CONCEPT OF CYBER SECURITY AND ROLE OF SOCIAL MEDIA

Manoj Kumar[1] Dr. Kuldeep Kumar[2]

1. **Research Scholar, Shri Khusal Das University Hanumangarh**

2. **Research Supervisor, Shri Khusal Das University Hanumangarh**

ABSTRACT

In a society where individuals readily disclose their personal data, firms must promptly recognize potential risks, react in real-time, and prevent any sort of security breach. Given the susceptibility of individuals to be drawn to social media platforms, hackers use this vulnerability as a means to get the specific information and data they need. Therefore, individuals should implement suitable precautions, particularly while engaging with social media, to safeguard their personal information from being compromised. The core problem that social media poses to corporations lies in the capacity of individuals to disseminate knowledge to a vast audience of millions. Not only does social media empower individuals to share economically sensitive information, but it also grants them the ability to propagate incorrect information, which may be as detrimental. Ensuring the privacy and security of data is always a top priority for every firm. Currently, we are in a world where all information is stored in a digital or cyber format. Social networking services offer a secure environment for users to engage with their friends and family. Regarding residential users, cyber-criminals would persist in focusing on social media platforms to pilfer personal information..

Keywords: *Concept , Cyber Security , Role , Social Media*

INTRODUCTION

Cyber Crime

Cybercrime refers to any illicit conduct that utilizes a computer as its principal tool for perpetration and the act of stealing. The U.S. Department of Justice broadens the scope of cyber crime by include any unlawful behavior that utilizes a computer for the purpose of preserving evidence. The expanding roster of cyber crimes encompasses offenses facilitated by computers, such as network intrusions and the propagation of computer viruses, as well as computer-based iterations of preexisting crimes, such as identity theft, stalking, bullying, and terrorism, which have emerged as significant challenges for individuals and nations. Cybercrime may be described as the act of committing a crime utilizing a computer and the internet, such as stealing someone's identity, selling illegal goods, harassing victims, or

causing harm through malicious software. With the increasing relevance of technology in people's lives, cyber crimes are also on the rise due to technical advancements..

Concept of Cyber Security

The problem has been the subject of much debate among experts and policymakers for a considerable period of time. There is increasing worry about the security of ICT systems due to deliberate cyber assaults by unauthorized persons who want to get access to ICT programs with the goal of stealing, disrupting, or destroying them, or engaging in any other criminal activity. Analysts widely anticipate an increase in both the quantity and magnitude of cyber assaults in the upcoming years. Cyber security refers to the practice of protecting ICT systems and data. The phrase "cyber security" was created to denote the safeguarding of digital information. Cyber security, once a vague concept, has now emerged as a vital asset in promoting diversity and inclusivity.

Ensuring the privacy and security of data is always a top priority for every firm. Currently, we are in a world where all information is stored in a digital or cyber format. Social networking services offer a secure environment for users to engage with their friends and family. Regarding home users, cyber-criminals would persist in focusing on social media platforms to illicitly get personal information. It is essential for individuals to adopt necessary security precautions not only when using social networking platforms, but also during financial transactions..

Nevertheless, it is challenging to provide an exact definition. Typically, it pertains to one or many of the subsequent matters:

1) Cybersecurity refers to a set of measures and procedures aimed at protecting servers, computer networks, hardware, software, and data from unauthorized access, damage, or other potential threats. This includes safeguarding devices, applications, and the information they contain, as well as other components of the digital environment.
2) The state or level of being protected from certain dangers.
3) The extensive endeavor focused on implementing and improving the effectiveness of such activities..

Role of Social Media in Cyber Security

In an era of growing socialization in a highly interconnected society, organizations must devise novel strategies to safeguard personal data. Social media has a significant impact on cyber security and will greatly contribute to personal cyber dangers. The use of social media

by staff is rapidly increasing, and so is the risk of assault. Due to the widespread usage of social media or social networking sites on a daily basis, they have become a significant platform for cyber criminals to hack private information and steal important data. In a society where individuals readily disclose their personal data, firms must promptly recognize potential dangers, react in real-time, and prevent any sort of security breach. Due to the strong allure of social media, hackers exploit them as a lure to obtain the specific information and data they need. Therefore, individuals must implement suitable precautions, particularly while engaging with social media, to safeguard their personal information from being compromised. The core problem that social media poses to corporations lies in the capacity of individuals to disseminate knowledge to a vast audience of millions. Social media not only enables the distribution of economically sensitive information, but also facilitates the dissemination of misleading information, which may be as detrimental. One of the rising threats highlighted in the Global threats 2013 report is the fast dissemination of incorrect information via social media..

OBJECTIVES OF THE STUDY

1) To study on Role of Social Media In Cyber Security
2) To study on Concept of Cyber Security

Cyber Security in India: In-Depth

The IT industry in India has become a major driver of the country's economic growth and is an essential component of its business and government. The industry is exerting a beneficial impact on the lives of Indian citizens by directly or indirectly contributing to the enhancement of several socio-economic indicators, including the quality of life, employment, and diversity. Furthermore, Information Technology (IT) has been instrumental in elevating India's status as a prominent provider of commercial services and cutting-edge technological solutions on a worldwide scale (DEITY 2011).

Simultaneously, the expansion of the IT industry has brought about a significant and escalating need to protect the computing environment, as well as the imperative to establish sufficient confidence and trust in this field (DEITY 2012). Financial institutions and the banking industry have integrated IT into their operations, which has created numerous growth opportunities. However, this integration also exposes these institutions to cyberattacks on a regular basis. The lack of strategies to address these threats is a cause for concern (Jain 2014). The government sector has played a role in promoting the use of IT-enabled services and

programs, such as the Unique Identification Development Authority of India (UIDAI) and National e-Governance Programs (NeGP). This has led to the development of a large-scale IT infrastructure and encouraged corporate involvement. Key sectors like as defense, banking, energy, telecommunications, transportation, and other public agencies rely extensively on computer networks to transmit data for business transactions, as well as for information and communication reasons. Currently, the government has ambitious objectives to further elevate ecommerce services, cyber connection, and overall improve the utilization of IT in communications. Indian Prime Minister Narendra Modi has announced that the cabinet has given approval to the ambitious 'Digital India' program. The objective of this program is to establish broadband internet connections in all gram panchayats, promote e-governance, and transform India into a connected knowledge economy. This statement by the Prime Minister is representative of his usual approach (The Economic Times 2014b). The significant financial support from the government towards emerging technologies necessitates the implementation of stringent rules to ensure strong security measures in these industries (Verma and Sharma 2014).

Kalakuntla, Rohit & Vanamala, Anvesh & Kolipyaka, Ranjith. (2019) In the realm of information technology, the field of cyber security plays an active and vital role. The information needs to be protected, which has become a significant challenge in this day and age. When one thinks of cybersecurity, the first thing that typically comes to mind is the term "cyber crimes," which refers to the massive amount of daily data breaches. Numerous actions are being taken by a variety of governments and organisations to prevent these illegal activities in cyberspace. In spite of the various precautions that have been taken, many people continue to remain concerned about cybersecurity. The topics of cyber terrorism and cyber security take up the majority of this article's focus. It discusses the key developments that are occurring in cybersecurity as well as the consequences of cybersecurity. The potential for cyberterrorism to cause losses of billions of dollars for firms in an area is concerning. In addition to this, the study discusses the components of cyber terrorism as well as the motivations behind it. In addition, this article provides two case examples that are all about cybersecurity. It also includes explanations of some potential solutions pertaining to cyber security and cyber terrorism.

Gade, Nikhita Reddy & Reddy, Ugander. (2014) The field of information technology is significantly impacted by the role that cyber security plays. One of the most difficult difficulties facing people in this day and age is ensuring the safety of the information. The

first thing that comes to mind whenever we consider the topic of cyber security is the alarming rise in the volume of online criminal activity that has been observed in recent years. Many governments and businesses throughout the world are cooperating to take many preventative actions against cybercrimes. In spite of the many precautions that have been taken, many people are still quite concerned about cyber security. This article focuses mostly on the difficulties encountered by cyber security when applied to the most recent technology. In addition to that, it concentrates on the most recent information regarding the tactics, ethics, and trends that are transforming the face of cyber security.

In light of this, Sadik et al. (2020) demonstrated that cybersecurity requires the creation and maintenance of systems connected to the monitoring of prospective cyberattacks and the reduction of associated expenses. In practise, the adoption of a reliable computing environment is a prerequisite in order to safeguard the operational capabilities of new and creative communities. There is a growing need to improve the current state of cybersecurity, yet developments in security are lagging behind due to the consistent growth in activities that are disruptive online. According to the World Economic Forum's (WEF) Global Dangers Report for the year 2019, cyber-security assaults are now surrounded by the top global risks.

Al Amro (2020) conducted research on the topic of cyber security and infrastructure security in the government. In his study, he highlighted the fact that the link between human rights and cybersecurity, particularly the right to freedom of expression and the right to privacy, is dynamic and subject to change. Government ID's education indicates that the value and importance of information have become valuable to individuals who want to infiltrate the system for reputational profit, financial winnings, and to cause weakness to show vulnerabilities that already exist. This is in addition to the increasing movement in electronic records for health. However, a significant portion of the world's data sources are being sent across public networks, which means that the world's information is vulnerable to attack because it was not developed with security in mind and was not addressed in the design process (Michael et al., 2019).

According to Al Amro (2020), since the infrastructure of the internet has not taken cybersecurity into consideration, including security protection of the current internet architecture and IP required substantial modification. This modification included infrastructure security, the incorporation of security into its design, secure operating systems, secure coding, and mechanisms that protect computers, data, capacity, and access control lists. Al Amro also stated that this modification was necessary in order to protect the current

internet architecture and IP. The rise in the usage of technological apps has led to an increase in the number of cybercrimes, which has led to an improvement in cybersecurity. The implementation of information security strategies such as the use of one-time login protection, the prevention of malware threats, and the virtualization of users is one way to achieve increased cyber security (Baazeem and Qaffas, 2020).

Energy and Cybersecurity

India has recognized that ensuring the security of the energy industry is a crucial non-traditional security concern. According to TERI 2013, the country is ranked fourth globally in primary energy consumption. However, the average per capita consumption is very modest. The lack of adequate regulation and poor institutional frameworks for information exchange has resulted in a dearth of knowledge on cyberattacks and equipment vulnerabilities in the Indian energy sector. However, based on the patterns seen in global cybersecurity, it can be inferred that the sector is facing a rising number of advanced assaults. This is especially true since India has started integrating contemporary technology into its energy infrastructure to address its expanding energy demands (Walstrom 2016).

Defence and Cybersecurity

India possesses a substantial defense industry base and sustains the world's third-largest military forces (KPMG 2010). Simultaneously, the government has connected its defense industry with emerging technologies, which has exposed it to a range of constantly changing risks. This is because the country is dependent on these technologies and relies on integrating networks. In 2012, hackers conducted an assault on the computer systems of the Indian Navy's eastern command. These systems are responsible for overseeing the testing of India's ballistic missile submarines and maritime activity in the South China Sea. The navy computer systems were compromised by a virus that covertly gathered sensitive papers and data and sent them to IP addresses located in China.

Although Indian authorities have not revealed the specific nature of the material that was the focus of this assault (Pubby 2012), it is important to note that the Navy is not the alone Indian defense agency to have encountered such detrimental incidents. The National Security Agency (NSA) and the Air Force have also demonstrated vulnerabilities. In 2010, hackers specifically aimed at infiltrating the NSA's headquarters and many computers belonging to the Indian Air Force. They successfully gained unauthorized access by creating multiple minor openings, allowing them to pilfer confidential information and papers (Unnithan 2012). In the same year, the country experienced the largest cyberattack to date, in which

over 10,000 email addresses belonging to high-ranking government officials, particularly those in the military, the Prime Minister's Office (PMO), defense, home ministries, external affairs, and intelligence agencies, were compromised (Singh 2012).

Finance and Cybersecurity

India is experiencing rapid economic growth and the widespread use of information technology (IT) is playing a crucial role in driving this progress. However, increased dependence on information technology has resulted in the emergence of new weaknesses. The prevailing assumption is that the primary motivation behind the majority of cyberattacks is the pursuit of monetary or financial benefits (KPMG 2014). Undoubtedly, the intricate nature of contemporary banking and financial services renders them susceptible to cyberattacks perpetrated by both governmental and non-governmental entities (Singh 2013). The interconnectedness of contemporary technology has intensified the issue, leading to extensive possibilities for fraud, theft, and various types of abuse (Bamrara et al. 2013). Former Indian Telecom Minister, Kapil Sibal, has emphasized the need of cybersecurity for economic security, stating that any negligence in ensuring cybersecurity will result in economic destabilization (Singh 2013).

Telecommunications and Cybersecurity

Telecommunications has been a crucial catalyst for the advancement of social and economic growth in India. Currently, India is recognized as one of the most rapidly expanding telecommunications markets worldwide, with the total number of telephone connections reaching 943 million by February 2012. In the same month, the country recorded a total of 911 million mobile phone connections (NTP 2012) and over 160 million Internet users, with nearly half of them using social media. The Indian government has expressed its commitment to achieving 600 million broadband connections and 100 percent teledensity by 2020 (Singh 2013).

Role of Government

Regarding cyber security, the government's stance include safeguarding government infrastructure as well as assisting in the protection of networks that are not under government control. Every government agency is now accountable for ensuring data security on their own networks, and many also have special duties for critical infrastructure under current laws. The National Cyber Security Policy is a legal framework developed by the Department of Electronics and Information Technology (Deity), which operates under the Ministry of Communication and Information Technology of the Government of India. The objective is to

safeguard both public and private networks against cyber-attacks. The rule aims to protect personal information, financial and banking information, and sovereign data. This was particularly crucial considering the recent disclosure of NSA leaks, which revealed that US government agencies are conducting surveillance on Indian customers, who lack legal or technological safeguards against such activities. As per India's Ministry of Communications and Information technologies, cyberspace is a complex environment consisting of human actions, software services, and the global distribution of information and communication technologies. Multiple papers and research studies have identified several shortcomings and vulnerabilities in India's National Cyber Security Policy of 2013. India is ill-prepared for cyber threats, notwithstanding the official declaration of the strategy. Furthermore, the plan was not ratified until November 2014. (till November 21, 2014). India's data security issues are anticipated to exacerbate, necessitating prompt and resolute measures. India's planned initiatives, such as the National Cyber Coordination Centre and the National vital Information Infrastructure Protection Centre (NCIIPC), have the potential to enhance the country's cyber security and safeguard its vital infrastructure. Now we shall examine how the Cyber Security Strategy 2020 safeguards the digital realm.

CHALLENGES OF LONG TERM

The executive branch engages in various initiatives and pending legislation to prevent cyber-based dangers and espionage, minimize the consequences of successful attacks, enhance collaboration across different sectors, define the tasks and responsibilities of federal agencies, and combat cyber crime..

Design: It is commonly asserted by experts that effective security measures should be integrated into every ICT design. Historically, developers have prioritized functionality above reliability due to economic considerations. Moreover, designers face a daunting problem due to the unpredictability of some security needs..

Incentives: The system of economic cyber security incentives has been characterized as being biased or even counterproductive. Cybercrime is perceived by criminals as a cost-effective, highly lucrative, and comparatively safe option. Conversely, cyber security may be expensive, has inherent weaknesses, and the financial benefits of acquiring it are frequently unpredictable..

Consensus: Cybersecurity encompasses varying interpretations and lacks a universally agreed upon definition, implementation, and risk assessment. Consensus faces substantial cultural barriers, not only within different sectors, but also inside sectors and organizations..

Environment: Cyberspace is often regarded as the fastest-growing technical domain in human history, both in terms of size and characteristics. The evolving threat environment is being complicated by the emergence of new features and applications, such as social media, mobile computing, Big Data, cloud computing, and the internet. However, these advancements have the potential to enhance cyber security through several means, such as the cost-effectiveness of cloud computing and the utilization of big data analytics..

CONCLUSION

The field of computer security is expansive and more crucial due to the growing interconnectedness of the world, where networks are utilized for carrying out vital activities. Each passing year sees cyber crime evolving along many trajectories, and the protection of information follows suit. Organizations are facing challenges in securing their infrastructure due to the emergence of new and disruptive technologies, as well as the constant evolution of cyber tools and threats. This necessitates the use of new platforms and intelligence. While a flawless solution for cyber crimes may not exist, it is imperative that we make every effort to mitigate them in order to ensure a safe and secure future in the realm of cyberspace..

REFERENCES

[1] Aiyengar, S. R. R. (2010). National Strategy for Cyberspace Security. New Delhi: KW Publisher.

[2] Bamrara, A., G. Singh and M. Bhatt (2013). "Cyber Attacks and Defence Strategies in India: An Empirical Assessment of the Banking Sector." International Journal of Cyber Criminology, 7 (1): 49–61

[3] Cavelty, M. D. (2012). "The Militarisation of Cyber Security as a Source of Global Tension." In Mockli, Daniel, Wenger, and Andreas, eds. Strategic Trends Analysis. Zurich: Center for Security Studies.

[4] DSCI. (2013). Analysis of National Cyber Security Policy (NCSP–2013). New Delhi: Data Security Council of India.

[5] Gercke. (2009). Understanding Cybercrime: A Guide for Developing Countries, Geneva: ITU publication.

[6] Government of India. (2012). National Cyber Security Strategy, India: DEITY. IANS. (2014). "69 Percent of Cyberattacks Targeted at Large Companies in India: Report." Business Standard, New Delhi, April 24.

[7] ITU. (2009). Series-X: Data Networks Open System Communication and Security, Overview of Cybersecurity ITU-T X.1205, Geneva: ITU.

[8] Kumar, A. V.; K. K. Pandey, and D. K. Punia (2013). Facing the Reality of Cyber-Threats in the Power Sector. Bangalore: Wipro Technologies.

[9] Madaan, N. (2013). "More in City Fall in Net Trap." Times of India, Pune, September 8.

[10] Singh, H. and J. T. Philip (2010). "Spy Game: India Readies Cyber Army to Hack into Hostile Nations Computer Systems." Economic Times, New Delhi, August 6.

[11] The Indian Express (2014). "Modi to Visit Australia after G-20 Summit." New Delhi, September 6.

[12] Walstrom, M. (2016). "India's Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges." Seattle: Henry M. Jackson School of International Studies.