ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 10, Issue 4, April 2023

Cyber Security: Attention from Indian Enterprises, Institutions and Individuals

Dr.Shashirekha Malagi*

Assistant Professor of Law, Sir Siddappa Kambali Law College [Formerly University College of Law], Karnataka University, Dharwad, Karnataka.580001

ABSTRACT: Cyber security is the practice of securing networks, systems and digital infrastructure from attacks which include theft, malware, phishing, DDoS (Distributed Denial of Service Attack) and social engineering. With one cyber-attack happening every 14 seconds, it is imperative to have multiple layers of protection in the form of firewalls, encryption tools, Anti-virus software etc dispersed throughout the organization's network and systems. Companies have a lot of invaluable data like sensitive information with regard to their business, business insights and private data of customers and employees on their networks and mandated by law for companies to protect the data. To be secure, India will have to be vigilant and resilient, not only by looking at how to prevent and respond to attacks, but by managing cyber risks that would unleash new opportunities. Indian law did not take cyber security into its cognizance. This research paper has discussed the cyber security and its effects on the Indian enterprises, Institutions and individuals. Knowledge of the latest regulatory policies, cyber laws and General Data Protection Regulation is a must to excel in the field of cyber security.

I.INTRODUCTION

Cyber-attacks have multiplied worldwide, with studies suggesting that 2022 saw a 38% increase in attacks compared to the previous year. India has unsurprisingly recognized cyber security as a key national security policy priority. Over the past decade, a number of institutions have been set up for this purpose. This includes the National critical information Infrastructure Protection Centre and the office of the National Cyber Security Coordinator, who advises the Prime Minister on cyber security strategy. India's Computer Emergency Response Team (CERT-IN) is the nodal agency for proactively detecting, responding to and mitigating various cyber security threats. The National Cyber Security Policy remains India's only national level legislation dealing cyber security and it does not clearly articulate an overarching cyber doctrine.

II.WHAT IS CYBER-SECURITY?

The term "cyber security" refers to the collection of tools, policies, guidelines, training, actions, security concepts and safeguards, risk management approaches, assurance, and technologies that can be used to secure and protect the cyber environment as well as organization and user assets (ITU 2009). In addition, cyber security aims to secure information technology and focuses on protecting computer programs, networks, and data, along with preventing access to information by unauthorized users as well as preventing unintended change or intended/unintended destruction.[1]

[11] Cybersecurity in India: An Evolving Concern for National Security Sushma Devi Parmar (Central University of Gujarat), https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf,(Visited on 4.1.2023)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

Cyber-Security refers to the act of protecting and ensuring the safety of computer systems and electronic devices from targeted cyber-attacks, opportunist malware (- viruses, trojans and bugs) or accidental introduction of malware by users. The global scale of cyber-threats continues to rise rapidly. In the modern day and age, access to volumes of data has gained currency, and hence every year, numerous attempts are made to breach data, and/or sensitive, confidential or classified records to expose information for political or economic gains. Effective cyber-security practices as a counter measure, thus have become important.

There are three types of cyber threats:

- Cyber-Attack: involves gathering information for political or economic means
- Cyber-Terrorism: aims to undermine electronic systems with intent to instill fear or to cause panic.
- End-user Protection: it is an important aspect of cyber security. It is imperative to ensure that users are educated to protect their systems and themselves from cyber-threats. It is found that introduction to malware is (accidentally) often caused by users themselves. It is thus crucial that users are able to detect such malware, update their systems timely, and refrain from using unsecure networks awareness among the population is also very low.[2]

III.THE FOLLOWING CYBER SECURITY AREAS REQUIRE ATTENTION FROM INDIAN ENTERPRISES, INSTITUTIONS AND INDIVIDUALS:

[2] 7 Types of Cyber Security Threats, https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/,(Visited on 11.3.2023)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

a). BYOD Management:

BYOD (bring your own device) is a policy that allows employees in an organization to use their personally owned devices for work-related activities. Those activities include tasks such as accessing emails, connecting to the corporate network, and accessing corporate apps and data. Smartphone's are the most common mobile device an employee might take to work, but employees also take their own tablets, laptops and USB drives into the workplace.[3]

This rise in the use of personal devices encourages companies to implement BYOD policies. BYOD is not simply to eliminate the need for employees to carry two phones; a BYOD policy is designed to ensure that the employees use strong security practices when connecting to the company network.[4]

As more people switch to smart mobile computing devices due to even online classes, and work from home, there will greater threats. Thus, businesses or workplaces will be required to implement clear, strong BYOD policies, as well as next generation tools to automatically enforce these policies.[5]

(b)Data loss Prevention:

There are always threats from hackers and competitors. It is vital to protect data from both insider (data leaks by employees –either willingly or accidentally) and outside threats. As data becomes more valuable , businesses will be required to deploy technologies like next generation firewalls with data loss prevention capabilities. Personal data protection will become more important due to the increased awareness of data security by the consumers and the enforcement of data privacy laws by the Indian government. To avoid losing reputation among customers and to escape government imposed penalties, enterprises will have to implement strong data loss prevention measures in their business networks.[6]

c) Endpoint protection:

Endpoint security, or endpoint protection, refers to securing endpoints such as desktops, laptops, and mobile devices from cyber security threats. Endpoints can create entry points to organizational networks which cybercriminals can exploit. Endpoint security protects these entry points from malicious attacks.

In recent years, the number of endpoints within businesses has increased. This has been especially the case since the Covid-19 pandemic, which has led to increased remote working around the world. With more employees working from home or connecting to public Wi-Fi on the go, enterprise networks now have more endpoints than ever. And every endpoint can be a potential entry point for attacks. Businesses of all sizes can be targets for cyber attacks. It is increasingly difficult to protect from attacks that enter through endpoints, such as laptops or mobile devices. These devices can be hacked, which in turn can lead to data breaches. It's estimated that 70% of successful data breaches originate on endpoint devices. In a 2020 report by Ponemon, commissioned by IBM, found that the average cost globally of a data breach is $3.86 million (and more in the US). Data is often the most valuable asset a company has and losing that data, or access to that data, can put the entire business at risk.[7]As the Internet of things expands across different industries, the number of weak spots in their cyber defense will also increase. To prevent the Internet of Things networks from becoming a liability to businesses, they will have to adopt next generation firewall solutions that can offer comprehensive endpoint protection and give total visibility over their networks.[8]

d) Proactive Security:

Being proactive means to anticipate future problems, needs, or changes, and take action appropriately. In the context of cyber security, proactive implies just the same. Proactive cyber security is everything you do before an attack takes place. Every business should look at how security procedures can protect its assets, employees and customer data. These procedures can range from physical locks and electronic security systems to firewall software and online password management systems. Businesses can choose to take a proactive approach, in which they act to prevent any dangers before they occur, or a reactive approach, in which they respond to a security breach after it has happened. Proactive security measures can range from a simple padlock to a sophisticated security system. They can be physical barriers, such

[3] https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device,(Visited on 10.2.2023)
[4] *Ibid*
[5] *Ibid*
[6] Data Loss Prevention (DLP), https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/,(Visited on 11.3.2023)

[7] What is endpoint security and how does it work?, https://www.kaspersky.com/resource-center/definitions/what-is-endpoint-security,(Visited on 10.2.2023)
[8] *Ibid*

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

as heavy doors or fireproof file cabinets, or electronic countermeasures, such as pressure sensors, surveillance cameras and keycard readers. Proactive security systems can be unmanned or can involve a full staff of security professionals. Many companies employ proactive security procedures on both their physical assets and their sensitive data, such as intellectual property and customer records.[9]

e). Information Security:

According to the 2012 Securitas report, the biggest challenge for most companies, regardless of size, is how best to protect the company's proprietary information. In the past, this simply meant ensuring the information was locked in a desk drawer or safe, but in the technology era, the challenge extends to securing all the information contained on the company's computers and related systems. Threats can come from competitors, hackers or even foreign espionage efforts to obtain personal or corporate information contained on the systems that might be of potential value to others. Cyber security is therefore a paramount issue for company security personnel. [10] Corporate security deserves serious consideration, because companies can't afford to ignore the importance of both physical and data security. That means taking steps to keep the confidential data on the company network, and to ensure the safety of the building. Companies can enhance the safety of their operations and protect their businesses by taking both physical and virtual security into account.[11]

IV.CYBER SECURITY IMPERATIVE FOR INDIA

The vulnerability of critical technological infrastructure is a growing national security concern. Since the 2013 National Cyber security Policy (NCSP), there have been major paradigm shifts that include the push for digital financial inclusion and next generation technological shifts, such as artificial intelligence, Internet of Things (IoT), and the Smart Cities Mission. In 2015, Prime Minister Narendra Modi outlined the risks that the world faces from a “bloodless” cyber war threat . The criticality of information and communication technology (ICT) and allied areas, such as cyber security, is increasing with threats that can be propagated by cyber terrorism, military espionage, corporate espionage, and financial fraud. The Hon’ble Prime Minister observed that, given that India is a major service provider in global technology, solutions around the global problem should emerge from India, not only to enhance cyber security in the country, but also to make India a global leader in this realm. The World Economic Forum (WEF) Global Risks Report 2019notes that malicious cyber attacks and lax cyber security protocols led to massive breaches of personal information in 2018,ranging from a security incident at T-Mobile affecting 2 million users’ data to a personal data breach affecting 150 million users of the My Fitness Pal application . In February 2019, India’s MeitY outlined India’s digital vision of unlocking the potential of a USD 1 trillion digital economy by 2025 from its current value of around USD 200 billion. To realize this potential and build a stable digital economy, it is imperative that all government and private digital systems are safe, secure, and resilient. As India prepares to refresh its National Cyber security Policy, it must move in sync with present day technological and ecosystem realities. India’s cyber security framework should be able to adapt and be resilient to protect against intrusions at all levels in the public sector, including critical infrastructure, and citizen services, enterprise systems, and public and private data assets.[12]

V. LEGAL AND INSTITUTIONAL FRAME WORK TO DEAL WITH THESE CHALLENGES

The Information Technology Act 2000 continues to be the omnibus legislation that governs cyber security policy in the country, and it includes provisions for digital signatures, e-governance, e-commerce, data protection, cyber offences, critical information infrastructure, interception and monitoring, blocking of websites, and cyber terrorism. Rules under the Act are issued from time to time. In addition to this legislation, regulatory guidelines are issued by sectoral regulators, such as the banking regulator Reserve Bank of India (RBI), telecom regulator Telecom Regulatory Authority of India (TRAI), capital markets regulator Securities and Exchange Board of India (SEBI), and insurance regulator

[9] Reactive vs. proactive security: Three benefits of a proactive cybersecurity strategy, https://resources.infosecinstitute.com/topic/reactive-vs-proactive-security-three-benefits-of-a-proactive-cybersecurity-strategy/,(Visied on 10.3.2023)
[10] https://smallbusiness.chron.com/ebusiness-security-concerns-44182.html,(Visited on 10.2.2023)
[11] *Ibid.*
[12] INDIA’S NATIONAL CYBERSECURITY STRATEGY 2020https://amchamindia.com/wp-content/uploads/2021/01/AMCHAM_FTI_Whitepaper_Cybersecurity.pdf, (Visited on 14.2.2023)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

Insurance Regulatory and Development Authority (IRDA), for organizations under their purview. The Indian Computer Emergency Response Team (CERT-IN), established within the Ministry of Electronics and Information Technology (MeitY), issue alerts and advisories regarding the latest cyber threats and countermeasures on a regular basis, and has published guidelines for securing IT infrastructure.[13]

National Cyber security Policy (Ncsp) 2013 and Key Policy Developments [14]

The National Cyber Security Policy intends to facilitate the construction of a safe computer environment and to enable enough trust and confidence in electronic transactions, as well as to guide stakeholders' activities for cyber space security.

National Cyber Security Policy 2013

a. The Government of India issued the National Cyber Security Policy (NCSP) in 2013, which included many tactics for countering cyber security threats.

b. The purpose of this policy is to provide individuals, companies, and the government with a secure and dependable cyberspace. It also strives to monitor, protect, and enhance cyber security defenses.

c. Through a mix of institutional structures, procedures, technology, and collaboration, this Policy intends to secure the information infrastructure in cyberspace, decrease vulnerabilities, create capacities to avoid and respond to cyber attacks, and limit damage from cyber events.

Vision of National Cyber Security Policy, 2013:

- To build secure and resilient cyberspace for citizens, businesses and the Government.

The mission of National Cyber Security Policy, 2013:

- To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

Recent Update

a. The Data Security Council of India (DSCI), led by Lt. General Rajesh Pant, created the National Cyber Security Strategy in 2020. The research focused on 21 areas to guarantee India's cyberspace is safe, secure, trustworthy, resilient, and dynamic.

b. The revised National Cyber Security Strategy 2021, which takes a holistic approach to addressing the concerns of national cyberspace security, was presented to the Parliament in 2022.

c. Recently, in 2022, the UK Government and the National Cyber Security Coordinator of India's National Security Council Secretariat (NSCS) collaborated with the International Counter Ransomware Initiative- Resilience Working Group.

[13]India's National Cybersecurity Strategy 2020 Executive Summary White Paper Prepared For The Office Of The National Cybersecurity Coordinator (Ncsc), Government Of India, Https://Amchamindia.Com/Wp-Content/Uploads/2021/01/Amcham_Fti_Whitepaper_Cybersecurity.Pdf,(Visted On 2023)

[14] National Cyber Security Policy - Recent Update, Objectives, Main Components and Cyber Security, https://testbook.com/ias-preparation/national-cyber-security-policy,(Visited on 8.3.2023)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

d. The Prime Minister's Office (PMO) is actively reviewing the country's national cybersecurity policy. Despite an increase in assaults on India's networks, the Centre has yet to execute the National Cyber Security Strategy.

e. The International Counter Ransomware Initiative – Resilience Working Group, which is being led by India under the leadership of the National Security Council Secretariat, successfully designed and conducted the Cyber Security Exercise "Synergy" for 13 Countries. This was done by the Indian Computer Emergency Response Team (CERT-In) and the Cyber Security Agency of Singapore (CSA).

f. In 2022, CERT-In observed "Cyber Jaagrookta Diwas" in order to educate and inform Internet users on how to protect themselves against cybercrimes and fraud.

Need for a National Cyber Security Strategy

a. India's society is increasingly reliant on digital technology for communication, banking, and other areas of daily life. The use of social media and digital payments has increased significantly.

b. In 2022, ransomware occurrences increased by 51%, according to the Indian Computer Emergency Response Team (CERT-In).

c. Cybercrime against individuals and institutions is on the rise. Rogue elements and criminal syndicates have become more adept in their local and international hacking operations and targeted phishing attempts.

d. In light of increasing geopolitical dynamics in South Asia and the Indo-Pacific, cyber-attacks by India's rivals have increased. State and non-state actors have launched attacks against India's nuclear infrastructure, electricity systems, telecom equipment ecosystems, and financial systems.

e. After Galway, China already attacked India's energy network and attempted to enter the National Security Adviser in 2010. These attempts have had a profound influence on India's view of national security.

Objectives of National Cyber Security Policy

a. To build a safe cyber environment in the country, develop appropriate trust and confidence in IT systems and cyberspace transactions, and so increase IT adoption in all sectors of the economy.

b. To provide information protection when in process, processing, storage, and transport to preserve citizen data privacy and reduce economic losses due to cybercrime or data theft.

c. To improve law enforcement skills and allow successful cybercrime prevention, investigation, and conviction by appropriate legislative action.

d. To raise awareness of the integrity of ICT goods and services by developing infrastructure for testing and validating their security.

e. To give firms financial incentives for adopting standard security procedures and processes.

f. Through a successful communication and promotion approach, a culture of cyber security and privacy will be established, allowing responsible user behaviour and activities.

g. To meet national security needs by developing appropriate indigenous security technologies through frontier technology research, solution-oriented research, and commercialization.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

h. To provide an assurance framework for the establishment of security policies, as well as to promote and enable activities for conformance to global security standards and best practices through conformity assessment.

i. To fortify the regulatory framework to ensure a secure cyberspace ecology.

Main Components of the National Cyber Security Strategy

National cyber security strategies (NCSSs) are the primary documents used by national governments to establish strategic directives, goals, and specific actions to reduce cybersecurity risk. This section describes the Main Components of the National Cyber Security Strategy for a deeper understanding of cyber security strategy:

a. Strengthening the Regulatory Framework

- To require frequent audits and evaluations of the sufficiency and effectiveness of information infrastructure security by the regulatory framework.
- To empower, educate, and increase public understanding of the regulatory system.

b. Promotion of Research & Development in cyber security

- Encourage R&D to generate cost-effective, tailor-made indigenous security solutions that address a broader variety of cyber security concerns, with an eye toward export markets.
- To assist the transfer, dissemination, and commercialization of R&D outputs into commercial goods and services for use in the public and private sectors.

c. Securing E-Governance services

- To promote the use of Public Key Infrastructure (PKI) for trustworthy communication and transactions throughout the government.
- To hire information security specialists to help with e-Government projects and to assure compliance with security best practices.

d. Encouraging Open Standards

- To promote the adoption of open standards to improve interoperability and data sharing among various goods or services.
- To encourage the formation of a public-private partnership to increase the availability of tested and certified IT solutions based on open standards.

e. Creating an assurance framework

- Identify and categorise information infrastructure facilities and assets at the entity level in terms of risk perception to implement appropriate security protection measures.
- To promote secure application procedures that adhere to global best standards.

f. Creating a secure cyber ecosystem

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 10, Issue 4, April 2023

- To guarantee that all firms set up a designated budget for developing cyber security programmes and responding to cyber events.

- To offer fiscal schemes and incentives to incentivize entities to establish, enhance, and update cyber security-related information infrastructure.

VI. SUGGESTIONS

Majority of Indian enterprises, institutions, individuals are unprepared with adequate cyber security measures. So Indian companies should gear up for implementing a desired level of cyber security with the following solutions:

a. Al and machine learning based cyber security solutions to mitigate the risks posed by ever evolving malware, hacks and other types of cyber-attacks.
b. Al-based self learning applications that will ensure continued protection against evolving risks.
c. Al based next generation firewall solutions that are more contextually intelligent.
d. 7 Layer deeper inspection performing inspection and analyze a broader range of parameters to determine the safety.
e. Anticipate potential cyber risks and take measures accordingly.

VII. CONCLUSION

Cyber-attacks targeting Indian enterprises, Institutions & individuals, such as energy ,financial services, defense and telecommunications, have the potentials of adversely impacting upon the nation's economy and public safety from the perspective of national security, the securing of the critical information infrastructure has become a top priority, but minimal digital literacy or low thresholds of educational attainment and awareness among India's Internet users can significant risks for cyber crime and data misuse. Thus, there exists a vital need for India to form government policies, proper laws in order to combat with the cyber threats effectively. The Information Technology Act guidelines recently issued by CERT-IN, and several draft of the Data Protection bill impose obligations on any entity handling data to undertake 'reasonablr security practices' in line with international standards and notify the relevant authorities within set time frames. However, the law does not provide compensation to individual victims whose data may have been breached or stolen as a result of a cyber attack. The hitherto largely untested mechanism of cyber insurance policies may be of some use here. However, across jurisdictions, insurance companies have often refused to pay off claims arising from a cyber attack by invoking the 'act of war' exception. Ultimately, improved cyber resilience will require robust cooperation within the government institutions, with the private sector and with trusted geopolitical partners. This cooperation must be utilized to make technical cyber defence capabilities stronger and to implement awareness mechanisms that can ensure widespread adoption of cyber hygiene practices.

REFERENCES

1.Cybersecurity in India: An Evolving Concern for National Security Sushma Devi Parmar (Central University of Gujarat), https://www.academicapress.com/journal/v1-1/Parmar_Cybersecurity-in-India.pdf,(Visited on 4.1.2023)
7 Types of Cyber Security Threats, https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/,(Visited on 11.3.2023)
2.https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device,(Visited on 10.2.2023)
[3].Data Loss Prevention (DLP), https://www.imperva.com/learn/data-security/data-loss-prevention-dlp/,(Visited on 11.3.2023)
[4].What is endpoint security and how does it work?,https://www.kaspersky.com/resource-center/definitions/what-is-endpoint-security,(Visited on 10.2.2023)
[5].Reactive vs. proactive security: Three benefits of a proactive cybersecurity strategy, 6.https://resources.infosecinstitute.com/topic/reactive-vs-proactive-security-three-benefits-of-a-proactive-cybersecurity-strategy/,(Visied on 10.3.2023)
7.https://smallbusiness.chron.com/ebusiness-security-concerns-44182.html,(Visited on 10.2.2023)
8.National Cyber Security Policy - Recent Update, Objectives, Main Components and Cyber Security, https://testbook.com/ias-preparation/national-cyber-security-policy,(Visited on 8.3.2023)