Analysis of the Effectiveness of Current Cybersecurity Protocols in Organizations

Syeda Hajira Kawsar

syedakawsar@gmail.com

Abstract

The assignment will focus on a detailed assessment of the effectiveness of existing cybersecurity protocols in light of businesses. Notably, cybersecurity is imperative today for small to large-scale corporations. The reason is that data is most important, and so for its protection from malicious users online, cybersecurity protocols are essential. Hence, the assignment takes into account multiple sources & delves into the world of cybersecurity protocols, the CIA Triad, and even five main pillars of the cybersecurity framework. Additionally, in the analysis section, the assignment explores the main pros and cons of the protocols. In the end, it underlines some findings based on the examination of current cybersecurity protocols. It suggests improvements to be made in the same for better usage, data protection, and higher organizational growth in all senses.

Keywords: Cybersecurity, CIA Triad, Cybersecurity Protocols, Benefits, Limitations

Introduction

Organizations have tons of data & resources to boost their operations, improve customer experience, and ensure business growth. However, cybercrimes are making it difficult for them to protect their assets. So, the cybersecurity protocols are leveraged by them to prevent digital threats & ensure asset protection. The assignment here dives into an overview of cyber security & mainly explores the analysis of cybersecurity protocols within organizations today. From merits to limitations of the protocols including chief findings, the assignment is based on thorough research.

Overview of Cybersecurity

As per our understanding, it can be said that cybersecurity is an approach that focuses on the safety of confidential information. However, it has been found during the research that cybersecurity not only safeguards data but also emphasizes the protection of online communication, systems, as well as technological infrastructure from external threats [1]. It is worth noting that as a result of cybersecurity, operational efficiency strengthens, and user satisfaction can be ensured. In addition to this, research opines that cybersecurity significantly relies on three chief elements. These include "confidentiality" meaning authorized data access, "integrity" meaning authorized modifications in the system, and eventually "availability" meaning timely data availability for users.

Figure 1. CIA Triad

(Source: [6])

Other than the triad, cybersecurity is based upon a cybersecurity framework that is used by organizations around the world to boost their cybersecurity. To make certain of robust cybersecurity within firms of all sorts, it is crucial to follow the framework's five key pillars in order. Before delving into that, it is vital to pinpoint that the cybersecurity framework is produced by the rigorous work of the National Institute of Standards and Technology, US [2]. Nevertheless, the first pillar is "identify" for which the responsibility of the organization is to assess assets, risks, business environment, and governance practices. Further, the second pillar is "protect" meaning safeguarding sensitive data & assets via solutions like access control, maintenance, and training.

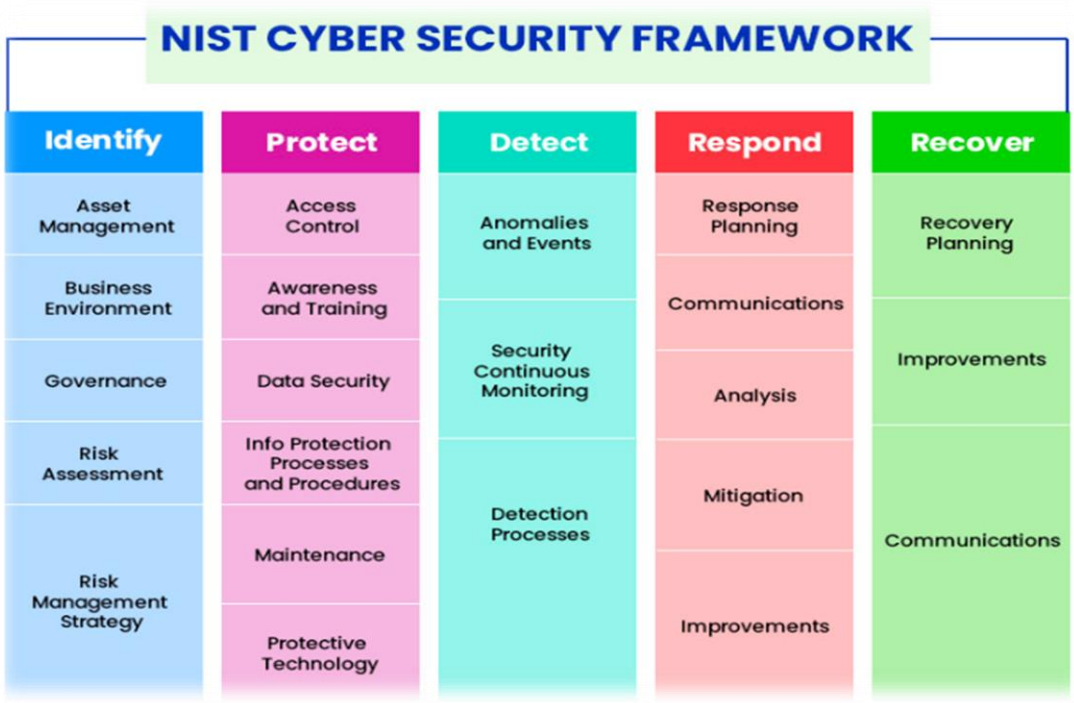

Figure 2. NIST Cybersecurity Framework

(Source: [7])

Moving forward, the third pillar is “detect” emphasizing detection of security bottlenecks through regular monitoring. Then, the fourth pillar is “respond” focusing on responding to cyber threats by thorough planning, analysis, and reporting. Last but not least, the fifth pillar is “recover” which pinpoints recovery planning& continuous improvement to get back to normal operations. It can be said that by using the cybersecurity framework, organizations today get to understand digital risks. Additionally, it boosts stakeholder communication and ultimately aids in shaping the security posture of the company.

Current Cybersecurity Protocols in Organizations

No matter how small or big a company is size-wise, it needs to utilize a solid plan of action, strategies, or protocols to secure its overall network & operations. In simple terms, cybersecurity protocols can be elucidated as those techniques that aid organizations in ensuring safety against data breaches and other cybersecurity challenges. Today, it is not impossible for individuals to infiltrate organizational networks as they just have to install some key protocols to be used against organizational websites [3]. Henceforth, it is vital to leverage cybersecurity protocols, more than one, and update them from time to time.In light of the cybersecurity protocols, it can be said that it is vital to “educate & aware” employees within the organization foremostly. It can be added here that open conversations & discussions with the workforce on topics like cyber threats & cybersecurity solutions should be conducted.

Furthermore, organizations today implement "multi-factor authentication" which serves as an additional protective layer for network safety. The technique comprises robust additional elements like facial recognition or even a user fingerprint. So if the account's password is in the intruder's hands, the additional credential has to be filled up to access data, thus preventing security threats.

More so ever, organization seeks to implement "firewalls" to boost the security of their network infrastructure. Advanced firewalls are known to prevent different cyber-attacks including application-layer threats. In addition, the advanced firewalls can identify & respond to cybercrimes and ensure intrusion prevention [4]. Further, organizations emphasize "data backups" regularly. Despite acting and making strategies for cyber-attack prevention, there are still possibilities of experiencing such threats in organizations. So organizations back up their data continuously, in a day-to-day manner, weekly manner, or monthly manner. All the operational data, consumer information, financial data, and other information is backed up &stored in the cloud or other storage devices. As a result, it becomes easier to access such data during distressful times like data breaches or malware attacks.

Eventually, organizations use stronger & unique passwords, update their system & software, and also train their workforce to give strong yet effective responses to cyber-crimes. The cybersecurity protocols ensure data safety, network safety, prevention of hacking, and safer communications. However, it is crucial to examine the current cybersecurity protocols discussed here, in general, to find out how effective they are.

Analysis of Current Cybersecurity Protocols

- **Benefits**

Research opines that cybersecurity protocols are so powerful that they aid, in protecting organizations from cyber vulnerabilities. There are different types of cyber threats like SQL injection, malware attacks, phishing, and more. Yet by implementing security layers and using the protocols & framework, organizations can protect their sensitive data and financial information. Moreover, it can be noted that due to the rise in cyber-crimes, governments around the world have implemented stricter cybersecurity regulations. In case businesses & corporations fail to adhere to the government policies related to cybersecurity, they

have repercussions and even pay penalties to the administration [5]. So, to avoid penalties and other legal issues, companies today ensure compliance with evolving cybersecurity regulations. In addition, cybersecurity protocols make certain that financial transactions safely take place online. For instance, individuals & businesses today can pay bills online, shop from online retailers like Amazon, and get details regarding their bank accounts with utmost protection. Subsequently, cybersecurity protocols help in identifying financial scams as well. As a result, organizations develop stronger strategies to deal with fraud & stay cautious. Eventually, cybersecurity protocols also help protect user identity associated with their names, credit card details, and even residential addresses.

- **Limitations**

Despite the various advantages of the protocols, their drawbacks cannot be understated. Small and medium-sized businesses find it challenging to apply solid cybersecurity measures. One of the reasons behind this is its expensive cost. For example, deploying firewalls as well as cybersecurity software demands lots of money, thus posing a financial strain on companies with tight budgets. Furthermore, it is not easy to maintain the cybersecurity protocols or solutions because they require additional costs. More so ever, it is worth mentioning that cybercriminals are becoming more and more advanced in terms of their knowledge & skills. They are not fearful at all and are working on new ways to break security protocols efficiently. Even the best security measures fail and at times, businesses themselves do not put much effort into implementing the cybersecurity layers. Next, cybersecurity protocols are complex and cannot be easily comprehended by all types of organizations. Advanced knowledge, as well as skills, are required in many companies to analyze risks, manage them, and respond to them effectively. Ultimately, some cybersecurity protocols are known to be tracking user data. This poses privacy issues and thus dissatisfies the users as without their consent, organizations may monitor their online behavior. This can eventually generate a rift between firms & customers.

Findings

From preventing cyber threats to ensuring data & asset privacy, the cybersecurity protocols have it all. Be it encryption, multi-factor authentication, firewalls, data backup, or any other protocol, it is imperative for organizations to foremostly examine their security posture, and then make use of these protocols as per needs. It has been found from the analysis that cyber security protocols are effective today, within organizations, but they have their limitations. Henceforth, to boost the protocols, it is important to keep working on them, improving them, and implementing them. Consequently, the influence of the cybersecurity protocols will be that they will ensure data safety, regulatory compliance, stakeholder satisfaction, data management, improved customer experience, integrity maintenance, and operational continuity.

Conclusion

In the final words of the assignment, it can be said that cybersecurity has become one of the most prevailing issues for organizations out there. Scams, malware attacks, ransomware, and other cyber threats have become common and resulting in reputational & financial damage to organizations. Henceforth to ensure cyber security in all aspects, firms & corporations need to assess their current security health. Based on the findings, they can layer up the overall network & assets with protective measures like firewalls, intrusion detection, and more. As a result, better relationships between the organizations and their clientele will take place & asset confidentiality, integrity, and availability will be guaranteed.

References

[1] F. Zuccari, “An introduction to Cybersecurity,” *www.linkedin.com*, 2023. https://www.linkedin.com/pulse/introduction-cybersecurity-fabrizio-zuccari/

[2] B. ABENE, "NIST Cybersecurity Framework version 2.0, what's new?" *www.linkedin.com*, 2023. https://www.linkedin.com/pulse/nist-cybersecurity-framework-version-20-whats-new-bertin-abene-cissp/

[3] Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments,” *Energy Reports*, vol. 7, no. 7, pp. 8176–8186, 2021, doi: https://doi.org/10.1016/j.egyr.2021.08.126.

[4] Gunasundaram, “7 Cyber Security Practices Every Business Must Employ,” *Medium*, 2021. https://medium.com/gunasundaram/7-cyber-security-practices-every-business-must-employ-abbf8f7ce5f0

[5] M. Aathinathan, “The Pros and Cons of Cybersecurity: What You Need to Know,” *www.linkedin.com*, 2023. https://www.linkedin.com/pulse/pros-cons-cybersecurity-what-you-need-know-mageshkumar-aathinathan-v5wgc/

[6] Ledesma J. (June 2023) What is CIA Traid? Varonis.com. https://www.varonis.com/blog/cia-triad

[7] Jaiswal M. (2022, November). Leveraging the NIST Cybersecurity Framework for business. WeSecureApp :: Securing Offensively. https://wesecureapp.com/blog/leveraging-the-nist-cybersecurity-framework-for-business/.