nation that is not fully developed technologically and is being largely threatened by cyber-attacks. Being the second largest country of Internet users and 49th on the cyber security index (NCSI, 2022) India must consider taking initiatives to protect its citizens and economy from the most feared crimes in recent days, which are cyber frauds and violations. The present work will highlight the major challenges that the country India is currently facing in to fight against cyber-attacks and reduce cyber-crimes that are rapidly growing.

To give the readers a better understanding of this work, this section of the work will introduce cyber security and various forms of cyber threats. Cyber crimes have been referred to as any criminal activity in which computers or computer networks are a tool, target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks (Goyal, 2012). The existing literature has suggested that cyber-attacks could be of different forms. Here comes the necessity of cyber-security as it can protect individuals and organizations from those fraudulent activities. Cyber-security refers to the precautionary measures that are intended to protect computers and computer networks from cyber-criminals and cyber-security could be broadly categorized into three types namely network security, data security, and system security (Ghate and Agarwal, 2017). Since people and organizations today are using the web and web applications for various purposes to get benefits and improve opportunities for their well-being, this has been attracting the attention of cyber-criminals to conduct some kind of fraudulent activity over the Internet with these people and organizations (Mehta et al., 2013, Karali et al., 2015). Unlike usual crimes, the cyber-crimes are sometimes hard to track and in

some cases it's impossible. This has further raised cyber crimes all over the globe, specifically in developing nations such as India where there are no strong defensive mechanisms to face such crimes. India has been noted as one of the top nations regarding the rate of cybercrime activities. Furthermore, the existing literature has strongly suggested the feeble status of the Indian cyber-security environment and its practices (Kshetri, 2016; Paul and Aithel, 2019; Rai et al., 2019; Datta et al., 2020). Thus, the present work highlights the major cyber-security challenges that India is facing. In a way, the present work presents the current status of cyber-security and its effectiveness in dealing with the cyber-crimes in the country.

Infrastructural Challenges

India is witnessing considerable developments in the field of ICT. With the developments of ICT in India, in addition to the opportunities (Maiti et al., 2020), the rate of cyber crimes has also gone up and is one of the critically threatening challenges that question the effectiveness of ICT infrastructure in India (Paul and Aithal, 2018; Shairgojri and Dar, 2022). It has been strongly recommended that to protect the ICT infrastructure in any country or region, one must develop a strong cyber-security infrastructure which provides opportunities to build effective defence mechanisms to protect the nation from cybercrimes (Chaturvedi et al., 2008; Chaturvedi et al., 2014). Nevertheless, fighting cybercrimes involves building effective mechanisms and practices to defend an organization or individuals from any kind of cybercrime. But predicting any such crimes in advance would give a higher hand against the cyber criminals, and is only possible with stronger ICT infrastructure and policies that can support and strengthen the cyber-security infrastructure (Ghate et al., 2017). The existing literature does strongly suggest that the Indian ICT and Cyber-security infrastructures have largely failed in anticipating such cyber-crimes to help the nation with its fight against the cyber-crimes. This can be seen as a major challenge for India as one of the leading users and contenders in the global ICT ecosystem. This is also the major reason for India being not able to put up a strong fight against cyber crimes constructively. The socioeconomic developments in the country have surely resulted in greater associations of citizens of India with web-based technologies and applications for both individual and organisational purposes. Furthermore, the rapid urbanization in the country has resulted in the wider and deeper spread of Internet access to even the remote areas of the country. This has indeed further improved the growth in cybercrimes since the majority of the users are not very familiar with them (Mokha and Kaur, 2017; Paul et al., 2018; Datta et al., 2020). Thus, this lack

of people's awareness of the trends in cybercrimes has posed another challenge for India in its fight against cybercrimes. This also motivates cyber criminals to improve their activities since a considerable amount of the users are not familiar with the ways of protecting themselves from these cyber criminals. Thus, the aforementioned two main contextual reasons are downgrading the country India when it comes to its fight against cybercrimes.

Concerns Related To Governance And Policy Making

The legal environment of India, specifically the laws relating to cyber crimes has a great role to play in the fight against the cyber-crimes in the country. There is a considerable amount of research that has studied the effectiveness of cyber laws in dealing with the cyber-crimes in India. Observing the present state of criminal laws in the area of cyber-security in India, one can say that the government of India has been underrating the negative impacts of cyber-crimes on citizens. The Information Technology Act, 2000 of India which is suggested to be the Indian legislation for fighting cyber crimes, has been suggested to be incompetent in dealing with the number of fraudulent activities taking place currently in the nation (Jain and Chaudhary, 2019). Compared to the US legislation relating to cyber-security, the Indian cyber-law ecosystem seemingly is not so effective considering the number of criminal activities in the country. Despite the strong suggestions to implement strict rules to promote the cyber-legislation from the research world (Blythe, 2006), the Indian government seemingly failed to consider any such suggestions from existing literature, and the results can be seen in the form of a rapidly growing cyber-crime rate every year in India. Furthermore, the amendments that were made to the act to match the growing number of cyber crimes in the nation are not so effective and are not matching with the latest trends in the cyber-crime environment (Mohanty, 2011; Kalia et al., 2017). This needs to be changed and must require careful consideration. A developing nation such as India which has a population of over a billion people and has a larger number of internet users and activities, operating with less-effective cyber-legislation can not be useful in the long run. Also, it could result in serious problems if not given serious consideration to improving the effectiveness of cyber laws to reduce cyber crimes and strengthen the cyber-security and ICT infrastructure in India. The policymakers that are responsible for changes in cyber legislation in India must consider these issues and should take measures to strengthen the cyber securities in India.

Conclusion

The present work has highlighted the major challenges that the Indian cybersecurity ecosystem is facing currently. The challenges have been presented separately in the work. The challenges are classified as concerns relating to the ICT and user infrastructure and concerns relating to Indian cyber laws. The incompetence of Indian ICT and cyber security infrastructure is one of the reasons for the growth in the rate of cyber crimes in the country. Something must be done to improve the robustness of both infrastructures and the focus should not be restricted to chasing cyber crimes and criminals but rather anticipating their activities. Secondly, the work has highlighted the necessity of improving user awareness of cybercrimes. Finally, the cyber laws of India must be carefully upgraded to match the current cyber crimes in the country. The laws relating to cybercrimes must bring changes to the behaviour of cybercriminals. For this, the laws must be toughened and must create a sense of freight among cybercriminals.

References

- Suggestions to focus more on preventive and defensive mechanisms for Indian context have been recommended : Rai, S., Singh, K., & Varma, A. K. (2019). Global research trend on cyber security: A scientometric analysis. *Library Philosophy and Practice (e-journal), 3339.*
- Blythe, S. E. (2006). A critique of India's Information Technology Act and recommendations for improvement. *Syracuse J. Int'l L. & Com.*, *34*, 1.
- Chaturvedi, M. M., Gupta, M. P., & Bhattacharya, J. (2008). Cyber security infrastructure in India: a study. *Emerging Technologies in E-Government ', CSI Publication*.
- Chaturvedi, M., Singh, A. N., Gupta, M. P., & Bhattacharya, J. (2014). Analyses of issues of information security in Indian context. *Transforming Government: People, Process and Policy*, *8*(3), 374-397.
- Curtis, P., Mehravari, N., & Stewart, K. Evaluating and Improving Cybersecurity Capabilities of the Electricity Critical Infrastructure.: use for some established cyber security models and their applications.
- Chudasama, D., & Rajput, N. (2021). Protecting ourselves from digital crimes. *National Journal of Cyber Security Law*, *4*(1), 1-6.
- Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020, March). A technical review report on cyber crimes in India. In *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 269-275). IEEE.

- Ghate, S., & Agrawal, P. K. (2017). A literature review on cyber security in indian context. *J. Comput. Inf. Technol*, *8*(5), 30-36.
- Goyal, M. (2012). Ethics and cyber crime in India. *International Journal of Engineering and Management Research (IJEMR)*, *2*(1), 1-3.
- Jain, M. J., & Chaudhary, M. R. (2019). Understanding the concept of cyber crimes in India Vis-a-Vis cyber laws of USA. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, *6*(2), 427-438.
- Kalia, P., Arora, R., & Law, P. (2017). Information technology act in India: E-commerce value chain analysis. *Kalia, P., Arora, R. and Law, P.(2016),"Information Technology Act in India: e-Commerce value chain analysis", NTUT Journal of Intellectual Property Law and Management*, *5*(2), 55-97.
- Karali, Y., Panda, S., & Panda, C. S. (2015). Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India. *International Journal of Engineering and Management Research Page Number*,*(5)*, 43-48.
- Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, *66*(3), 313-338. Weaknesses of indian cyber security infra
- Mokha, A. K. (2017). A study on awareness of Cyber Crime and security. *Research Journal of Humanities and Social Sciences*, *8*(4), 459.
- Paul, P., & Aithal, P. S. (2018). Cyber crime: challenges, issues, recommendation and suggestion in Indian context. *International Journal of Advanced Trends in Engineering and Technology.(IJATET)*, *3*(1), 59-62.
- Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, *66*(3), 313-338.
- Maiti, D., Castellacci, F., & Melchior, A. (2020). Digitalisation and development: issues for India and beyond. In *Digitalisation and Development* (pp. 3-29). Springer, Singapore.
- Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, *12*(9), 157. : Cyber risk management and cyber securities
- Mehta, S., & Singh, V. (2013). A study of awareness about Cyber Laws in the Indian Society. *International Journal of Computing and Business Research*, *4*(1), 1-8.

- Mohanty, A. (2011). New Crimes under the Information Technology (Amendment) Act. *Indian JL & Tech.*, *7*, 103.
- Shairgojri, A. A., & Dar, S. A. (2022). Emerging Cyber Security India's Concern and Threats. *International Journal of Information Technology & Computer Engineering (IJITC) ISSN: 2455-5290*, *2*(04), 17-26.
- Global rankings,https://ncsi.ega.ee/ncsi-index/ (accessed on 28/11/2022)
- Global cyber crime statistics, 2022,https://aag-it.com/the-latest-2022-cyber-crime-statistics/#:~:text=Cyber%20crime%20statistics%20worldwide%202022,a%2013%25%20decrease%20over%202020.
- Cyber security stats, 2022,https://purplesec.us/resources/cyber-security-statistics/#:~:text=The%20global%20annual%20cost%20of,than%20it%20was%20in%202015.
- Cyber security rankings, 2020,https://www.statista.com/statistics/733657/global-cybersecurity-index-gci-countries/