GLOBUS

Cosmos An International Journal of Management
A Refereed Research Journal
Vol 11 / No 2 / Jan-Jun 2022 ISSN: 2278-1218

CYBERSECURITY AND DATA PRIVACY

[*]Mukul Kumar Singh
[**]Sakshi Tripathi
[***]Preeti Singh

Paper Received: 02.02.2022 / **Paper Accepted**: 03.04.2022 / **Paper Published**: 10.04.2022
Corresponding Author: Mukul Kumar Singh; Email: mukulsingh186@gmail.com; doi:10.46360/cosmos.mgt.420221001

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. By a great rise in digitalization hundreds of terabytes of data is being transferred every second. Lot of this data flowing over the internet contains sensitive personal data which is analysed by companies, hackers and organizations to make monetary benefits out of it. This is the time where data security comes into picture.

Cybersecurity 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 cybersecurity and the precautions which we can take to secure our precious data and belongings.

Keywords: Data, Cybersecurity, Digital, Awareness.

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. It is the data which is in target of the cyberattacks because Data is an asset in the 21st Century where information rules the world. Cyberattacks are too frequent not just in headlines, but a concern among policymakers, industry leaders, academics, and the public. The cryptocurrency stealing, attacks on power grids of India by China, Ransomware scam, sim card swapping, debit and credit card crimes are some most common cyberattacks 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. 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 cybersecurity 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 cybersecurity 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 cybersecurity deals only to secure the data whereas the data privacy refers to making the content and the data private. Many measures employed to enhance cybersecurity pose a risk to privacy. For example, proposals to enhance cybersecurity by requiring identity verification, reducing online anonymity and sharing potentially personal information about cyberattacks all pose risks for personal privacy.

Data is the only search in each and every cybercrime because if you want to identify a person you just need its data. Data includes attributes regarding a specific natural person. Different pieces of information when collected which can identify a person can also be called a personal data. A Personal Data will include things like Your Name, Address, Phone number, Email Address, Aadhar card number, your IP address or something like the health record held by a doctor or a hospital. For an organization, it includes the data of its employees and other financial assets. This data has huge commercial value and is used for monetary gains by many companies and even this data is used by companies to stay a step forward from others'.

Data Privacy

By the exponential growth of amount of data and the users of internet it has now became much

*-***B.Ed Student, Integrated School of Education, Ghaziabad, UP, India.*

important to safeguard the data as right to privacy is guaranteed by many countries. For smooth running we need to provide the data to access something but the main problem is the way it is to be accessed and processed. Privacy is the right to be left alone or to be free from misuse or abuse of one's personality. A data breach at any organization can put top secrets into enemy's hands. The consequences of data theft can be severe for businesses and individuals. Common examples of data theft are through USB Drive, malicious links, remote sharing and malware attacks.

What is Cybersecurity?

Cybersecurity refers to the protection of digital data against the criminal or unauthorized use and the measures taken to achieve it. It is a collection of tools, policies, security guidelines, risk management approaches, training, assurance and technologies that can be used to protect the decorum of cyber environment.

Review of Literature

Raynor F. Ereje, Richard G. Chan, (2021) This study aimed to develop a system that can disseminate information to platforms like the internet, SMS, and mobile application. The study also aimed to test the system's technical features on data management of stakeholders, news, school calendar, SMS keyword customization, asynchronous message broadcasting, and SMS information inquiry. Likewise, the study will also determine the system's usability in terms of system usefulness, information quality, interface quality, and overall usability and develop a user's manual. The study utilizes the developmental-descriptive method of research. The Post-Study System Usability Questionnaire (PSSUQ) a standardized instrument was used for the overall system usability. The functionality evaluation revealed that the developed system passed all test cases for its technical features. The system's usability revealed a satisfactory evaluation in terms of system usefulness, information quality, interface quality, and overall usability. This implies that the evaluators are satisfied with the developed system and thus ready for use. A user's manual guided the users on operating and making the most of the system's capabilities. It is recommended that the system may be used in various institutions wherein information dissemination is crucial, has to be secured, and urgent, especially at this pandemic time.

Bispham, Mary and Creese, Sadie and Dutton, William H. and Esteve-Gonzalez, Patricia and Goldsmith, Michael, (2021) [2], This paper presents the findings of an exploratory study of the implications of a shift to working from home (WFH) in the context of the COVID pandemic. The literature and news coverage of this topic focuses on rising concerns over cybersecurity, but exploratory interviews suggest a need to reframe this issue. A focus on the threats or rising security problems tied to WFH is important but too narrow. An equally critical question is whether early experiences with and adaptation to WFH created a cybersecurity infrastructure and practices that have enabled a much greater scale of WFH. In essence, for some kinds of work for some types of individuals, is it possible that advances in cybersecurity have been an enabler of WFH and other remote telework, rather than a barrier? This question provides a basis for expanding research on whether cybersecurity is a barrier or enabler of WFH patterns, including many mixed or hybrid modes of splitting work between the office, home and other remote locations. Given the issues tied to the limited perspectives of even those with expertise in support of WFH, we suggest the basic need for survey research and selected case studies on several well-defined sets of individuals to gain a more empirically anchored perspective on whether cybersecurity has shifted from a barrier to becoming an enabler of remote work.

Azhar, Ishaq, (2016) [1], The primary objective of this study is to assess the effect of artificial intelligence on the cybersecurity environment, particularly in the area of cyber-attack mitigation. The world is changing at a breakneck speed, and businesses that embrace technology have a bright future ahead of them. Digitization has accelerated the pace of change in a variety of areas, including entertainment, new goods, and business. The client receives what they want immediately since the service provider is armed with everything necessary to provide goods or services. While the digital age offers many benefits and conveniences, it also has a few drawbacks. The danger of losing your private information is one of the most serious and damaging risks associated with it. Over the past decade, there have been many instances of identity theft, data breaches, and financial loss. Cyberattacks are often widespread, affecting people, government entities, and companies. Cybercriminals may now reach their targets from anywhere in the globe and at any time. The assault surface in contemporary business settings is enormous, and it is growing at a breakneck pace. This implies that evaluating and enhancing a business's cybersecurity posture requires more than human involvement. Artificial intelligence is increasingly critical to information security since these technologies are capable of rapidly evaluating millions of data sets and identifying a broad range of cyber risks, ranging from malware attacks to suspicious behavior that may result in a phishing assault. This system is always evolving and improving, relying on previous and current events to identify new types of attacks that may occur today or tomorrow. In this paper, I

will discuss the employment of artificial intelligence (AI) in cybersecurity (both positive and negative) in the business world.

How is Cybersecurity Helpful?

Cybersecurity ensures to secure our data and restricts the access of data to the authorised personnel only. A cybersecurity outbreak can result in entirety from individuality theft, to blackmail attempts, to the damage of vital data and similar family footprints. Cybersecurity 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 help 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 cybersecurity suggests that privacy professionals in government, industry, civil society, and academia should, at a minimum, be paying close attention to the emergence of cybersecurity.

Types of Cybersecurity

1. **Phishing**- the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. It is the most common cyberattack and can be dealt manually by being aware of such cases and not revealing any confidential data to anyone.
2. **Malware**- software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. This is generally used by cyber attackers to get into bank servers.
3. **DOS attack**- A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.
4. **Man in the middle attack**- It is a general term for when a perpetrator positions himself in a conversation between a user and an application either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

Goals of Cybersecurity

The main objective of data security is to defend the data from being stolen and prevention from unauthorised access. It is achieved by three main steps to be followed-

1. **Confidentiality**- making a guarantee that the data is accessible to the authorised persons only. It is achieved by data encryption, multi-step verifications and confirmations.
2. **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.
3. **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.

Measures to Secure the Data

1. Using strong passwords
2. Avoiding unnecessary buffering
3. Visiting only trusted websites
4. Keeping the software updated
5. Installing a firewall and antivirus
6. Not sharing the sensitive information without safeguarding it
7. Using multifactor authentication
8. Verification of threats
9. Minimising the exposure of data
10. Changing the passwords over regular intervals

Cryptography - Method of Approach of Cybersecurity

Cybersecurity 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 unauthorised 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 unauthorised 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

By the rapid growth of digitalisation and more reliance on the digital world we are in the strong need of data security and privacy. The aspect of cybersecurity and data privacy is so extensive and this is the only basis of our prevention in future. With the rising demands of digitalisation and its boom after pandemic of Covid-19 we must now focus on the cybersecurity 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. India, has a strong need of data security and facing unemployment so it can deploy its youth based on academic background and work experience to do the role of security administrators, network defence analyst, application security testers, security auditors and web administrators.

Conflict of Interest

There is no conflict of interest between the authors in this manuscript.

References

1. Azhar, Ishaq, (2016). “How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks: A systematic review”.
2. Bispham, Mary and Creese, Sadie and Dutton, William H. and Esteve-Gonzalez, Patricia and Goldsmith, Michael, (2021). “Cybersecurity in Working from Home: An Exploratory Study.”
3. Mohammed, Ishaq Azhar, (2016). “How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks: A Systematic Review”. International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, 4(2), 659-663.