EVOLUTION OF CYBER SECURITY AND IT'S SIGNIFICANCE ON MODERN TECHNOLOGY

Amritanjali Singh[1], Namrata Singh[2], Anirban Bhar[3], Shyamapriya Chatterjee[4]

[1,2] *B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*
[3,4] *Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.*

ABSTRACT

Cyber security is essential in the field of knowledge technology. Cyber security is currently the most urgent concern due to the exponential growth of internet threats and attacks. An active role is accepted by cyber security in the field of information technology. In the modern day, information security has grown to be a major issue. The term "cybercrimes" comes to mind first when discussing cyber security, because they occur on a massive scale every day. Numerous steps are being taken by various governments and groups to stop these cybercrimes. In addition to other measures, many people continue to have serious concerns about cyber security. This essay focuses mostly on cyberterrorism and security. It discusses the key developments in cybersecurity as well as their effects. Associations could lose billions of dollars as a result of cyber terrorism in the area of organizations. The essay also describes the elements and causes of cyber terrorism. It also explains several solutions for cyber terrorism and security.

Keyword: - *Cyber Security, Information Security, Cyber Terrorism, Cyber Crime.*

1. INTRODUCTION

Today, anyone may send and receive any kind of information with the click of a button, whether it be a video, an email, or something else entirely, but has that person ever considered how secure that information is when it is sent to another person? Cybersecurity is the ideal response. Today, more than 61% of all industry trades take place online, making high-quality security in this sector a must for direct and successful exchanges. Consequently, cybersecurity has emerged as a pressing problem (Dervojeda, et. all., 2014). The scope of cybersecurity extends beyond simply validating data in the IT sector to other areas like cyberspace and so on. The security and economic well-being of each nation depend heavily on enhancing cybersecurity and making sure that required data systems are in place.

The improvement of new management as well as a legislative approach now depends on making the Internet safer (and protecting Internet users). A broad and secure practice is required to combat cybercrime (Gross, Canetti & Vashdi, 2017). The specific estimations alone cannot prevent any crime; it is crucial that law enforcement offices are permitted to effectively investigate and bring charges for cybercrime. In order to prevent the loss of any crucial data, several governments and countries nowadays are imposing severe regulations on cyber safety. Each person needs to be knowledgeable about cybersecurity to protect oneself from the rising number of cybercrimes.

Both the insecurity created by and through this new environment, as well as the techniques or procedures to make it (progressively) secure, are topics covered by cyber-security (Kumar, & Somani, 2018). It alludes to numerous practices and actions, both specialist and non-specialized, that are anticipated to protect the bioelectrical state and the data it holds and transmits from all potential dangers. This study attempts to compile all available data and an overview of cybercrime, as well as historical information and reports on the data analyzed from various attacks that have been widely published over the past five years. Based on the information examined, we would like to outline all the precautions that businesses may take to ensure greater security, which would aid in protecting them from hacker attacks and give a level of cyber-security that eliminates all dangers.

2. EVOLUTION OF CYBER SECURITY

Cybersecurity is a subset of IT security. Your networks, computers, and other electronic equipment are safeguarded by cyber security against illegal access, attack, and destruction. Cybersecurity guards the digital data on your networks, computers, and devices from unwanted access, attack, and destruction whereas IT security safeguards both physical and digital data. We'll discuss the operation of cyber security in this section. The initial approach for developing criteria for evaluating crime that originates in cyberspace is described by Brenner [1]. Despite acknowledging that it is exceedingly difficult to construct metrics and scales for cybercrime due to "apprehension," "size," and "proof" concerns, she suggests a straightforward taxonomy of harms that consists of three basic types, namely individual, systemic, and other. Using a similar approach to Laube et al. [2], Kshetri attempts to develop a cost-benefit calculation, but he concentrates on the attacker's point of view. He argues that when these three groups of people interact, cybercrime spirals out of control. He describes the traits of cybercriminals, cybercrime victims, and law enforcement authorities. He creates a formula that weighs the benefits and expenses of an attacker as well as the case for or against a cybercrime. This paper [3] employs interruption detection along with information-digging techniques for digital inquiry. Cybercrime is sometimes described in terms of the crime triangle [4], which asserts that three elements must be present for a cybercrime to take place: a victim, a motive, and an opportunity. The person who will be attacked is the victim. The reason why the crime will be committed is the motive, and the time will be the opportunity (e.g., it can be an innate vulnerability in the system or an unprotected device).

Opportunistic untargeted assaults are still widespread, despite the fact that modern attacks are more sophisticated and targeted to certain victims depending on the attacker's objectives, such as monetary gain, espionage, coercion, or retaliation. Attacks that target victims based on their susceptibility to assault are referred to as "opportunistic attacks" [5]. In this article, the 128-bit block cypher Camellia is presented. Camellia complies with the interface requirements of the Advanced Encryption Standard by supporting 128-bit block sizes and 128-, 192-, and 256-bit keys (AES). In addition to its high level of security, Camellia is renowned for its effectiveness on both software and hardware platforms [6]. It has been demonstrated that Camellia provides strong protection from both differential and linear cryptanalysis. Camellia's encryption speed in terms of hardware and software is at least on pace with that of the AES finalists, notably MARS, RC6, Rijndael, Serpent, and Twofish.

The author of this [7] applied sentiment analysis and machine learning to cyber security to create a method for identifying cyber dangers that have previously eluded detection by conventional technology. A framework for empirically evaluating harm that takes into account a number of procedures is provided by Greenfield et al. [8]. The five fundamental dimensions where injury may manifest are functional integrity, material support and amenity, freedom from humiliation, privacy or autonomy, and reputation. Additionally, by examining actual crimes that have had a large influence on society, they study the cascading nature of harm and develop five levels of scale for distinct types of harm. The phrase "cyberspace cartography" was created by Grant et al., who also used the idea of "cyber-geography" in military operations. Additionally, they make the case that their ontology might be applied in studies to assist in resolving the issue of attribution caused by the inability to recognise hostile actors in cyberspace without delay [9]. When a lawsuit crosses numerous states, it might be difficult to determine which forum has legal power. Chertoff et al. [10] address this issue and the current state of Internet jurisdiction law. They offer four potential formulations for clearly and fairly establishing the controlling jurisdiction in various circumstances. The citizenship of the subject of the unlawful information, data, or system, the location where the harm took place, the citizenship of the data originator, or the citizenship of the data holder or custodian are the bases for these legislation. According to Mathieu and Guy [11], a high-quality solitary literature review offers trustworthy information and insights into prior research, enabling other researchers to seek new directions on related areas of interest. The results of this study can also be used as a basis for future research or as references in related subjects. The potential challenges that these two technologies may bring, which he categorises as strategy, operations, acquisition, and arms control, are compared by Lin [12] by comparing nuclear and cyber technology and regulation. He draws numerous contrasts as well as a few parallels between these challenges. According to the author of paper [13], hacker-activist groups have carried out online security attacks with the intention of hurting web services in a certain situation. The author used Twitter content to show a sentiment analysis technique. The author's approach was based on a daily collection of tweets from people who use the platform to express their thoughts on important issues and to distribute content related to web security breaches. The data was translated into information that could be statistically analysed to assess the likelihood of an assault. By analysing the overall sentiment of users and hacktivist organisations in response to an international issue, the latter was accomplished. Using a Bayesian Generalized Linear Model, Edwards et al. [14] use a publicly available dataset of data breaches to identify trends in data breaches. They come to the conclusion that while the volume and frequency of data breaches have been stable in recent years, their impact is growing as threat actors get more adept at making money off of the sale of personal data and as the volume of electronic financial transactions rises. A survey study [15] offered a thorough literature review of machine learning and data mining techniques for cyber analytics in support of intrusion detection. By putting a strong emphasis on the victimisation component of these crimes, Van Slyke et al. [16] develop a taxonomy of harms for white-collar crimes. Combining desktop research with victim questionnaires, they examine a number of white-collar offences and the expenses connected with them, concentrating on the long-term effects of damages in particular individuals.

3. TRENDS OF CYBER SECURITY

In the field of data technology, cyber security plays a crucial role. Data security has emerged as the biggest challenge in the modern day. Cybercrimes, which are steadily growing in severity, are the key concern in cybersecurity (Samuel, & Osman, 2014). Numerous efforts are being taken by various governments and organizations to stop these cybercrimes. Additionally, many people continue to have serious concerns about the various cybersecurity methods. The following are some major trends that are affecting cybersecurity:

3.1 Web Servers

Attacks on web apps to steal data or spread harmful code continue to be a concern. Using reliable web servers they have purchased, cybercriminals transmit their code. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. People today need to place a more unique emphasis on safeguarding web servers and web applications (Bendovschi, 2015). The major entry point for these crooks to take the information is through web servers. Therefore, one should consistently use a second secure programme, especially

3.2 Mobile Networks

Radio waves are the medium through which communications are transmitted to and from users on a mobile network, also known as a wireless network. It is made up of base stations, each of which covers a distinct area or "cell" in the network. These individual cells, when combined with others of their kind, can give radio coverage for a significant geographic region.

3.3 Encryption

It is a technique for encoding communications so that programmers cannot read them. When a communication is encrypted, it is converted into a stirred-up figure of speech. In most cases, it is finished with the use of a "encryption key" that specifies how the message is to be encoded. The protection of information and its credibility are ensured by encryption at the earliest possible reference point level (Sharma, 2012). Cybersecurity issues increase as encryption is used more frequently. Information sent across systems (such as the Internet, in online transactions), mobile phones, wireless radios, and other communication mediums are all protected by encryption.

3.4 ADP's and targeted attacks

Advanced Persistent Threat (APT) is a whole of the dimension of cybercrime ware. For quite a long-time network security capacity. For example, IPS or web filtering have had a key influence in distinguishing such focused-on assaults (Bendovschi, 2015). As attackers become bolder and utilize increasingly dubious methods, network security must incorporate with other security benefits to identify assaults. Thus, one must recover our security procedures to counteract more dangers coming later on. Subsequently the above is a portion of the patterns changing the essence of cybersecurity on the planet.

4. IMPACT ON SOCIAL MEDIA

For some people, social media has become an integral part of their lives. We use it to remain in touch, organize events, share our photos, and provide comments on recent happenings. It has taken the role of email, and using the phone takes a lot of us. But it's important to be aware of the risks, just like with anything else online. Computers, smartphones, and other devices are priceless possessions that give people of all ages the exceptional ability to interact and work with the rest of the world. People can accomplish this in a variety of ways, including by using social media or networking websites.

People can share their thoughts, images, workouts, and other aspects of their lives thanks to social media (Gross, Canetti & Vashdi, 2017). Whether someone is nearby or far away, they might offer an unexpected window into the lives of others. Unfortunately, these networks also signify protection for one's PC and even their own security. Both the use of social media and the risk of attack are increasing among professors (Sharma, 2012). Social media platforms have become a prime target for cybercriminals because the majority of people use them regularly, making it easy for them to get into user accounts and steal important information.

The organizations must ensure that they are as quick to identify threats, respond increasingly, and prevent any kind of rupture. People must therefore take the necessary precautions, especially when managing social media, to prevent the loss of their data. The basis of the exact test that social media offers to businesses is the ability of individuals to disseminate information to a group of millions of individuals (Cabaj, Kotulski, Ksiopolski, & Mazurczyk, 2018). Although social media allows anybody the opportunity to disseminate financially sensitive information, it also gives them the same ability to spread incorrect information. It might only be as harmful. One of the growing risks is the quick dissemination of false information via social media. Even if social media might be used for cybercrimes, these groups are unable to stop using it because it plays a crucial part in capturing their attention. They should instead create plans that will alert them to the risk so they can remedy it before any actual harm is done. The authors are Dervojeda, Verzijl, Nagtegaal, Lengton, and Rouwmaat (2014). Organizations should be aware of this and the significance of deconstructing the data, particularly in social debates, and provide sound security measures to prevent risks. One must use specialised plans and the appropriate technologies to get into contracts with social media.

5. FUTURE DIRECTION

This article will contribute to the advancement of scientific inquiry into cybersecurity, specifically by providing a procedural response to the issue of foreseeing future data and activities that will have a substantial impact on security patterns. This study establishes the context for starting to implement regulations for all purposes as stated by the typical security concerns and solutions for data systems. This study combines a number of processes that are related to cybersecurity and may be enhanced in terms of anticipating the operational legitimacy of the methodology of assessment benchmarks. The emphasis on containing, recovering from, and getting rid of weakness is the final point. These are the fundamental patterns and responses to the always growing progress (Panchanatham, 2015).

In the following five years, cybercrime might seriously harm information technology. The researchers claim that they have calculated a loss of about close to 6 trillion dollars. Therefore, there would be excellent opportunity for those who strive to tackle cybercrime-related difficulties and supply the necessary security measures. Since cybersecurity is the future of information technology safety, large firms like CISCO, which is entirely focused on networking technology and is among the top organisations, have millions of opportunities in this field. Additionally, there are numerous opportunities in domains relating to government and defence that can protect a nation's protected data from cyberattacks.

6. CONCLUSIONS

Both the insecurity created by and through this new space and the methods or procedures to make it (progressively) secure are discussed in terms of cyber-security. In order for the "information technology" to be effectively employed by customers, the effort to validate the cyberspace must demonstrate a clear demand. If action is not made to deal with the pervasiveness of the expansion in such a cyber-attack, the terrorist of the future will win the wars without firing a shot by simply destroying the nation's essential substructure. Whether someone is nearby or far away, they might offer an unexpected window into the lives of others.

In one way or another, "cyber-terrorism" may result in fatalities as well as serious harms. Even if social media might be used for cybercrimes, these groups are unable to stop using it because it plays a crucial part in capturing their attention. Numerous innocent lives have been saved as a result of cyber terrorism, which has also caused many homes to deteriorate to the point where it is occasionally causing emotional harm to the impacted families. Cyberterrorism continues to be a major problem in today's society. Not only is the fight against cyberterrorism lagging, but current cybercrime attacks are becoming more aggressive and belligerent. There is an intriguing analogy between terrorism and cybersecurity. It is noticeably more difficult to ensure the security of information, data, and correspondence than it is to hack into a system.

7. REFERENCES

[1]. Kshetri N. The simple economics of cybercrimes, IEEE Secur Priv, 4, pp. 33–39, 2006.
[2]. Maloof, M. A. (Ed.), Machine learning and data mining for computer security: methods and applications. Springer Science Business Media, 2006.
[3]. M. Cross and D. L. Shinder, Scene of the cybercrime.Syngress Pub., 2008.
[4]. N. Dhanjani, B. Rios, and B. Hardin, Hacking: The Next Generation: The Next Generation. O‟Reilly Media, Inc., 2009.
[5]. Y Perwej, K Haq, U Jaleel, F Parwej, "Block ciphering in KSA, A major breakthrough in cryptography analysis in wireless networks", International Transactions in Mathematical Sciences and Computer, India, ISSN-0974-5068, Volume 2, No. 2, Pages 369-385, July-December 2009.
[6]. Fink, E., Sharifi, M., & Carbonell, J. G. "Application of machine learning and crowdsourcing to detection of cybersecurity threats", In Proceedings of the US Department of Homeland Security Science Conference–Fifth Annual University Network Summit, Washington, DC., 2011.
[7]. Greenfield VA, Pa. L. A framework to assess the harm of crim. Br J Crimi., vol. 53, pp. 864–885, 2013
[8]. T. Grant and S. Liles, On the military geography of cyberspace," Proc. Int. Conf. Inf. Warfa, p. 66, 2014
[9]. M. Chertoff and P. Rosenzweig. (Mar. 1, 2015). A Primer on Globally Harmonizing Internet Jurisdiction and Regulations, accessed on oct. 15, 2015.
[10]. Mathieu, T. & Guy, P., "A Framework for Guiding and Evaluating Literature reviews", Communications of the Association for Inf. System, 37(6), pp 6, 2015.
[11]. H. Lin. (May 15, 2015). Thinking About Nuclear and Cyber Con_ict: Same Questions, Different Answers, accessed on Oct. 15, 2015.
[12]. Hernández, A., Sanchez, V., Sánchez, G., Pérez, H., Olivares, J., Toscano, K., & Martinez, V. (2016, March). Security attack prediction based on user sentiment analysis of Twitter data. In 2016 IEEE international conference on industrial technology (ICIT) (pp. 610-617). IEEE.
[13]. Edwards B, Hofmeyr S, Forrest S. Hype and heavy tails: a closer look at data breaches. J Cyber secur 2016;2:3–14.
[14]. Buczak, A. L., & Guven, E ,"A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), pp. 1153-1176, 2016.
[15]. Van Slyke SR, Van Slyke S, Benson ML. The Oxford Handbook of White Collar Crime. Oxford University Press, 2016.
[16]. Mittal, S., Das, P. K., Mulwad, V., Joshi, A., & Finin, T. ,"Cyber twitter: Using twitter to generate alerts for cyber security threats and vulnerabilities", Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 860-867, 2016.