Impact of Cyber Security in our Society

First Dr.K.Santhi[1], Second E.Asvitha[2] ,Third D.Hemala[3],Fourth P.Mahalakshmi[4]
[1]*Assistant Professor, Dr. N. G. P. Arts and Science College*
[2,3,4]*Student, Dr. N. G. P. Arts and Science College*

***Abstract*: Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as** information technology security **or electronic information security. Lives of human being reached a point where they can't live without internet-enabled technology. As new technologies, devices and services are constantly being invented to improve the human daily lives. At the same time, this creates many security gaps. Appropriate security measures should be taken. Cybercrime can happen on any device/service at any time and can have devastating consequences. This study provided an overview of cybersecurity concepts. This paper first explains what cyberspace and cybersecurity are. Next, we discuss the costs and implications of cybersecurity. Briefly discuss the sources of security vulnerabilities within your organization and the challenges involved in protecting your organization from cybercrime.**

I. INTRODUCTION

Information technology security (IT security), also known as computer security, cyber security, or digital security, is the defence of computer systems and networks from malicious actors who may disrupt or misdirect the services they offer, expose confidential information to the public, or steal or damage hardware, software, or data.

II. DEFINITION OF CYBER SECURITY

The technique of protecting networks, computers, servers, mobile devices, electronic systems, and data from hostile intrusions is known as cyber security. It is often referred to as electronic information security or information technology security. The phrase is used in several areas, including business and mobile computing.

III. HISTORY OF CYBER SECURITY

The topic of cybersecurity emerged in the 1960s and 1970s and gained widespread attention in the late 1980s as a result of a number of incidents that demonstrated how risky a lack of security could be. Through the 1990s, cybersecurity grew steadily and is now an essential aspect of contemporary life. Let's explore the brief history of this field!

3.1. 1970S: ARAPNET AND THE CREEPER

When researcher Bob Thomas developed the computer software Creeper in the 1970s, it marked its path by leaving a breadcrumb trail as it moved throughout the ARPANET network. The program Reaper was created by email's creator, Ray Tomlinson, and it chased and removed Creeper. Reaper, the first computer worm ever, was also the first instance of antivirus software and the first self-replicating program.

3.2. 1980S: BIRTH OF THE COMMERCIAL ANTIVIRUS

Commercial antivirus initially appeared in 1987, despite conflicting claims over who invented the first antivirus product. In 1987, Andreas Luning and Kai Figge launched Ultimate Virus Killer along with their first antivirus program for the Atari ST. The original version of the NOD antivirus was developed by three Czechoslovaks in the same year that John McAfee launched McAfee in the US and made VirusScan available.

3.3.1990S: THE WORLD GOES ONLINE

More people started posting their personal information online as the internet became more widely used. As a possible source of income, organized crime groups began stealing data from citizens and governments online. By the middle of the 1990s, network security threats had grown tremendously, necessitating the mass production of firewalls and antivirus software to safeguard users.

3.4. 2000S: THREATS DIVERSIFY AND MULTIPLY

Beginning in the early 2000s, organized crime groups began to heavily invest in funding professional cyberattacks, while governments started to crack down on the illegality of hacking by handing out increasingly harsher punishments to those responsible. Sadly, viruses also grew in number as the internet

expanded, despite the fact that information security continued to progress.

3.5. 2021: THE NEXT GENERATION

The cybersecurity sector is expanding at an astronomical rate. By 2026, Statista predicts that the size of the worldwide cybersecurity market will increase to $345.4 billion. One of the most prevalent dangers to any organization's data security is ransomware, and its prevalence is expected to rise.

IV. THE DIFFERENT TYPES OF CYBER SECURITY

Due to the rise in cybercrime, both organizations and individuals are becoming more concerned about cyber security. Virens, malware, and hacking are just a few of the many various types of cyberthreats that might exist. There are numerous types of cyber security to take into account, including: The confidentiality and integrity of data are protected by data security. Preventing illegal access, usage, or disclosure of data is a part of this. Identity theft, financial fraud, and other major repercussions can result from data breaches. Hacker defences concentrate on preventing assaults from happening. This entails putting preventative measures like firewalls and intrusion detection systems in place, planning for and responding to cyberattacks, watching network traffic for indicators of an attack, and responding to cyberattacks.

The three varieties of cyber security can work together or against one another. Data security, for instance, can assist lessen the effects of a breach if one does occur while hacker defences can help prevent data breaches from occurring in the first place.

V. CYBER THREATS

A malicious act that aims to destroy data, steal data, or otherwise interfere with digital life is referred to as a cyber or cybersecurity threat. Computer viruses, data breaches, DoS assaults, and other attack methods are examples of cyberthreats. Cyber threats also refer to the potential for a successful cyber assault with the intent of stealing sensitive data, damaging or disrupting a computer network, or gaining unauthorized access to an information technology asset. Cyberthreats may originate from a company's own trusted employees or may come from distant, unidentified parties. Cyber threats come from numerous threat actors, including:

5.1. HOSTILE NATION STATE

Emerging cyber dangers include propaganda, website vandalism, espionage, disruption of vital infrastructure, and even human casualties, according to national cyber warfare programs. When compared to other threat actors, government-sponsored programs are becoming more sophisticated and pose advanced dangers. Their expanding capabilities might seriously harm the national security of numerous nations, including the United States, over the long term. Due to their ability to use technology and techniques against the most challenging targets, such as classified networks and crucial facilities like electrical grids and gas control valves, hostile nation-states offer the greatest risk.

5.2. TERRORIST GROUPS

Terrorist organizations are utilizing cyberattacks more frequently to harm national interests. They are less skilled at cyberattacks and are less likely than nation-states to use cyber methods. With the influx of younger, more technologically savvy generations into terrorist organizations, it is conceivable that they will pose significant cyber dangers. Corporate Spies and Organized Crime Organization. The potential of corporate spies and organized crime groups to engage in industrial espionage to steal trade secrets or commit massive financial crimes makes them a risk. In most cases, these parties are motivated in profit-based activities, either making money or interfering with a company's capacity to make money by assaulting competitors' vital infrastructure, stealing trade secrets, or getting access to and using blackmail to obtain information.

5.3. HACKERS

A zero-day exploit could be used by malicious attackers to gain unauthorized access to data. Information systems may be breached by hackers as a challenge or for bragging rights. This used to need a lot of expertise. Today, sophisticated attacks are made simple by the availability of automated attack scripts and protocols on the Internet.

5.4. NATURAL DISASTERS

Natural disasters pose a cyber danger since they have the same potential to damage your vital infrastructure as a cyberattack.

5.5. ACCIDENTAL ACTIONS OF AUTHORIZED USERS

An authorized user can neglect to configure S3 security properly, which could result in a data breach. Poor configuration has been the root of some of the biggest data breaches, not hackers or irate insiders.

VI. EXAMPLE OF CYBER THREATS

Malware: It is possible for an authorized user to improperly configure S3 security, which could lead to a data breach. Some of the biggest data breaches have not been the result of malicious insiders or hackers, but rather poor configuration.

Spyware: Spyware is a type of malware that conceals itself on a device and shares real-time information with its host, allowing the host to steal information like bank account numbers and passwords.

Phishing attacks: Phishing attacks occur when a cybercriminal tries to trick people into disclosing sensitive information, including passwords, banking and credit card information, and personally identifying information (PII).

Distributed denial of service attacks: In order to overload the system and prevent legitimate requests from being fulfilled, distributed denial of service attacks bombard a computer network with unnecessary requests from a botnet.

VII. CYBER SECURITY AND THE ECONOMY

Both consumers and corporations are becoming more and more concerned about cybersecurity. It not only physically endangers our personal safety and privacy, but it also has a major financial impact. The National Institute of Standards and Technology (NIST) estimates that the cost of cybersecurity to the American economy is more than $600 billion a year. That is greater than 1% of the GDP! In fact, a recent research by the Ponemon Institute discovered that businesses can see a 36 percent gain in revenues by being proactive in tackling cyber threats. Businesses can defend themselves against cyberattacks in a variety of ways, but prevention is always the most crucial action. Businesses can prevent security breaches by implementing multilayer security measures, encrypting data, and routinely monitoring activity severe occurrences collectively.

VIII. HOW DOES CYBER SECURITY AFFECT OUR SOCIETY?

Cybersecurity is a rapidly growing industry that has the potential to impact our society in a number of ways. It is important for businesses and individuals to be aware of the effects cyber security has on our everyday lives, particularly when it comes to our privacy and security.

IX. HERE ARE THREE WAYS CYBERSECURITY AFFECTS OUR SOCIETY:

1. Cybersecurity Affects Our Privacy In A Significant Way Cybersecurity is all about protecting our information and privacy. When hackers gain access to personal data, they can use it to steal identities, commit fraud, or even spy on us. Cybersecurity can protect us from these types of attacks by ensuring that our data is secure and accessible only to those who should have access to it.
2. Cybersecurity Affects Our Security In A Significant Way Cybersecurity also protects our security. If hackers are able to breach our security measures, they could gain access to our personal information, as well as confidential company data. By implementing strong cybersecurity measures, we can protect ourselves from these types of attacks and keep our businesses safe from harm.
3. Cybersecurity Affects Our Overall Quality Of Life When we're not able to access our email or online banking account, we feel inconvenienced and frustrated.

X. CYBER CRIME LAW IN INDIA

Cybersecurity is a concern for every government in the globe, including that of our own nation. It is crucial that India accepts responsibility for the growing number of cyber security concerns it is particularly confronting. An investigation of worldwide cybercrime by the Economic Times found that

cyberattacks cost the government roughly Rs. 1.25 lakh crore annually.

Every government on the planet, including that of our own country, is concerned about cybersecurity. India must take responsibility for the increasing number of cyber security issues it is facing in particular. The Economic Times reported that cyberattacks cost the government about Rs. 1.25 lakh crore yearly after looking into global cybercrime.

The only way to combat the virtually infinite risks offered by the internet is to put in place a cyber security policy. Protecting important data assets requires a considerable investment of resources from the government.

When it comes to cybersecurity, there are four main cyber laws to cover:

Cyber laws in India are especially important in nations like India, where the internet is widely utilized. Cyber laws that are strict serve the objective of regulating the electronic exchange of data, software, security, and financial activities.

India's Cybersecurity Law has paved the way for electronic commerce and electronic government in the nation while reducing cybersecurity worries. It has also increased the scope and applications of digital media.

10.1.Information Technology Act, 2000

The IT Act is the salient one, guiding the entire Indian legislation to govern cybercrimes rigorously: Section 43: People who harm computer systems without the owner's consent are subject under Section 43. In such circumstances, the owner is entitled to full reimbursement for the total harm.

Section 66: Applicable if it is discovered that someone committed one of the acts listed in section 43 dishonestly or fraudulently. In such cases, the maximum possible sentence is three years in prison and/or a fine of Rs. 5 lakh.

Section 66B: Include the sentences for obtaining computers or other electronic equipment that have been reported stolen fraudulently, which confirms a likely sentence of three years in jail. Depending on the severity, a fine of Rs. 1 lakh may be added to this sentence.

Section 66C - This section examines identity frauds including fake digital signatures, compromised passwords, or other distinguishing characteristics. If found guilty, a Rs. 1 lakh fine might be added to the three years of prison time.

Section 66 D - This on-demand addition focuses on punishing cheaters who use computer resources to impersonate others.

10.2. Indian Penal Code (IPC) 1980 Identity thefts and associated cyber frauds are embodied in the Indian Penal Code (IPC), 1860 - invoked along with the Information Technology Act of 2000. The primary relevant section of the IPC covers cyber frauds:

- Forgery (Section 464)
- Forgery pre-planned for cheating (Section 468)
- False documentation (Section 465)
- Presenting a forged document as genuine (Section 471)
- Reputation damage (Section 469)

10.3. Companies Act of 2013 Business people cite the Companies Act 2013 as a necessary legal requirement to improve their day-to-day operations. This legal guideline enforces all required technical and legal compliance and exposes non-compliant companies to legal bindings.

The Companies Act 2013 empowers the SFIO (Serious Fraud Investigation Office) to prosecute Indian companies and their directors. After the issuance of the 2014 Corporate Inspection, Investment and Investigation Regulations, the SFIO has become even more proactive and strict in this regard.

Legislators ensure comprehensive coverage of all regulatory compliance requirements, including cyber forensics, eDiscovery, and cyber security diligence. The Companies (Administration and Management) Regulations 2014 mandate strict policies that review the cybersecurity duties and responsibilities of company directors and officers.

10.4. NIST Compliance Accredited by the National Institute of Standards and Technology (NIST), the Cybersecurity Framework (NCFS) is the most trusted global certification body and offers a harmonized approach to cybersecurity.

The NIST Cybersecurity Framework contains all the guidelines, standards, and best practices necessary to address cyber risk responsibly. This framework focuses on flexibility and cost efficiency. Promote

resilience and protection of critical infrastructure through:

- Allowing better interpretation, management, and reduction of cybersecurity risks – to mitigate data loss, data misuse, and the subsequent restoration costs
- Determining the most important activities and critical operations - to focus on securing them
- Demonstrates the trust-worthiness of organizations that secure critical assets
- Helps to prioritize investments to maximize the cybersecurity ROI
- Addresses regulatory and contractual obligations
- Supports the wider information security program

By combining the NIST CSF framework with ISO/IEC 27001 - cyber security risk management becomes simplified. It also makes communication easier throughout the organization and across the supply chains via common cybersecurity directives laid by NIST.

XI. CONCLUSION

Cyber security has become one of the greatest needs in the world today as cyber security threats pose a great danger to national security due to the high pervasiveness of the Internet. Governments as well as the public need to keep their system and network security settings updated and raise public awareness to keep their system and network security settings safe from viruses and malware by using appropriate antivirus programs.

XII. REFERENCE

[1] Ravi Sharma, Study of Latest Emerging Trends on Cyber Security and its challenges to Society, International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1 ISSN 2229-5518 IJSER © 2012

[2] Abraham D. Sofaer, David Clark, Whitfield Diffie, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy http://www.nap.edu/ catalog/12997.htmlCyber Security and International Agreements, Internet
Corporation for Assigned Names and Numbers pg185-205

[3] ThillaRajaretnam Associate Lecturer, School of Law, University of Western Sydney, The Society of Digital Information and Wireless Communications (SDIWC),International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 232-240 2012 (ISSN: 2305-0012)

[4] Thomas H. Karas and Lori K. Parrott , Judy H. Moore , Metaphors for Cyber Security ,Sandia National Laboratories P.O. Box 5800 Albuquerque, NM 87185-0839

[5] BinaKotiyal, R H Goudar, and Senior Member, A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India PritiSaxena, IACSIT International Journal of Information and Education Technology, Vol. 2, No. 2, April 2012

[6] Loren Paul Rees, Jason K. Deane, Terry R. Rakes , Wade H. Baker, Decision support for Cyber security risk planning, Department of Business Information Technology, Pamplin College of Business, Virginia Tech., Blacksburg, VA 24061, United States b Verizon Business Security Solutions, Ashburn, VA 20147, United States

[7] S. Bistarelli, F. Fioravanti, P. Peretti, Using CP-nets as a guide for countermeasure selection, Proceedings of the 2007 ACM Symposium on Applied Computing (Seoul, Korea, 2007), 2007, pp. 300–304.

[8] Admiral Dennis C. Blair, Annual Threat Assessment, House Permanent Select Committee on Intelligence, 111th Congress, 1st sess., 2009. Win the Cyber-war We're Losing,‖ February 28, 2010, (accessed on July 19 2010).