Cyber Security in America

Rahul Reddy Nadikattu*

Vivekananda Journal of Research
January - June 2020, Vol. 9, Issue 1, 166-174
ISSN 2319-8702(Print)
ISSN 2456-7574(Online)
Peer Reviewed Refereed Journal

http://www.vips.edu/vjr.php

Abstract

The following article will substantially focus on understanding cybersecurity. The analysis will focus on the factors leading to the increased cases of cyber-attacks and how to reduce the effects upon the occurrence in the organizations and the business. The article will also look into the impacts of implementing effective cybersecurity measures not only to the organizations but also in America. Additionally, the item will focus on the various ways of improving cybersecurity, among which training of the employees about the emerging technologies will adversely create awareness in the organizations and significantly impact change in the society. The article will also focus on the various challenges that are affecting the effectiveness of cybersecurity in the organizations, and thus, the study of the primary cause of the increased rate of information insecurity. Therefore, the following research will substantially focus on most of the factors that have continued to affect the protection of information systems and the variety of remedies to rectify the situation. Some of the keywords include phishing, malware, spyware, IT, data confidentiality, and cyber-attack.

Keywords *: Cybersecurity, Threats, America, Attacks, Information Technology*

* University of the Cumberlands,Department of Information Technology, 6178 College Station Dr, Williamsburg KY 40769

Introduction

Cybersecurity is the protection of the connected internet systems and appliances, including both the hardware and the software, and the data involved from any cyber-attacks. Primarily, cybersecurity is about the human, the processes, and the technology utilized in cohesion to broadly embrace the reduction of vulnerability and threats, comprehend international engagements and recover policies, law enforcement, and computer networks, among other elements. Cybersecurity refers to the technology that utilizes the network systems and the data or programs; security refers to the protection of the systems, network, and data. Therefore, cybersecurity can as well be defined from the perspective of a body of processes, technologies. Practices that are incredibly designed for the acute protection of the networks, the devices utilized, and data form activities that include theft, attacks, damage, unauthorized access, and unauthorized modifications. As a result of the heavy dependency of the computers, in the modern society and industries in the data storage systems and the transmission of abundantly confidential and critical data, concerning humanity. Cybersecurity is, therefore, an essential element and function that is quite necessary for the insurance of most of the business organizations and business practices (Singh, & Chatterjee, 2017).

Cybersecurity is the set of principles and practices that are adequately designed to protect the computing resources and online-based data from threats that could distort or even release the information to unauthorized persons. Based on the above information, cybersecurity can be categorized as essential to the digital era we live in and thus the need for the privatization of the information, as it is more vulnerable now. Living in a world where all the network systems are intertwined, especially from the banking systems to the government resources and data is computerized for storage, most of it is sensitive, and there is more need for increased security systems on the networks and the devices. In today's society, due to the technological systems' sufficient advancement, cyber-attacks exist as international concerns due to the existence of several hacks to the computers and organizations, endangering the economy globally. (Keys, h Chhajer, Liu, & Horner, 2016).

Overview

In modern society, organizations, and government systems, the improvement of the utilized technologies has posed a significant threat to the security and the confidentiality of most sensitive data in these elements. Through the innovation of better systems of technology, the more they need for the advancement of security increases. Cybersecurity

comprehends everything that primarily concerns the protection of sensitive data, including one's identity, health data, governmental data, and industrial data systems. Cybersecurity ensures protection of the network and the data systems from unauthorized individuals and provides improved information protection and the sustainability of business management. Additionally, cybersecurity is quite essential as it ensures improved confidentiality in the organizations, especially concerning the information about the stakeholders and the improved security on the organization's credentials due to the proper management of the security controls (Kshetri, 2017). In case of breach of data from the organization's computer systems, through improved cybersecurity, there exist faster means of data recovery and retrieval means ensuring the security of the organization and the data from unauthorized people. The computerized systems are protected against viruses, malware, and spyware, and cybersecurity ensures the organization's technological systems are protected against hackers and theft of identities. (Henri, 2018).

However, cybersecurity is quite expensive and costly for the average user companies and individuals. Hence, there exists a higher probability that not all can afford the installations and consistent updates. Additionally, the firewalls are quite tricky for correct configurations, and thus if incorrectly done, the organization's data is risked and vulnerable to viruses and hackers. The installations of the various cybersecurity systems make the computer operations and systems slower than they operated before and thus more costs on time management. However, the benefits reaped from cybersecurity is more important than the costs, and therefore it's better to incur the expenses rather than losing sensitive data to hackers and unauthorized modifications.

Factors affecting cybersecurity

Cybersecurity is an element that is adversely affected by the ever-evolving aspect of computer security. Unlike in the tradition whereby the organizations and the government systems were adequately focused on the management of the known threats, the approach is insufficient in modern society due to the advancement of the risks at a rate that organizations can hardly manage. Today, several factors are the critical drivers for cyber-attacks, including the exploitation of weak systems and increased sabotage with these systems. In the business world, increased rivalry among organizations for illegal business competitions has motivated increased cyber-attacks. Additionally, ideological differences are not limited as causative agents of the increased cyber-attacks today. However, despite the massive increase of the attacks, lack of supportive management systems in the organizations and governments has the implementation and correspondence of cybersecurity policies and

strategies adversely and thus increased attacks.

Moreover, lack of proper education and management to the employees has led to the exploitation of the systems for self-gains. Internationally, the development of the Internet of Things has significantly posed a threat to cybersecurity due to the interconnection of networks globally. The expanded use of the unsecured micro-chips increases the vulnerability of the systems globally, and thus international policies need to be developed and implemented to limit the vulnerability (Mendel, 2017).

Another factor that poses an increased threat to cybersecurity with the increased cybercrime is the increased profitability and the ease of commerce from the dark web and thus a great motivation to the hackers. Primarily, operations in the wicked web lack policies and government regulations, and this increases the rate at which individuals make profits then costs. Cybercriminals are growing more sophisticated, consistently an aspect that makes them change their objectives, the effects on the firms attacked, and the approaches and strategies they use in the various security systems. As a result, the more the attacks, the more the options they develop, posing more danger to cybersecurity globally. Additionally, information theft in the current society is the most expensive and speedily growing cybercrime. Also, data theft is viewed as adequately motivated by the increased exposure of sensitive information to the cloud-based systems making it more vulnerable. As a result, the lack of organizations to partner for the widespread development and improvement of standard security systems in the defense and elimination of vulnerability has increased the danger of cyber-attacks. (Hagy, 2017).

Egotistical is another factor that is posing a challenge to cybersecurity. Apart from financial gains and quest for corporate information from the dark web, a cyber attacker is intentionally attacking organizational information systems for recognition acknowledgment of the skills and abilities in IT in the defeat of the security systems and standards implemented. Attacks from the dark web are on the rise due to power and ease, making the attacks more on the increase due to the ease of compromising the digitalization from their rooms, unlike the physical robberies and assaults. Also

Management of cybersecurity

Cybersecurity is a risk that can adequately be managed, just like any other risk management aspects globally. Cybersecurity management requires strategic identification of the risks and the factors leading to the vulnerability of security. Also, the management of cybersecurity involves the application of the most effective administrative measures

and sophisticated solutions to ensure the information is adequately and well protected. In consideration of the best risk management protocol, one must consider the culture of cybersecurity management for the entire organization. Through the specific definition of the authoritative structure and the intentions of the communication intention of the firm, the administration has to ensure the application of efficient leadership accountability and proficiency. (Gonzalez, n.d.).

For the cyber-attack mitigation and management procedures, the organization has to consider the limited application of the computerized devices that have access to internet network systems. Also, the incorporation of the organization has to consider the establishment of the anti-virus programs as well as the end-point security systems to avoid interruption of the stored data by the viruses. Another essential management program is the limitation of the administrative rights to access the most sensitive systems of operation in the organization and, thus, the implementation of ethical practices with the employees. Advancement of the data encryption systems is quite essential for mitigation of the cyber-attacks risks through the strategic and systematic applications for the protection of the data from cyber attackers. (Ackerman, 2017). Primarily, advanced encryption of data involves the advanced management systems as well as the use of the algorithms that adequately helps in the reduction of the risk exposure to the cyber-attacks (Mukhopadhyay, 2017). More importantly, data encryption helps protect information against external breaches. For internal data theft, the firm has to implement the removable media systems for the protection of data from the insiders.

Redaction is another risk management system that involves the protection of the data simultaneously with the ability to ability to share the data. With the implementation of the redaction policy, the firms can adequately share minimal information, concealing sensitive data. Another primary strategy for risk management strategies is the element-level security that involves the organization's customs towards the protection of the data. Cyber risk management is quite essential as it helps in the mitigation and prevention of the attacks. The implementation of effective cyber risk management strategies helps identify possible threats to the organization's data, and thus, the development of strategic plans to counter the attacks and the consequences.

Impacts of cyber-attacks

Lack of sufficient cybersecurity results in massive damage to the individuals and businesses and organizations. Regardless of the organization's size, or leadership, all firms

have to ensure all the involved players will understand the impacts of cyber-attacks, and how to mitigate the effects effectively. Generally, one of the most severe consequences of cyber-attack is the ruined public reputation towards the organization despite the size. Vulnerability to the attack makes the organization seem unaccountable to the customers due to insufficient security measures. Thus the company may end up losing a lot of its clients to the competitor firms. The clients' lack of trust mounts to the loss of the initial and the current customers in the firm to the rival companies and, thus, reduced sales in the company. Additionally, ruined reputation leads to increased economic costs to the organization due to the theft of the intellectual information, property, and thus critical disruption of the ordinary business operations in the firm and the adverse costs of rectifying the encountered damage on the systems (Kamiya et al. 2020).

The regulatory costs incurred in the firm are another significant negative impact that results from cyber-attacks in the firm. Regulatory costs were created from the breach of data law and the GDPR laws. Thus the organization is liable for the regulatory fines that emerge as a result of the attacks. The costs of investigation are massive as cases of data hacks can hardly be administered by the systems. Therefore, the organization is coerced to hire external forensic investigators, and depending on the size of the hacked data, and the costs are immense. (Gonzalez, n.d.) Also, in the case that the hack occurred to criminally weak security systems of the organization, the organizational clients have the right to sue the management for exposing their data. Thus the company has to pay for the legal defense. With the legal defense costs, the lawyers are quite expensive to higher, and in the United States, the prices of legitimate defense rise quickly.

New implementations on cybersecurity

There are several ways by which the organizations can improve the information and computer security and thus enhance reduced risks of the occurrence of cybercrimes within the organization. (Gherman, 2017) Among the widespread measures, the organization needs to consistently educate the employees on the various effects of social engineering and the several common scams in the internet networks such as phishing emails. Through such pieces of training, the employees are made aware of how to avoid the adverse consequences and hence to protect the organization from the occurrence of the risks. Also, through consistently making them aware of the recent attacks, the employees are cautioned against engaging in malicious acts that can affect the organization's reputation. Also, training them on the various advanced technological systems helps them to know how they operate effectively and involve in the maintenance of the organization's culture. .(Faggella,

Gigliotti, Mezzacapo, & Spacone, 2017).

The organization can also focus on the investment in tools and systems that help in limiting the information loss. Implementation of such systems helps in monitoring of the third and the fourth party vendor risks in the organization. It hence helps in the consistent scans of the information exposure and prevention of loss of sensitive data. Additionally, the organization can ensure consistency in monitoring intrusion through the use of detectors of unusual activities with the network systems. Through such detections, the organization can raise the alarm for the potential breach of security. Implementation and consistent change of the strong passwords, and controlled access help the firm build an influential protection culture through different systems. Application of firewalls, acts as safeguards between the computer devices and the internet connections and thus hinders and prevents the spread of the cyber threats and attacks even with the viruses. (Hagy, 2017).

How cybersecurity helps America

In the United States of America, integration of high-quality security systems on the computer devices and information systems has helped maintain their national security and, thus, promote American prosperity. Enhancement of cybersecurity in America has become a significant endeavor in the national security systems and the economy and the defense systems of the society. Through the implementation of modernized cybersecurity systems, the Americans have achieved more robust measures and, hence, have to make more defensive standards on their business from cyber-attacks. (Hayward & Quinn, 2016). Through the digitalized protection measures, the Americans have achieved better services in ensuring the potential cyber threats do not risk the employees. (Shinde & Ardhapurkar, 2016)

Also, America has realized high productivity and massive growth in terms of business due to the adoption of effective cybersecurity strategies that have eliminated the possibilities of attacks to the companies. (National Institute of Standards and Technology, 2018). As a result, the nation has relatively increased its output with the implementation of advanced technological systems and, thus, sustainability. Through the implementation of the latest cyber protection devices, U.S., based organizations have ensured the protection of the consumers in the markets through the sufficient protection of their data and credentials (McDermott, 2018). Through such acts, American government systems and organizations have secured accountability and reliability aspects to their customers through safety measurements placed on their data. The nationality has ensured the sustainability

of the organizations through the protection of the business websites as the cyber breach occurrence would cause massive damages to the individuals concerned. (Shedden, Ahmad, & Ruighaver, 2018).

Conclusion

Despite the increasing technological advancements posing a threat to cybersecurity globally, organizations and government systems need to embrace measures that can consistently counter the emerging risks in the field. By continuously improving the technology in the various institutions, the firms can eventually develop means to counter cyber-attacks and thus protect sensitive data. (Henri, 2018). Upon the implementation of the necessary measures to ensure cybersecurity, the future of information technology and security will be countered and well managed for future generations. (Gleichauf, et al. 2017)

References

Ackerman, P. (2017). Industrial Cybersecurity: Efficiently secure critical infrastructure systems. Packt Publishing Ltd.

Brianna Keys, Aashish Chhajer, Zilong Liu, and Daniel Horner. (2016). A Framework for Assessing Cyber Resilience: A Report for the World Economic Forum: Retrieved from: https://bloustein.rutgers.edu/a-framework-for-assessing-cyber-resilience/

Rahul Reddy Nadikattu, “New ways of Implementing Cyber security in America”, Journal of Xidian University, Vol.14 Issue 05, pp 6004-6015, https://doi.org/10.37896/jxu14.5/651

Faggella, M., Gigliotti, R., Mezzacapo, G., & Spacone, E. (2017). Graphical dynamic trends for earthquake incidence response of plan-asymmetric systems. In COMPDYN 2015, 5th ECCOMAS Thematic Conference on Computational Methods in Structural Dynamics and Earthquake Engineering.

Gherman, L. (2017). Information Age view of the OODA loop. Review of the Air Force Academy, (1), 69.

Gleichauf, R. E., Randall, W. A., Teal, D. M., Waddell, S. V., & Ziese, K. J. (2017). U.S. Patent No. 6,301,668. Washington, DC: U.S. Patent and Trademark Office.

Gonzalez, M. (n.d.). Incident Response Tools. Retrieved from https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools.

Hagy, D. W. (2017). Investigative Uses of Technology: Devices, Tools, and Techniques. National Institute of Justice. Retrieved from: https://www.ncjrs.gov/pdffiles1/nij/213030.pdf

Hayward, L Quinn, M. (2016). It's Not if but When: How to Build Your Cyber Incident Response Plan. Retrieved from https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1506371074.pdf

Henri, V. (2018). Key Roles and Responsibilities for your Incident Response Team. Retrieved October 29, 2019, from https://www.hitachi-systems-security.com/blog/roles-responsibilities-incident-response-team/.

Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy, 41(10), 1027-1038.

McDermott, J. P. (2018). Attack net penetration testing. In Proceedings of the 2000 workshop on New security paradigms (pp. 15-21).

Mendel, J. (2017). Smart grid cybersecurity challenges: Overview and classification. E-mentor, 68(1), 55-66.

Mukhopadhyay, D. (2017). Cryptography: Advanced Encryption Standard (AES). Encyclopedia of Computer Science and Technology, 279.

National Institute of Standards and Technology (2018). Computer Security Incident Handling Guide. National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Shedden, P., Ahmad, A., & Ruighaver, A. B. (2018). Organizational learning and incident response: promoting active learning through the incident response process.

Shinde, P. S., & Ardhapurkar, S. B. (2016). Cybersecurity analysis using vulnerability assessment and penetration testing. In 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) (pp. 1-5). IEEE.

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.