International Journal of Information technology and Computer Engineering
ISSN: 2455-5290
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/IJITC
DOI: https://doi.org/10.55529/ijitc.24.27.34

Framework and Challenges of Cyber Security in India An Analytical Study

A. Panneerselvam*

**Research Scholar of Political science Department of Political science Annamalai University Tamil Nadu, India.*

Corresponding Email: *selvampaneera@gmail.com

Received: 26 March 2022 **Accepted:** 10 June 2022 **Published:** 15 July 2022

***Abstract:** Cyber security threats come in a wide variety of forms, including ransomware, phishing, malware attacks, and many others. India is currently ranked 11th in the world in terms of the number of local cyberattacks and it has already experienced 2,399,692 of these incidents in the first three months of 2020. Because cyber security is a topic that is growing more and more essential, businesses are undoubtedly well aware of the hazards and threats that hackers offer to their corporation. However cybersecurity would continue to be a difficult issue for three reasons: It goes beyond a simple technological issue. Cyberspace operates under a distinct set of regulations than the real world. Law, policy, and practise in the area of cybersecurity are still in their infancy. Every firm requires a security analyst to ensure that their system is secure given the rise in cyber-attacks. These security analysts must secure private company servers; protect the confidential data of governmental organisations, and other cybersecurity-related difficulties. Research indicates that there is a significant need in India for qualified cybersecurity specialists and that this demand will continue to rise in the near future. Employers anticipate a scarcity of qualified cybersecurity specialists. The goal of the study is to analyse and explain India's cyber security framework and difficulties. The study used a combination of descriptive and analytical method to draw a result. The Thematic software tool QADMAX also used in the study to analyse the qualitative data for secondary sources*

***Keywords:** Cyber; Challenges; Laws; Security; Threats.*

1. INTRODUCTION

How much people with web access is continually filling in India. India is at present the world's second-biggest web market notwithstanding its neglected potential. Albeit the improvement of innovation and the web enjoys every one of the related benefits, it has likewise brought about an ascent in cyber crime that influences individuals from one side of the planet to the other. The Pegasnus snoonping (Economic Times 2022) scandal and the Wana- cry assault have both featured how weak India is to risks from cyber crime. The nation positions second on the planet for designated assaults, as per EY's latest Global Information Security Survey (GISS) 2018-19 - India version, and has one of the biggest quantities of cyber threats recognized. Albeit the most often designated businesses are banking and media communications, assembling, medical services, and retail have likewise seen a sizable number of cyber attacks Protecting data, networks, and other information from illegal access, partial or complete destruction, or alteration is the (Al-Daeef 2017) essence of cyber security. Because we all have online presences, cyber security can play a significant part in our daily lives. "A reputation takes twenty years to establish, and only a few minutes of a cyber incident can destroy it." This assertion accurately depicts how vulnerable we are to security risks and online attacks. Many businesses are creating various forms of software to protect data in the modern environment. In the modern era, cyber security is essential since it protects not only our systems from viral attacks but also helps to secure information. The fact that we have such a large user base—India has the third-highest number of internet users, behind the United States and China—makes it crucial. Cyber threats can be divided into two categories: cybercrime, which typically targets businesses or individuals, and Cyberwarfare, which targets states or entire nations.

Cybercrime is the use of a computer, the internet, a cellphone, or other technological devices by an individual or a group to (Drishti 2020) commit a crime. Hackers perpetrate cybercrime by using a variety of programmes and scripts. In India, hacking has grown to be one of the biggest problems. (Showkat Naseer Ahmad 2020)

The process of locating and exploiting vulnerabilities in the security of a computer system or network in order to obtain unauthorized access to sensitive or private information is known as hacking. Hacking has emerged as one of the most pressing issues in India in recent years. The process of locating and exploiting vulnerabilities in the security of a computer system or network in order to obtain unauthorized access to sensitive or private information is known as hacking. Malware is a type of (Saudi, M. M. (2017). malicious software that is regularly utilized by hackers. Malware typically takes the form of computer codes and other programmes like worms and adware. It is possible that it will access a personal computer or collect sensitive data. It is plausible to foresee, given the potential of cyber threats, that future conflicts would not be waged on land or in the air but rather through the deployment of cyberattacks. This is one of the implications of the rise of Cyberwarfare. According to data provided by the National Crime Record Bureau, there were only 550,055 instances of cybercrime that were reported in the year 2020 in a nation that aspires to have a digital economy worth $1 trillion and around 80 crore Internet users (NCRB 2020). Because of this, India needs comprehensive regulations and standards for its cyber security.

2. LITERATURE REVIEW

01	Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017).	Security awareness training: Areview. Lecture Notes in Engineering and Computer Science.
02	Abawajy, J. (2014	User preference of cyber security awareness delivery methods. Behavior & Information Technology
03	Alnasser, A., Sun, H., & Jiang, J. (2019)	Cyber security challenges and solutions for V2X communications: A survey.
04	Reddy, G. N. & Reddy, G. J. (2014	A study of cyber security challenges and its emerging trends on latest technologies
05	Tonge, A. M., Kasture, S. S., & Chaudhuri, S. R. (2013)	Cyber security: challenges for society-literature review

3. RESEARCH OBJECTIVES

➢ To explain and analyze the various threats and challenges to cyber-security in India and initiatives, laws are being taken by the government to enhance cyber security in India.

4. METHODLOGY

In light of the recent study, both research approaches—ex post facto and analytical—are relevant. As a result of this, the study can be classified as both analytical and descriptive. During the course of the study, both primary and secondary sources were utilized. MAXQDA, a tool for theme analysis, was used to conduct a qualitative study of the secondary data. Books, websites, articles from newspapers, a variety of Indian reports, and a number of other international periodicals and magazines were the secondary data sources thatwere utilized.

5. DISCUSSION AND RESULT

Causes and Reasons for Cyber Attacks

- To pursue financial advantage through the illegal hacking of financial institutions and banks.
- To launch an assault on vital aspects of a nation's infrastructure.
- To break into corporate as well as (Dunn Myriam (2005) military data servers in orderto gain plans and intelligence.
- To break into websites in order to spread an idea by word of mouth for the sake of some specific political or social campaign.

a. Need for Cyber Security

Individuals, businesses, and the government all have a need for cyber security, which may be divided down into three categories: personal, commercial, and government.

A person's images, videos, and other personal information can be misused by others on social networking sites, which (Alnasser 2019) can result in significant or even life-threatening consequences.

Companies often keep a vast amount of data and information in their systems. Competitive information (such patents or original works), private data belonging to employees or customers, and public trust in the integrity of the firm can all be lost in a cyber attack. (Kshetri, N. (2016)

Each of the three levels of government (municipal, state, and national) maintains a large amount of sensitive information about their respective countries and their inhabitants. There are serious consequences (Alnasser 2019) for the nation if the data is improperly accessed.

There are many different dangers and obstacles to cyber security in India.

Cyber terrorism is an attack that is premeditated and driven by political motivation against information, computer systems, computer programmes, and data. This attack results in physical harm. The danger posed by digital data, the increasing volume of business conducted online has provided more opportunities for cybercriminals. Establishments not only produce intellectual property that is in and of itself a desirable target, but they also actively seek to mine data, which might include information on customers, the outcomes of product surveys, and information about the market in general. Cyber warfare is when a nation-state or (Tonge 2013) an international organization launches an attack on the computers or information networks of another nation with the intention of causing damage to such systems.

The Concerns Regarding the Cyber Infrastructure, the vast majority of pieces of machinery and information technology systems are susceptible to cyber attacks, just like any other connected system. Despite the fact that the government has established the National Critical Information Infrastructure Protection Centre (NCIIPC), it has not yet determined and put into effect any measures to protect critical information infrastructure. A deficiency of qualified experts India is at present positioned second on the planet, behind just China, as far as the quantity (Kasture, S 2013) of individuals who utilize the web (Internet World Stats, 2017). Notwithstanding, when contrasted with the quantity of individuals that utilization the web, India has a tiny base of network protection skill. India's approach to cyber security has been ad hoc and unsystematic up until this point. The country's lack of solid law enforcement mechanisms is the sixth problem. The execution of these agencies, policies, and projects has not been anything near sufficient, despite the fact that there are a number of them. A Deficitin Coordination, because there are too many agencies in the field of cyber security performing overlapping responsibilities, there is a deficit in the level of coordination that exists between these organisations.

In order to improve the nation's cyber security, the government has enacted a number of frameworks and initiatives, including the following

The Information Act of 2000, as revised in 2008, is India's principal piece of legislation addressing cybercrime and digital trade. The 2013 National Cyber Security Policy is the next step in the process. The policy sets out a vision and outlines a strategy for securing the nation's cyberspace. It's been around since 2004, when the Cyber Emergency Response Team – India (CERT-In) was established. Organizing a response to emerging computer security threats is the (Harknett, R. J., & Stever, J. A. 2011)) responsibility of the government agency in question. This is a decision that has been made by the Union Government. Counter- cybercrime actions will be coordinated from here.

The Cyber Swachhta Kendra site was sent off toward the start of 2017. Digital Swachhta Kendra gives an entry that clients (IAS, F. (2018) might use to sweep and eliminate malware from their machines. The Cyber Surakshit Bharat drive was created by the Ministry of Electronics and Information Technology to improve familiarity with cybercrime and construct the capacity of Chief Information Security Officers (CISOs) and cutting edge IT experts across all government organizations for security measures. CWPF represents the Cyber Warrior Police Force. The organization has expressed that it expects to execute CWPF by 2018. Likewise with the Central Armed Police Force, they will be prepared along these lines (CAPF). The Cyber-Crime Prevention against Women and Children Scheme is managed by the Ministry of Home Affairs. The drive's motivation is to decrease the quantity of (IAS, F. (2018) violations committed against ladies and youngsters however much as could be expected.

Way forward

There is an immediate requirement to construct capabilities and capacity for the testing of applications, equipment, and infrastructure. It is imperative that immediate attention be paid to the development of human resources, which would result in an increase in the number of specialists who are able to successfully manage the nation's cyber security. Making investments in research and development is necessary in order to create more inventive technology to combat (Guru, S. 2021)) the growing number of cyber security threats. It is essential to develop a sound policy and then to put it into effect in an efficient manner. In addition, roles and responsibilities need to be outlined very specifically in order to ensure that everything runs well and that there is adequate coordination between the many departments and parties involved. To make people more aware of the dangers posed by cyber attacks, the government and large business enterprises should run regular awareness campaigns. The public-private relationship in the area of cyber security needs to be strengthened urgently.

6. CONCLUSION

In this day and age, when more and more individuals are connected online, proper cyber security is a necessity. Even if the government has taken a number of preventative measures, there is still a lot of work to be done to improve the nation's cyber-security. Maintaining proper levels of cyber security is one of the most serious challenges in our lives nowadays because of the internet's pervasive influence. We must take steps to ensure the safety of information and communication technology, one of which is the creation of an emergency response team for computers. If you're looking for a way to keep track of all your passwords, there are a number of password management options out there. One approach to avoid beinga victim of a cyberattack is to keep our software up-to-date at all times. It is probable that it will gain private computer systems or sensitive information. Future conflicts may not be waged on the ground or in the air, but rather through cyberattacks. This is a possibility. This is owing to the enormous potential of cyber attacks. Using antivirus software and changing our passwords on a regular basis can help us protect ourselves against cyberattacks. It's also a good idea to change our passwords from time to time. The general public and private businesses must be protected, as well as government organisations, by effective measures of cyber security. Educating the public on the importance of online security is critical for the government and other security organisations. Additionally, computer users should make sure their antivirus software is up-to-date in order to protect themselves against dangerous malware and viruses.

Acknowledgement

Without the help and backing of all of my kindred understudies, the development of this exploration piece could not have possibly been practical. I might want to offer my genuine thanks to every one of the scientists that set forth a ton of hard effort to compose papers associated with the article and who worked with me to plan a system for effectively observing our work. For their endeavors, I am really grateful. I might want to offer my genuine appreciation to every one of you.

Conflict Of Interest Statement

The author affirm that they have no known financial or interpersonal conflicts that would have appeared to have an impact on the research presented in this study.

7. REFERENCES

1. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behavior & Information Technology, 33(3), 237-248.
2. Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. Lecture Notes in Engineering and Computer Science.
3. Alnasser, A., Sun, H., & Jiang, J. (2019). Cyber security challenges and solutions for V2X communications: A survey. Computer Networks, 151, 52-67.
4. Ahmad, P. A. (2021). Cyber Security Is More than Just a Question of Information Technology. Journal of Image Processing and Intelligent Remote Sensing (JIPIRS) ISSN 2815-0953, 1(02), 1-7.
5. Ayofe, A. N., & Irwin, B. (2010). Cyber security: Challenges and the way forward. Computer Science & Telecommunications, 29(6).
6. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? ArXiv preprint arXiv: 1901.02672.

7. Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). Cyber security policy guidebook. John Wiley & Sons.
8. Chaturvedi M.M.,Gupta M.P., Bhattacharya J.(2007),"Analysis of Information and Communication Technology Infrastructure vulnerabilities in Indian context" In J. Bhattacharya(Ed),Towards next generation E- government(PP 192-202) India: Gift Publishing.
9. Chaturvedi, M. M., Gupta, M. P., & Bhattacharya, J. (2008). Cyber security infrastructure in India: a study. Emerging Technologies in E-Government ', CSI Publication.
10. Chock lingam, K. (2003). Criminal victimization in four major cities in southern India. Forum on Crime and Society, 3(1/2), 117–126
11. Drishti. (2019). Cyber Security. Drishti IAS; www.drishtiias.com. https://www.drishtii as.com/to-the-points/paper3/cyber-security.reterived on 12, April 2022
12. Dunn Myriam (2005), "A Comparative Analysis of Cyber security Initiatives Worldwide", Center for Security Studies, Swiss Federal Institute of Technology (ETH Zurich) for the WSIS Thematic Meeting at ITU on Cyber security.
13. Economic Times (2022). Cyber Security: Why India needs strong cyber security norms to curb misuse of VPNs - The Economic Times. The Economic Times; economictimes.indiatimes.com. https://economictimes.indiatimes.com/news/india/why india needs strong cyber security norms to curb misuse of vpns/articleshow/91720342. cms retrieved on 23 June, 2022.
14. Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research, 5(4), 491-497.
15. Eeten, M.J.G. van, Roe, E.M., Schulman, P, Bruijne, M.L.C. de, (2006), "The Enemy Within: System Complexity and Organizational Surprises", in M. Dunn and V. Mayer (Eds), International CIIP Handbook 2006. Vol. II: Analyzing Issues, Challenges, and Prospects, Zurich, Center for Security Studies at ETH Zurich, at , pp. 89–109
16. Guru, S. (2021). Essay on cyber security for UPSC Archives – Study guru Pathshala. Study guru Pathshala; study guru pathshala.com. https://studyguru pathshala.com/tag/essay-on-cyber-security-for-upsc/ retrieved on 23 May,2022
17. Harknett, R. J., & Stever, J. A. (2011). The new policy world of cybersecurity. Public Administration Review, 71(3), 455-460.
18. IAS, F. (2018). Discuss various threats and challenges to cyber-security in India. What initiatives are being taken by the government to enhance cyber security in India? .Forum IAS Blog; blog.forumias.com. https://blog.forumias.com/answereddisc uss-various-threats-and-challenges-to-cyber-security-in-india-what-initiatives-are- being-taken-by-the-government-to-enhance-cyber-security-in-india/ retrieved on 23June, 2022.
19. Internet Crime Complaint Center (2011). 2010 internet crime report. Retrieved fromht tp://www.ic3.gov/media/annualreport/2010_ic3report.pdf.
20. Korpela, K. (2015). Improving cyber security awareness and training programs withdata analytics. Information Security Journal: A Global Perspective, 24(1-3), 72-77.
21. Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security

awareness and education in SA. South African Computer Journal, 52(1), 29-41.
22. Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. Crime, Law and Social Change, 66(3), 313-338.
23. Kshetri, N. (2009). Positive externality, increasing returns and the rise in cybercrimes. Communications of the ACM, 52(12), 141–144.
24. Reddy, G. N. & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. ArXiv preprint arXiv: 1402.1842.
25. Saravade, Nandkumar, (2007), "Cyber Security Initiatives in India", paper presented at ITU conference at Hanoi in August 2007.Director, Cyber Security and Compliance, NASSCOM.
26. Saxena, P., Kotiyal, B., & Goudar, R. H. (2012). A cyber era approach for building awareness in cyber security for educational system in India. International Journal of Information and Education Technology, 2(2), 167.
27. Shapsough, S., Qatan, F., Aburukba, R., Aloul, F., & Al Ali, A. R. (2015, October). Smart grid cyber security: Challenges and solutions. In 2015 international conference on smart grid and clean energy technologies (ICSGCE) (pp. 170-175). IEEE.
28. Shapsough, S., Qatan, F., Aburukba, R., Aloul, F., & Al Ali, A. R. (2015, October). Smart grid cyber security: Challenges and solutions. In 2015 international conference on smart grid and clean energy technologies (ICSGCE) (pp. 170-175). IEEE.
29. Showkat Ahmad Dar & Dr. Naseer Ahmad lone (2020) "Cyber crime in India "Sambodhi UGC Care Journal Vol 43,No 04 ISSN -2249-6661, PP, 118-130.
30. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.
31. Tonge, A. M., Kasture, S. S., & Chaudhuri, S. R. (2013). Cyber security: challenges for society-literature review. IOSR Journal of computer Engineering, 2(12), 67-75.
32. Zhang, Z. J., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. Industrial Management & Data Systems