International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 54-57 ISSN: 2584-2145
www.ijemh.com

"Cybersecurity in India- Challenges and Solutions"

Dr.Sharmasth Vali Y
Assistant Professor
Department of Computer Science & Engineering
Presidency University
Bangalore India

Khandakar Nayeem Rejwan
Student, BTech (Computer Science and Engineering)
Presidency University, Bangalore, India

Date of Submission: 01-05-2024 Date of Acceptance: 09-05-2024

ABSTRACT
India, the most populous country in the world with a population of 1.4 billion (2022), with its burgeoning technical infrastructure which relies primarily on Network and Internet consists of 820 million users faces tough challenges in maintaining the cybersecurity resilience. To citizens, public and private agencies of the country, cyber security matters in their transactions and exchanges over the Internet. The Indian digital economy which encompasses from e-governance to online payments via UPI is prone to serious cyber threats. These threats include cyberattacks targeting government and financial institutions, data breaches affecting private enterprises, and ransomware compromising critical infrastructure. The growing threats are result of diverse issues like the outdated framework, shortage of skilled professionals, lack of awareness among the users among others. This paper dives into some critical challenges faced in the domain of cybersecurity and then explores about how the Government, Organisations and the citizens can work in an coordinated fashion to solve these challenges specific to India.

Keyword: Cybersecurity, vulnerability test,hacking,security breach, digital infrastructure, privacy concern,legal framework,network and internet,cyberbullying, awareness.

I.INTRODUCTION

A cyberattack encompasses a range of malicious activities targeting computer networks and systems, aimed at achieving various harmful objectives.These cyberattacks are designed to steal

sensitive information from individuals, businesses, or government agencies, manipulate or alter critical data, delete or damage records, and disrupt the normal operation of IT infrastructure.The use of smartphones, social media, online banking, e-governance, e-commerce among others are increasing at an exponential rate. The heavily reliance on internet poses a serious threat in the security and the privacy of every user. This again comes with a heavy cost as India is now one of those countries which ranks as one of the most attacked countries in the world the cyberspace from every side. This has brought several challenges to India in various forms. There are various instances of cyberattacks on individual level, various private firms and government institutes. There are also several cases of cyberbullying.

The main motive behind most of the cyberattack is financial. There can be other motives like espionage and data theft to gather intelligence, personal vendettas or revenge, Hacktivism, sabotage or dismantle, cyber warfare etc.. SQL Injection, Ransomware, Phishing, Cross-Site Scripting (XSS), Denial of Service (DoS) and Distributed Denial of Service (DDoS), Malware, Social Engineering, Backdoor Trojan, Internet of Things Attack, Brute Force Attack, Insider Threats, Spoofing, Man-in-the-Middle (MitM) Attack, Zero-Day Exploits, Advanced Persistent Threats, Clickjacking etc. are different types of attacks being carried out the hackers.

The consequences of these attacks are dangerous and can cause a ripple affect of harm beyond the initial target. These attacks can bring devastating consequences can shatter trust, bring the national

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 54-57 ISSN: 2584-2145
www.ijemh.com

security at risk, jeopardise the financial system and at worst cases it can destroy to a limit beyond repair. In order to combat these dangerous attacks we need to be take effective measures. A robust cybersecurity system is paramount for India. The Government of India over the last few years have taken initiatives and strict regulations in this context. National Cyber Security Policy, Indian Cyber Crime Coordination Centre (I4C), Critical information infrastructure (CII), Defence Cyber Agency (DCyA) are few examples of initiatives. For the cybersecurity regulatory framework, The Indian Government passed numerous regulations of which "The Information Technology Act, 2000", "National Cyber Security Policy, 2013", "National Cyber Security Strategy 2020" , "The Digital Personal Data Protection Act of 2023 (DPDP)" are notable ones. At the individual the citizens should be aware of the dangers which can come from a compromised system, the citizens should not disclose the private information. The users should keep their software updates and needs to be careful from malicious mails and other fraudulent activities from adversaries.

II. METHODOLOGY

Different approaches of methodologies have been studied to attain the key findings on the cybersecurityanalysis of India. These methodologies have been systematicallyand comprehensively studied in order to gain and synthesize the relevant information and data.

LITERATURE REVIEWS: The existing academic literature, industry white papers, newspaper articles, government publications are thoroughly studied to get the holistic view of the current state of India's cybersecurity. We have also delved into various industry publications and reports to understand the essence of practical challenges faced in this domain. Through the literature review we have identified the key issues in a broader context. We have also found severe gaps in the cybersecurity awareness among people and also in enforcement of policies where it deserves the attention.

SURVEYS AND DATA ANALYSIS: Another methodology used in this context is surveys and data analysis to understand how common people perceive and experience cybersecurity. Questions were asked to people about what they think about cybersecurity, how much they are aware of the present cybersecurity measures and policies set up by the government, if they have experienced cybersecurity threats or if their family members or friends were victims of such threats.
After completing the surveys, a proper analysis was done on the responses to find common trends and patterns. This analysis provided a brief notion about which type of threats are most common, which age group is more prone to such attacks, what security practices are commonly used.

CASE STUDIES: Some specific case studies related to cybersecurity landscape of India were studied extensively to understand the methods of attacks, the recurring patterns, and the responses of the victims post the attacks. These case studies were chosen to represent a diverse range of sectors, such as government, finance, healthcare, and telecommunications, allowing for a comprehensive analysis of cybersecurity issues across different industries. By analysing these real-world examples, the study aimed to provide insights into the commonalities among various attacks and evaluate the effectiveness of the measures taken to mitigate the risks and minimize the impact of cybersecurity threats.

III. KEY FINDINGS

After analysing the information and data gathered from various methodologies, some key findings have been identified.

LOW CYBERSECURITY AWARENESS: A significant segment of Indian population lacks awareness about the threats which can potentially came from vulnerable system. Some are not familiar with the safe practices related to handling their data online. Some innocent people fell prey into various financial scams. Being unaware of the security measures, will make the digital environment less secure. Therefore, enhancing cybersecurity education and promoting best practices among the general public is essential to reducing these risks.

RISING CYBER THREATS: The cyber threats have been on notable surge, with incidents such as ransomware attacks, data breaches, phishing scams, and denial-of-service (DoS) attacks becoming more frequent. This rise in cyber threats can be attributed to India's expanding digital presence, as more people and organisations go online, while many sectors lack strong cybersecurity defences. This provided cyber criminals more opportunities to exploit those

International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 54-57 ISSN: 2584-2145
www.ijemh.com

vulnerabilities which led to increasing number of successful attacks. To combat these growing number of attacks, India should strengthen its cybersecurity infrastructure and implement robust and transparent security measures.

RECOMMENDATION FOR IMPROVEMENT: Upon going through the findings it can be suggested that a cohesive national cybersecurity strategy, which would provide a clear framework for protecting digital assets and managing cyber risks across the country would prove to be a strong solutions to tackle those attacks. This study advocated for initiatives to raise awareness among the general public, as well as specialized training programs for IT professionals. Given that cyberattacks can originate from anywhere in the world, it is crucial for India to work with other nations to share intelligence, align regulations, and collaborate on cybersecurity initiatives.

III. CONCLUSION

Cybersecurity is a very sensitive and widespread topic that is directly involved in our daily life.With more than 52% of the population accessing the internet, India ranks as the second-largest online market globally. As our dependency on electronics and internet are rapidly increasing, so are the concerns related to cybersecurity are also growing. In this paradigm, in it is worth noting that these cyber threats can be very costly and its effect can sustain for a longer period of time. For example, a successful attack on the power grid could lead to widespread blackouts.So we should be very cautious dealing with internet and to avoid any suspicious emails or calls. This study discussed the various aspects of cybersecurity of India and the challenges it is facing in this context. And then some possible counter measures are outlined to address these issues. The rapid digitisation has brought various new opportunities, at the same time its vulnerabilities opened a ground for the cyber criminals to launch a wide range of attacks. The analysis revealed several key factors contributing to these challenges, including gaps in regulatory frameworks, a shortage of cybersecurity talent, limited awareness of the general public among others. For instance, weak passwords, lack of encryption, and insufficient security protocols make systems susceptible to breaches.

This study provides multifaceted solutions to protects the citizens, private and public institutions and organisations from such heinous attacks. If the recommendations are successfully implemented which requires commitment and coordination of the various stakeholders then India mitigate the future threats to certain extent. If the vulnerabilities get unnoticed and proper actions are not taken, the risks coming from the unethical attackers can pose a serious challenge towards a digitised economy. One important thing to note here is that the Indian cybersecurity market expanded to nearly USD 6 billion in 2023, achieving an average annual growth rate exceeding 30% between 2019 and 2023.The way forward from present time is that India should build its own cybersecurity capabilities and reduce external dependence. Innovation in cybersecurity technologies and collaboration at both national and international level can lead to better defence mechanisms and thus we can ensure a safe and secure future of digital India.

REFERENCES

[1]. India cybersecurity domestic report 2023, Data Security Council of India.
[2]. Cyber Security in India, clearias.com https://www.clearias.com/cyber-security-india/
[3]. Top Cybersecurity Regulations in India [Updated 2024] by Kyle Chin, upguard.comhttps://www.upguard.com/blog/cybersecurity-regulations-india
[4]. CYBER AND INFORMATION SECURITY (C&IS) DIVISION, Ministry of Home affairs, Government of India, mha.gov.in
[5]. Research overview: View key information for Australian and Indian cybersecurity researchers, arch-india.org Australian researchers Cooperation Hub
[6]. ETHICAL HACKING AND PENETRATION TESTING GUIDE, Rafay Baloch, CRC Press.
[7]. Shruti Sharma "Securing India's Digital Future: Cybersecurity Urgency and Opportunities" January 20, 2024, THE|DIPLOMAT https://thediplomat.com/2024/01/securing-indias-digital-future-cybersecurity-urgency-and-opportunities/#:~:text=For%20India%2C%20a%20nation%20with,resulting%20in%20million%2Ddollar%20damages.

[8]. Challenges to India's Cyber Security drishtiias.com, Drishti IAS

[9]. Press Trust of India, New Delhi, "Cyber risks biggest threat faced by Indian organisations, says survey" Business Standard.

[10]. Dr. Albina Muratbekova, "Discussion of India's Cyber Security Development Trends", EURASIAN RESEARCH INSTITUTE. https://www.eurasian-research.org/publication/discussion-of-indias-cyber-security-development-trends/