Emerging Cyber Security and Data Privacy Threats: Challenges and Opportunities: An Analytical Overview

Dr. Priya[1], Ms. Kanika Singh[2]

[1]Associate Professor, Mahalakshmi College for Girls, Duhai, Ghaziabad
[2]Student (M.Ed), Mahalakshmi College for Girls, Duhai, Ghaziabad

ABSTRACT:

In the digitally emerging world where everyone has the access to internet it is very crucial to secure our data because of right to privacy. Cyber security deals with all the laws designed for the cybercrimes. Digitalization and networking provide number of benefits to us in different fields like e-commerce, banking, education, communication but due to cybercrime, a new criminal methodology also arises. Systems, important files, data, and other important virtual things are at risk if there is no security to protect it. The need of the hour is to make people aware of the laws that already have been made and to amend the laws according to the development of technology. The objective of this paper is to spread awareness about the laws and the precautions which we can take to secure our precious data and belongings. With the advent of various types of technology and availability of such technology at lesser cost, every human being around the world has fallen trap to use technology in day-to-day life. From ordering food online to shopping clothes, books and other necessary items to booking tickets, appointments with doctors etc., to digital payments, every aspect of one's life has become dependent on technology. To put it in simple words, life has become dependent on two essential things – (i) smart phone; and (ii) internet access. However, it is important to note that the success of such technology is inter-alia dependent on the availability of data/information that it collects and/or collected for it. Thereby, data has definitely become the 'new oil' since availability of data, processing it and utilizing it in formulating a perfect algorithm for technology has become very expensive for companies providing digital services. Cyber security is a set of strategies, techniques, and controls to reduce risk and ensure that your data assets are protected. If data privacy is about control, then cyber security has the means to add, some, but not all, of the aspects of that control. Cyber security is at the heart of the discipline of data protection.

Keywords: Cyber Security, Digitalization, Networking, Data Privacy, Criminal Methodology

INTRODUCTION:

In the emerging and innovating digital world where technology has now been working on running humans on digits, it is very important to know what cybercrime is. Cyber attacks are too frequent not just in headlines, but a concern among policymakers, industry leaders, academics, and the public. The crypto currency stealing, attacks on power grids of India by China, Ransomware scam, sim card swapping, debit and credit card crimes are some most common cyber attacks that we hear regularly. The

Cambridge Analytica's case of stealing and revealing of data remained a talk among politicians and was discussed in the parliament also. s. In 2010, the U.S. and Israel reportedly cooperated in the development and use of Stuxnet, a software program that destroyed centrifuges critical to Iran's nuclear weapons program by inferring with their control systems. In 2015, thieves stole $81 million by exploiting weak security at the Central Bank of Bangladesh to persuade the network that controls international transfers of money between banks to transfer the money from the Federal Reserve Bank of New York to the thieves' accounts. It is no wonder that cyber security is attracting more attention, but such attention raises important issues for personal privacy and the data protection tools we use to protect it. Data privacy and cyber security are often advanced by common tools such as encryption, data minimization, and limits on collecting, retaining, and transferring personal data. Consumers must appreciate and obey with basic information security ethics like selecting strong passwords, verification of threats by accessories in email, and backing up data. The relationship between security and data privacy has always been complicated. The cyber security deals only to secure the data whereas the privacy refers to making the content and the data private. Many measures employed to enhance cyber security pose a risk to privacy. For example, proposals to enhance cyber security by requiring identity verification, reducing online anonymity and sharing potentially personal information about cyber attacks all pose risks for personal privacy.

How is cyber security helpful?

Cyber security ensures to secure our data and restricts the access of data to the authorized personnel only. A cyber security outbreak can result in entirety from individuality theft, to blackmail attempts, to the damage of vital data and similar family footprints. Cyber security is a practice formulated for the safeguard of complex data on the internet and on devices safeguarding them from attack, destruction, or unauthorized access. A threat can be anywhere between a minor bug in a code to a complex cloud hijacking liability. Risk assessment helps the organization to stay prepared and to look ahead for potential losses. The significance of the possible effects on data protection are both positive and negative—of the increased attention being paid to cyber security suggests that privacy professionals in government, industry, civil society, and academia should, at a minimum, be paying close attention to the emergence of cyber security. Employee behavior can have a big impact on security information in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness toward information security within an organization. Information security culture is the "...totality of patterns of behavior in an organization that contributes to the protection of information of all kinds."

Anderson and Reamers (2014) found that employees often do not see themselves as part of their organization's information security effort and often take actions that impede organizational changes. Indeed, the Verizon Data Breach Investigations Report 2020, which examined 3,950 security breaches, discovered 30% of cybersecurity incidents involved internal actors within a company. Research shows information security culture needs to be improved continuously. In "Information Security Culture from Analysis to Change", authors commented, "It's a never-ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.

Challenges of Cyber Security and Data Privacy: The biggest challenge in cyber security today is the ever-changing nature of cyber threats. Cybercriminals are constantly inventing new techniques and strategies to exploit vulnerabilities in networks and systems.

1. **Application Security:** Application security prevents unauthorized access and use of applications and connected data. Because most vulnerability are introduced during the development and publishing stages, application security includes many types of cyber security solutions to help identify flaws during the design and development phases that could be exploited and alert teams so they can be fixed.
2. **Cloud Security:** Cloud security focuses on protecting cloud based assets and services, including applications, data, and infrastructure. Most cloud security is managed as a shared responsibility between organizations and cloud service providers.
3. **Critical Infrastructure Security:** Special security processes and types of cyber security solutions are used to protect the networks, applications, systems, and digital assets depended on by critical infrastructure organizations (e.g., communications, dams, energy, public sector, and transportation). Critical infrastructure has been more vulnerable to cyber attacks that target legacy systems, such as SCADA (supervisory control and data acquisition) systems. While critical infrastructure organizations use many of the same types of cybersecurity as other subcategories, it is often deployed in different ways.
4. **Data Security:** A subset of information security, data security combines many types of cyber security solutions to protect the confidentiality, integrity, and availability of digital assets at rest (i.e., while being stored) and in motion (i.e., while being transmitted).
5. **End Point Security:** Desktops, laptops, mobile devices, servers, and other endpoints are the most common entry point for cyber attacks. Endpoint security protects these devices and the data they house. It also encompasses other types of cyber security that are used to protect networks from cyber attacks that use endpoints as the point of entry.
6. **IOT Internet of Things Security:** IoT security seeks to minimize the vulnerabilities that these proliferating devices bring to organizations. It uses different types of cyber security to detect and classify them, segment them to limit network exposure, and seek to mitigate threats related to unpatched firmware and other related flaws.
7. **Mobile Security:** Mobile security encompasses types of cyber security used to protect mobile devices (e.g., phones, tablets, and laptops) from unauthorized access and becoming an attack vector used to get into and move networks.
8. **Network Security:** Network security includes software and hardware solutions that protect against incidents that result in unauthorized access or service disruption. This includes monitoring and responding to risks that impact network software (e.g., operating systems and protocols) and hardware (e.g., servers, clients, hubs, switches, bridges, peers, and connecting devices). The majority of cyber attacks start over a network. Network cyber security is designed to monitor, detect, and respond to network-focused threats.
9. **Operational Security:** Operational security covers many types of cyber security processes and technology used to protect sensitive systems and data by establishing protocols for access and monitoring to detect unusual behavior that could be a sign of malicious activity.

10. **Zero Trust:** The zero trust security models replaces the traditional perimeter-focused approach of building walls around an organization's critical assets and systems. There are several defining characteristics of the zero trust approach, which leverages many types of cyber security.

The field is significant due to the expanded reliance on computer systems, the Internet, and wireless network standards such as Bluetooth and Wi-Fi. Also, due to the growth of smart devices, including Smartphone's, televisions, and the various devices that constitute the Internet of things (IoT). Cybersecurity is one of the most significant challenges of the contemporary world, due to both the complexity of information systems and the societies they support. Security is of especially high importance for systems that govern large-scale systems with far-reaching physical effects, such as power distribution, elections, and finance. **Computer security**, **cybersecurity**, **digital security** or **information technology security** (**IT security**) is the protection of computer systems and networks from attacks by malicious actors that may result in unauthorized information disclosure, theft of, or damage to hardware, software, or data, as well as from the disruption or misdirection of the services they provide.

Threats of Cyber Security and Data Privacy:

1. **Phishing and Social Engineering:** Phishing attacks occur when an attacker impersonates a trusted source in order to entice a user to click a malicious link, download a malicious file, or give them access to sensitive information, such as payment information or credentials. Phishing attacks have grown much more sophisticated in recent years, with attackers able to execute highly effective, finely-tuned phishing campaigns.
2. **Ransom ware And Malware:** Malware, and in particular ransom ware, is one of the most common and most damaging cyber attacks for small businesses. Malware is a varied term for malicious code that hackers create to gain access to networks, steal data, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices. Ransom ware is one of the most common and harmful types of malware, and is presently surging.
3. **Weak Passwords:** Weak passwords are a symptom of poor cyber hygiene that can weaken an organization's resilience against cybercrime such as phishing. Many small businesses today rely on multiple cloud-based services, for which users must create and manage different accounts. These services often can contain sensitive data and financial information. Using easily guessed passwords, or using the same passwords for multiple accounts, can cause this data to become compromised**.**
4. **Poor Patch Management:** Patch management is the process of ensuring all of your endpoint devices (laptops, PCs, smart phones), networks, applications, and more are up-to-date with the latest security updates. Out of date operating systems and software can be at risk of known vulnerabilities that cybercriminals actively look to exploit with ransom ware and malware attacks. Poor patch management therefore can ultimately put your business at risk of data breach.
5. **Insider Threats:** The final major threat facing small businesses is the insider threat. An insider threat is a risk to an organization that is caused by the actions of employees, former employees, business contractors, or associates. These actors can access critical data about your company, and they can cause harmful effects through greed or malice, or simply through ignorance and carelessness. Verizon report that 25% of data breaches were caused by insider threats.

Goals of cyber security: The main objective of data security is to defend the data from being stolen and prevention from unauthorized access. It is achieved by three main steps to be (followed) Confidentiality- making a guarantee that the data is accessible to the authorized persons only. It is achieved by data encryption, multi-step verifications and confirmations. b) Integrity- guarantees that all the data is precise; dependable and it must not be changed in the show from one fact to another. It is achieved by strict privacy measures, operated controls and backing up the data. c) Availability- guarantees that the data is available to the user whenever demanded by him and ensuring that the user doesn't get a Denial of Service. It is achieved by holding down possible threats, monitoring the data and iterative maintenance and bugs removal on demand.

Cryptography- Method of approach of Cyber Security: Cyber security experts use cryptography to design algorithms, ciphers, and other security measures that codify and protect company and customer data. Cryptography protects the confidentiality of information. Confidentiality is a key priority when it comes to cryptography. It means that only people with the right permission can access the information transmitted and that this information is protected from unauthorized access at all stages of its lifecycle. Confidentiality is necessary for maintaining the privacy of those whose personal information is stored in enterprise systems. Encryption, therefore, is the only way to ensure that your information remains secure while it's stored and being transmitted. Even when the transmission or storage medium has been compromised, the encrypted information is practically useless to unauthorized individuals without the right keys for decryption. In the security environment, integrity refers to the fact that information systems and their data are accurate. If a system possesses integrity, it means that the data in the system is moved and processed in predictable ways. Even when the data is processed, it doesn't change. Cryptography ensures the integrity of data using hashing algorithms and message digests. By providing codes and digital keys to ensure that what is received is genuine and from the intended sender, the receiver is assured that the data received has not been tampered with during transmission.

CONCLUSION:

The aspect of cyber security and data privacy is so extensive and this is the only basis of our prevention in future. With the rising demands of digitalization and its boom after pandemic of Covid-19 we must now focus on the cyber security and its enhancement. Since now nuclear weapons are also getting digital it is a need of concern to protect our data and valuables from getting into wrong hands. One of the most problematic elements of cybersecurity is the evolving nature of security risks. As new technologies emerge -- and as technology is used in new or different ways -- new attack avenues are developed. Keeping up with these frequent changes and advances in attacks, as well as updating practices to protect against them, can be challenging. Issues include ensuring all elements of cyber security are continually updated to protect against potential vulnerabilities. Cyber security is the practice of protecting systems, networks, and programs from digital attacks. These cyber attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransom ware or interrupting normal business processes. Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

REFERENCES:

1. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. **12** (2). ISSN 1558-7215.
2. Computer security at the Encyclopedia Britannica
3. Tate, Nick (7 May 2013). "Reliance spells end of road for ICT amateurs". The Australian.
4. Kianpour, Mazaher; Kowalski, Stewart; Øverby, Harald (2021). "Systematically Understanding Cybersecurity Economics: A Survey". Sustainability. **13** (24): 13677. Doi:10.3390/su132413677. hdl:11250/2978306.
5. Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods" (PDF). Politics and Governance. **6** (2): 1–4. Doi:10.17645/pag.v6i2.1569. Archived (PDF) from the original on 4 September 2019.
6. "About the CVE Program". www.cve.org. Retrieved 12 April 2023.
7. Zlatanov, Nikola (3 December 2015). Computer Security and Mobile Security Challenges. Tech Security Conference At: San Francisco, CA.
8. "Ghidra". Nsa.gov. 1 August 2018. Archived from the original on 15 August 2020. Retrieved 17 August 2020.