International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Security

Dr. Chandrika G

Assistant Professor, Sarvodaya Institution of Graduate studies

Abstract

Cyber security plays a vigorous role in the area of information technology. Safeguarding the information has become an enormous problem in the current day. The cybersecurity main thing that originates in mind is 'cyber crimes' which are aggregate colossally daily. Different governments and organizations are taking numerous measures to keep these cyber wrongdoings. Other than different measures cybersecurity is as yet a significant worry to many. This paper mostly emphasizes on cyber security and cyber terrorism. The significant trends of cybersecurity and the consequences of cybersecurity are discussed in it. The cyber-terrorism could make associations lose billions of dollars in the region of organizations. The paper also explains the components of cyberterrorism and its motivation of it. Two case studies related to cybersecurity are also provided in this paper. Some solutions for cyber security and cyber terrorism also explain in it.

1. Introduction

Today an individual can receive and send any information be video, or email or only through the click of a button but did s/he ever ponder how safe this information is transmitted to another individual strongly with no spillage of data? The proper response lies in cybersecurity. Today more than 61% of full industry exchanges are done on the internet, so this area prerequisite high quality of security for direct and best exchanges. Thus, cybersecurity has become a most recent issue (Dervojeda, et. all., 2014). The extent of cybersecurity is not merely restrict to verifying the data in IT industry yet also to different fields like cyberspace and so forth. Improving cybersecurity and ensuring that necessary data systems are vital to each country's security and financial prosperity.

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure (Kumar, & Somani, 2018). It alludes to a lot of exercises and measures, both specialized and non-specialized, expected to ensure the bioelectrical condition and the information it contains and transports from all possible threats. This research aims to gather all the information and overview related to cyber-crime and provide the historical facts and perform reports on the analyzed data of different attacks reported everywhere in the last five years. Based on the analyzed information, we would like to provide all the countermeasures that organizations may undertake in order to ensure improved security that would support in defending the organizations from being attacked by the hackers and provide a cyber-security to avoid all risks.

2. Purpose.

The paper provides information about cyber security and cyber terrorism. It covers various information about these topics in its subsections. Trends of cybersecurity and the role of social media in cybersecurity define in this paper. The paper provides some necessary information about cyber terrorism. The components of “cyber terrorism” and the consequences of this terrorism also explain in this paper. There are some examples of case studies those related to cybersecurity. The paper also provides some solutions regarding cyber security and cyber terrorism. It provides some techniques for preventing cyber terrorism. The future study and scope of cybersecurity define in it. Cybersecurity has become a major concern over

the last 10 year in the IT world. In the present world, everybody is facing a lot of problems with cyber crime. As hackers are hacking major sensitive information from government and some enterprise organizations the individuals are very much worried as cyber security assault can bring about everything from wholesale fraud, to blackmail big companies.

The Internet is today's fastest growing infrastructure. In today's technical environment many new technologies are changing mankind. But due to these emerging technologies, we are unable to protect our private information in an efficient way, so the cyber-crimes are drastically increasing on daily basis. Majority of the transactions both commercial and personal are done using the means online transaction, so it is important to have an expertise who require a high quality of security maintaining a better transparency to everyone and having safer transactions. So cybersecurity is the latest issue. Advanced technologies like cloud services, mobiles, E-commerce, internet banking and many more they require a high standards and safer process of security. All the tools and technologies involved for these transactions hold the most sensitive and cruicial user information. So providing the necessary security to them is very important. Improving the cybersecurity and safeguarding the sensitive data and infrastructures are important to every countries top priority security (Panchanatham, 2015).

3. Trends of Cyber Security.

Cyber Security assumes a critical role in the area of data technology. Safeguarding the data have become the greatest difficulty in the current day. The cybersecurity the main thing that raids a chord is cybercrimes which are increasing tremendously step by step (Samuel, & Osman, 2014). Different administrations and organizations are taking many measures to keep these cybercrimes. Additional the different measures cybersecurity is as yet an enormous worry to numerous. Some main trends that are changing cybersecurity give as follows:

3.1. Web servers The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications (Bendovschi, 2015). Web servers are mainly the pre eminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements.

3.2. Mobile Networks The risk of assaults on web applications to separate information or to circulate malicious code perseveres. Cybercriminals convey their code using good web servers they have traded off. In any case, information taking attacks, a considerable lot of which get the deliberation of media, are also a significant risk. Currently, individuals need a more unusual accentuation on securing web servers as well as web applications (Bendovschi, 2015). Web servers are mainly the pre eminent stage for these cybercriminals to take the information. Thus, one should reliably utilize an additional secure program, mainly amid vital exchanges all together not to fall as a quarry for these defilements. 3.3. Encryption It is the method toward encoding messages so programmers cannot scrutinize it. In encryption, the message is encoded by encryption, changing it into a stirred-up figure content. It commonly completes with the use of an “encryption key,” that demonstrates how the message is to encode. Encryption at the earliest reference point level secures information protection and its respectability (Sharma, 2012). Additional use of encryption obtains more problems in cybersecurity. Encryption is used to ensure the information in travel, for instance, the information being exchanged using systems (for example the Internet, online business), mobile phones, wireless radios and so on. 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 capacities. 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.

4. Role of Social Media in Cyber Security Social media has turned into a lifestyle for some individuals. We use it to stay in contact, plan occasions, share our photographs and comment on recent developments. It has replaced email and telephone requires a ton of us. However, similarly as with whatever else on the web, it is imperative to know about the dangers. PCs, cell phones, and different gadgets are priceless assets that furnish people of any age with the extraordinary capacity to connect and collaborate with whatever remains of the world. Individuals can do this in various ways, including the utilization of social media or networking sites. Courtesy of social media, people can share musings, pictures, exercises, or any part of their lives (Gross, Canetti & Vashdi, 2017). They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe. Unfortunately, these networks additionally represent security toward one's PC, protection, and even their security. Social media collection among faculty is soaring as is the risk of assault (Sharma, 2012). Since social media sites are nearly utilized by the majority of them reliably, it has become an excellent stage for cybercriminals for hacking private data and taking significant data.

5. Cyber Terrorism The term “terrorism” can allude to the illegal utilization of power or viciousness against people in order to threaten an administration or its residents and associations which might be to accomplish a political or a malicious site [10]. Terrorism has transformed from the conventional structure to the cyber type of innovation supported terrorism recognized as cyber terrorism. It stays vital issues of the present society. Not just that the battle against terrorism is falling behind, current cybercrime assaults are ending up progressively forceful and confrontational (Sharma, 2012). This terrorism is the utilization of cyber word to dispatch an assault to the essential foundations that the presence of associations and countries entirely depended after that can prompt its shut down.

5.1. Components of Cyber Terrorism A few attacks as cyber terrorism have a few parts which have been distinguished by numerous observational researchers in the exploration network. As indicated by Samuel and Osman (2014) in their hypothetical model recognize the five sections that a “cyber-terrorism” classified they are; the objective of the violence, inspiration and dedication towards the mission to be accomplished when such incident takes place, impact, instruments are utilized to dispatch such assault and attacking’s, area which is nature just as the strategy for activity. It can confidently know by knowing the profile of activities that drive the actions of the culprits (Kumar, & Somani, 2018). The critical issue in “cyber terrorism” is the motivation to complete such an action on the Internet, that outcomes in savagery/damage to people and their property Dervojeda, Verzijl, Nagtegaal, Lengton, & Rouwmaat, 2014). It is by a portion of the segments. The terrorists of the world proceed the upside of the cyber world with solid incentive as a stage with which they can use to dispatch more unusual outbreak. Yunos and Ahmad (2014) said that with the utilization of Information and correspondence innovation, a terrorist could present more noteworthy harms or exact the republic with troublesome conditions because of the interruption of necessary administrations that the “cyberspace terrorist” causes more damage and devastation by the cyberspace than done the conventional strategy for terrorism.

5.2. Motivating Factor of Cyber Terrorism

The motivating factors of cyber terrorism give as follows: 5.2.1. Websites’ Supportive Nature: The internet has viewed as a medium that is exceptionally tremendous, and that can in the meantime draw in light of a legitimate concern for some individuals to join some group of interest. The cyberterrorist prefers the utilization of the website as a result of its robust nature in that it can refer a message to a great many

individuals inside a twinkle of an eye; they consider it to be a stage that is anything but difficult to select absorbed individuals. 5.2.2. Anonymity Nature of the internet: Anonymity is the pivotal element that each evil culprit leans towards with the goal that their character could not be recognizable after playing out their devilish act. The Internet is a sheltered domain just as concealing stage for the terrorist as they can stay unknown so that their personality cannot be known.

5.2.3. Hacking: The overall term of all kinds of unapproved access to any "computer system" network organize is hacking that can occur in any structure all things measured as "cyber murder." A large number of these hackers make use of a "brute force‟ which is the combinations of every single imaginable letter just as numbers and images till they get the password Sreenu, & Krishna, 2017).

Conclusion

Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it (progressively) secure. Exertion to verify the cyberspace should give a definitive need else the "information technology" will not be viably used by clients. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe. The “cyber-terrorism” can in one method or alternate prompts the death toll just as causing severe harms. Though social media can utilize for cybercrimes, these organizations cannot stand to quit utilizing social media as it assumes an essential role in the attention of an organization. Cyber terrorism has guaranteed numerous innocent lives and in the meantime render numerous homes to a condition of the problem that is occasionally coming about to mental injury to the influenced families. Cyber terrorism stays vital issues of the present society. Not just that the battle against Cyber terrorism is falling behind, current cybercrime assaults are ending up progressively forceful and confrontational. Cybersecurity has an intriguing parallel to terrorism. Guaranteeing the security of information, data, and correspondence is impressively harder than hacking into a system.

References

1. Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 24-31. doi:10.1016/S2212-5671(15)01077-
2. Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. EURASIP Journal on Information Security. doi:10.1186/s13635 018-0080-0
3. Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union. On
4. Gade, N. R., & Reddy, U. G. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends Latest Technologies. Retrieved from https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies
5. Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cybersecurity, 3(1), 49–58. doi:10.1093/cybsec/tyw018
6. Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), pp. 175-186.
7. Kumar, S., & Somani, V. (2018). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. International Journal of Advance Research in Computer Science and Management, 4(4), pp. 125-129.