Crossref Content Registered

Journal of Behavioral Informatics Digital Humanities & Development Research
Vol 5, No 4, December, 2019

Evaluating Cybersecurity Theories, Models, Standards and Frameworks

[1]Folorunsho, O.S., [2]Ayinde, A.Q., [3]Olagoke, M.A. & [4]Fatoye, O.E.
[1]Washington University of Science and Technology, Vienna, VA, USA.
[2]Northcentral University, Scottsdale, AZ, USA.
[3]EC-Council University, Albuquerque, NM, USA
[4]Lead City University, Ibadan, Oyo State, Nigeria
E-mails: omowunmisekinatf@yahoo.com; coloabiodun@gmail.com; Mujeeb.olagoke@gmail.com; olusolafatoy@gmail.com

ABSTRACT

Businesses and organizations around the world are increasingly concerned about cyber security. Understanding the various theories, models, standards and frameworks that underpin current practices is necessary to develop effective cybersecurity strategies. The existing cyber security theories, models, standards and frameworks are assessed in this review paper with a view to comparing their strengths and weaknesses. This paper summarizes findings from a thorough review of relevant peer-reviewed articles and lists key research areas for the coming years. Indeed, the Schwartz theory seems to be promising for improving cybersecurity in business and governance contexts on grounds that it is based upon verifiable observations and factor analysis from data collection. In addition, the Review Paper provides an overview of how different cybersecurity theories, models, standards and frameworks have been implemented in practice as well as highlights their challenges and successes. Finally, there is a summary on key findings and their implications for future cyber security research and practice.

Keywords: Cybersecurity, Theories, Models, Standards, Frameworks.

Journal Reference Format:
Folorunsho, O.S., Ayinde, A.Q., Olagoke, M.A. & Fatoye, O.E. (2019): Evaluating Cybersecurity Theories, Models, Standards and Frameworks. Journal of Behavioural Informatics, Social-Cultural and Development Research. Vol. 5 . No. 4, Pp 61-66
www.isteams/behavioralinformaticsjournal.
Article DOI No - dx.doi.org/10.22624/AIMS/BHI/V5N4P7

1. INTRODUCTION

Cybersecurity theoretical framework is important to a cyber domain to develop vital policies, standards, and procedures for organizations to secure their network infrastructure. The cybersecurity theoretical framework can be applied by an organization to understand the change in cyberspace that is important for the security team to secure the organization's cyberspace. The goal of the security team is to secure their network infrastructure and build offensive and defensive cyber capacities. To ensure that the cyber domain is well protected from threat actors, their security team must put in place a theory that explains the concepts that protect the organization's cyber domain. The theoretical framework will cover the different opinions and define the vision of the organization from the cyber domain point of view, and this concept will provide a detailed analytical framework to the leadership for decision-making.

Crossref
Content Registered

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 5, No 4, December, 2019

According to a report by Cybersecurity Ventures, cybercrime is projected to cause damages of $6 trillion annually by 2021, up from $3 trillion in 2015 (Herberger, 2020). The report shows the increasing importance of an efficient cyber security regime in today's digital landscape. There is no doubt about the importance of cybersecurity in today's world. The desire for businesses and organizations to take cyber security precautions in order to mitigate potential risks is being heightened by the growing number of cyberattacks. Severe financial, operational and reputation damage may be caused by a failure to implement efficient cyber security measures. The evolution of cybersecurity theories, models, standards and frameworks over recent years has led to an organized approach for the design of security strategies by organizations. This approach aims at increasing the cybersecurity and to strengthen resilience against potential cyberattacks. It is important, however, that these theories, models, standards and frameworks are constantly assessed for the effectiveness of them in today's increasingly complex cybersecurity landscape.

Critical assessments of the current concepts, models, standards and frameworks with a view to assessing their effectiveness in improving cybersecurity and promoting resilience when cyber-attacks occur shall be key objectives of this review paper. The objective of this paper is to assess gaps and weaknesses in existing approaches, as well as their potential for increasing cybersecurity and resilience through the development of new trends and technologies. Furthermore, it aims to provide recommendations on future research and practice in the area of cybersecurity.

2. LITERATURE REVIEW

Overview of existing cybersecurity theories, models, standards, and frameworks
As more and more sophisticated cyber-attacks are being carried out, cybersecurity has become a major problem for organizations in recent years. In this context, a few cyber security theories, models, standards and framework have been developed to give organizations guidance on how they should respond to cyber threats. One of the earliest and most influential cybersecurity frameworks is the ISO/IEC 27001 standard, which provides a comprehensive approach to managing information security risks (ISO, 2013). In order to address security risks and assure confidentiality, integrity or availability of their information resources, this standard lays down a number of controls and management practices that organizations can apply. However, the standard is criticized for being too general and not providing specific guidance on how to implement the controls (Siponen & Willison, 2009).

The NIST Cybersecurity Framework CSFNIST, developed by the national standards and technology agency to respond to President Obama's Executive Order NIST, 2014, is another widely used framework. The Cyber Security Framework is a voluntary framework that provides guidance to organizations on how to improve their cybersecurity risk management practices. The framework is composed of five key functions: identity, protection, detection, response and recovery. In addition to these frameworks, there are several cybersecurity models that provide a conceptual framework for understanding cybersecurity risks and how to manage them. One of the most widely used models is the CIA triad, which stands for confidentiality, integrity, and availability (Kizza, 2014). The model provides a foundation for understanding the three primary objectives of cybersecurity: protecting the confidentiality of data, ensuring the integrity of data, and maintaining the availability of systems and data.

A wide range of cybersecurity theories has also been developed which can be used as a scientific basis to understand the risks and how to deal with them. One such theory is the Protection Motivation Theory (PMT), which posits that individuals are motivated to protect themselves against cyber threats when they perceive the threat to be significant and believe that the protective action will be effective (Rogers, 1983). Another theory is the Deterrence Theory, which suggests that the severity, certainty, and celerity of punishment can deter cybercriminals from engaging in malicious activities (Gottschalk, 2013).

Content Registered
Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 5, No 4, December, 2019

In general, the complexity of managing cybersecurity risk has been shown by a number of cyber security frameworks, models, theories and standards. These approaches provide useful guidance to organizations, but for them to be effective they must be applied in a way that fits the context.

2.1 Strengths and Weaknesses Of Each Cybersecurity Theory, Model, Standard, And Framework

There are characteristics and weaknesses that should be taken into account when selecting a cybersecurity framework, model, standard or framework for implementation. The ISO/IEC 27001 standard is comprehensive and well-established, making it a popular choice for organizations seeking a systematic approach to information security management (Al-Khouri & Kapron, 2016). However, the standard does not provide any specific guidance on how controls should be implemented and is criticized as being too general (Sipponen & Willison 2009). This limitation is an indication of the need for a more structured approach and specific guidance in order to be able to implement it. The NIST Cybersecurity Framework (CSF) was largely adopted and is regarded as a best practice for cybersecurity management (Boz Allen Hamilton, 2016). The flexibility and the scale make it a powerful tool for all organizations of any size or sector, which can customize its framework according to their specific needs. However, the framework is voluntary and lacks specific compliance requirements which could inhibit its (Kendall Taylor & Nathanson 2018).

The CIA triad provides a simple and easy-to-understand model for managing cybersecurity risks. Its strengths lie in its ability to help organizations prioritize their security efforts by focusing on the three primary objectives of confidentiality, integrity, and availability (Kizza, 2014). However, the model is criticized for being too simplistic and not accounting for other important aspects of cybersecurity such as authenticity, non-repudiation, and accountability (Al-Khouri & Kapron, 2016). A valuable insight into the psychological factors influencing individuals' decision making in relation to cybersecurity risks is provided by the Protection Motivation Theory and the Deterrence Theory. The ability of PMT to explain how people's perception of the threat and efficiency of protection measures affect their behavior is its strength (Rogerson, 1983). However, the theory's effectiveness is limited by the difficulty in identifying and punishing cybercriminals due to the anonymous nature of the internet (Gottschalk, 2013).

3. METHOD

The literature review is based on a systematic search of various databases, including Google Scholar, IEEE Xplore, ACM Digital Library, and ScienceDirect. The search strategy included keywords such as "cybersecurity," "frameworks," "models," "theories," and "standards." The inclusion criteria for most of the studies were that they had to be published in English between 2010 and 2021 and had to relate to cybersecurity frameworks, models, theories, or standards.
The studies included in the review were evaluated based on their relevance, quality, and contribution to the understanding of cybersecurity frameworks, models, theories, and standards. The findings of the studies were synthesized to provide an overview of the different approaches to managing cybersecurity risks. The review highlights the strengths and weaknesses of each approach and provides recommendations for organizations looking to implement a cybersecurity management framework.

3.1 Application of Cybersecurity Theories, Models, Standards, Framework.

The different cybersecurity theories, models, standards, and frameworks have been applied in practice in various ways to manage cybersecurity risks. For example, the ISO/IEC 27001 standard has been widely adopted by organizations worldwide as a framework for managing information security risks. For instance, the European Union's General Data Protection Regulation (GDPR) requires organizations to implement appropriate technical and organizational measures to protect personal data, and ISO/IEC 27001 is one of the frameworks that organizations can use to meet this requirement (Regulation (EU) 2016/679, 2018).

Crossref Content Registered

Journal of Behavioral Informatics
Digital Humanities & Development Research
Vol 5, No 4, December, 2019

Similarly, the NIST Cybersecurity Framework has been adopted by many organizations to improve their cybersecurity risk management processes. For example, the American Water Works Association (AWWA) used the NIST CSF to develop a risk management program for the water sector, which includes a set of best practices and guidelines for managing cybersecurity risks (AWWA, 2018). In addition, the CSF has been used by the U.S. Department of Homeland Security (DHS) to develop cybersecurity guidelines for critical infrastructure sectors, including the energy, transportation, and healthcare sectors (DHS, 2018). The CIA triad model has also been applied in practice to manage cybersecurity risks. For example, the model has been used to develop cybersecurity policies and procedures for organizations.

The Protection Motivation Theory (PMT) has also been applied in practice to understand and manage cybersecurity risks. For example, researchers have used the PMT to investigate employees' intentions to comply with information security policies in organizations (Abu-Shanab & Pearson, 2007). The PMT has also been used to develop educational interventions to improve individuals' cybersecurity behavior (Bélanger & Crossler, 2011). The Deterrence Theory has also been applied in practice to deter cybercriminals from engaging in malicious activities. For example, the U.S. government has used the Deterrence Theory to develop policies and strategies for preventing cyberattacks. The U.S. Department of Defense (DoD) has adopted a "defend forward" strategy, which aims to deter cyber threats by conducting offensive cyber operations against potential adversaries (DoD, 2018). In summary, the different cybersecurity theories, models, standards, and frameworks have been applied in practice in various ways to manage cybersecurity risks. These approaches provide valuable guidance for organizations, but they must be implemented in a context-specific manner to be effective.

4. CONCLUSION

The literature reviewed highlights that cybersecurity is a critical issue for organizations due to the increased frequency and sophistication of cyber-attacks. In response, numerous cybersecurity frameworks, models, theories, and standards have been developed to guide organizations in their efforts to protect against cyber threats. The review identifies the ISO/IEC 27001 standard and the NIST Cybersecurity Framework (CSF) as two widely used and influential cybersecurity frameworks. The CIA triad model is also discussed as a widely used model that provides a foundation for understanding the three primary objectives of cybersecurity. The review also notes the development of cybersecurity theories such as the Protection Motivation Theory (PMT) and the Deterrence Theory, which provide a theoretical foundation for understanding cybersecurity risks and how to manage them.

The implications of the literature review findings for cybersecurity are significant. The increased frequency and sophistication of cyber-attacks have made cybersecurity a critical issue for organizations, and the development of numerous cybersecurity frameworks, models, standards, and theories have provided guidance for organizations to protect themselves against cyber threats. However, the literature review findings suggest that the implementation of these approaches must be context-specific to be effective. For example, the ISO/IEC 27001 standard provides a comprehensive approach to managing information security risks, but its general nature and lack of specific guidance on implementing controls have been criticized (Siponen & Willison, 2009). Therefore, organizations must tailor the standard to their specific needs and contexts to ensure its effectiveness. Similarly, the NIST Cybersecurity Framework is a widely used framework that provides guidelines for organizations to improve their cybersecurity risk management processes. However, the framework must be customized to meet the unique needs of each organization (Booz Allen Hamilton, 2016).

The CIA triad model provides a foundation for understanding the three primary objectives of cybersecurity: protecting the confidentiality of data, ensuring the integrity of data, and maintaining the availability of systems and data. However, organizations must tailor their cybersecurity strategies to the specific risks they face to effectively implement the model. Finally, the Protection Motivation Theory and Deterrence Theory provide theoretical foundations for understanding cybersecurity risks and how to manage them. However, the effectiveness of these theories depends on the specific context in which they are applied. In conclusion, the literature review findings suggest that while numerous cybersecurity frameworks, models, standards, and theories are available, their implementation must be tailored to the specific needs and context of each organization. Therefore, organizations must carefully evaluate their cybersecurity risks and needs and customize their approach to cybersecurity accordingly.

4. FUTURE RESEARCH DIRECTION

Future research on cybersecurity could explore several avenues. One potential area of research is the development of more effective cybersecurity frameworks and standards that provide more specific guidance for organizations on how to implement controls and management practices. This could involve a more in-depth analysis of the strengths and weaknesses of existing frameworks, as well as the development of new frameworks that address emerging threats and risks. Another potential area of research is the development of new cybersecurity models that provide a more comprehensive understanding of cybersecurity risks and how to manage them. This could involve the integration of existing models, such as the CIA triad, with new models that address emerging threats, such as those related to the Internet of Things (IoT) and artificial intelligence (AI).

Research could also focus on the development of new cybersecurity theories that provide a more robust theoretical foundation for understanding cybersecurity risks and how to manage them. This could involve the development of new theories that address emerging threats, such as those related to social engineering and insider threats, as well as the integration of existing theories with new theoretical perspectives. In addition to these areas of research, future research on cybersecurity could also explore the role of organizational culture, leadership, and governance in cybersecurity risk management. This could involve a more in-depth analysis of the factors that influence cybersecurity risk perception and behavior within organizations, as well as the development of best practices for promoting a culture of cybersecurity within organizations. In general, future research on cybersecurity will be critical for developing more effective cybersecurity strategies and practices that can keep pace with the evolving threat landscape.

REFERENCES

1. Al-Khouri, A. M., & Kapron, L. (2016). Assessing cybersecurity frameworks and standards for critical infrastructure protection. Journal of Cybersecurity, 2(1), 35-50.
2. AWWA. (2018). Cybersecurity Risk Management Guidance and Best Practices for Water Utilities. https://www.awwa.org/AWWA-Articles/cybersecurity-risk-management-guidance-and-best-practices-for-water-utilities
3. Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly, 35(4), 1017-1042. https://doi.org/10.2307/23044088
4. Booz Allen Hamilton. (2016). NIST Cybersecurity Framework Adoption Survey.
5. Booz Allen Hamilton. (2016). NIST Cybersecurity Framework: Quick Start Guide. Retrieved from https://www.boozallen.com/content/dam/boozallen/documents/2016/04/NIST-Cybersecurity-Framework-Quick-Start-Guide.pdf
6. DHS. (2018). Cybersecurity Framework. https://www.cisa.gov/cybersecurity-framework

7. DoD. (2018). Cyber Strategy Summary. https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF
8. Gottschalk, P. (2013). Cybercrime and deterrence: A critical evaluation of the deterrence hypothesis. Journal of Financial Crime, 20(1), 5-20.
9. Gottschalk, P. (2013). Cybercrime and cyber warfare. CRC Press.
10. Herberger, J. (2020). Cybersecurity Ventures' 2019 cybercrime report
11. ISO. (2013). Information technology -- Security techniques -- Information security management systems -- Requirements. ISO/IEC 27001:2013.
12. Kendall-Taylor, A., & Nathanson, R. (2018). National cybersecurity frameworks: Setting the foundation for increasing cybersecurity capacity globally. Global Cybersecurity Capacity Centre.
13. Kizza, J. M. (2014). Ethical and social issues in the information age (6th ed.). Springer.
14. NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.
15. Regulation (EU) 2016/679. (2018). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj
16. Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Social Psychology Quarterly, 56(4), 329-339.
17. Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & Management, 46(5), 267-270.