cisdi Journal

Computing, Information Systems & Development Informatics Journal
Vol. 13 No. 4, December, 2022 - www.isteams.net/cisdijournal

Implementation of Cybersecurity Risk Theory and Model in Healthcare

[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

This review paper examines the implementation of cybersecurity risk theory and models in Healthcare, including their benefits and challenges. The paper begins with an overview of cybersecurity risk theory and models, including the STAMP theory and various types of models. It then compares different cybersecurity risk models and discusses their strengths and weaknesses. The paper also explores case studies of the successful implementation of cybersecurity risk models in Healthcare and the challenges these organizations face. The importance of risk assessment and management in healthcare cybersecurity and strategies for mitigating cybersecurity risks are highlighted. The paper concludes with future research and practice recommendations, including the need for more sophisticated risk models, addressing the cybersecurity workforce shortage, understanding the impact of emerging technologies, increasing collaboration between healthcare organizations, and conducting more empirical studies.

Keywords: Cybersecurity, Risk assessment, Risk management, Healthcare, Implementation, Risk models

CISDI Journal Reference Format
Folorunsho, O.S., Ayinde, A.Q., Olagoke, M.A. & Fatoye, O.E. (2022): Implementation of Cybersecurity Risk Theory and Model in Healthcare. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 13 No 4, Pp 65-72
Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V13N4P4

1. INTRODUCTION

Cybersecurity is becoming increasingly important in healthcare as medical organizations transition to digital platforms and incorporate electronic health records (EHRs) into their operations. Because of this information's sensitive and private nature, healthcare data is an essential target for cybercriminals. For both patients and healthcare organizations, a cybersecurity breach could result in the theft of patient data, misuse of medical identities, or financial loss. In 2020, 599 data breaches were reported in the healthcare sector, accounting for 29.7% of all data breaches reported in all sectors of industry, according to a report by the Identity Theft Resource Center, ITRC, 2021 It underlines the vulnerability of healthcare organizations to cyber threats, as well as the need for effective security measures. Effective cybersecurity measures can protect against data breaches and ensure the continuity of healthcare services. A cybersecurity event could cause a system failure, making it impossible for healthcare professionals to access patient data and provide care.

In emergencies, timely access to patient information may be vital for life and death. In addition, the growing threat landscape of cyber criminals is making it more and more critical for robust cybersecurity measures given the increasing prevalence of Internet of Things devices in healthcare sectors, such as smartwatches and telehealth tools.

1.1 Overview of Cybersecurity Risk Theories and Models

Cybersecurity risk theories and models are essential for assessing and managing cybersecurity risks in different sectors. These models can help organizations find potential security risks, assess the likelihood and impact of such threats, and layout strategies for mitigating them. The FAIR Factor Analysis of the Information Risk model is among the most prevalent cybersecurity risk models. The FAIR model, by considering factors like the potential for a threat to happen, its impact on current security controls and their effectiveness in place, provides a robust approach to cybersecurity risk assessments (The Open Group, 2019). The NIST National Institute of Standards and Technology Cybersecurity Framework is another frequently used model. This model provides a framework for organizations to identify, protect, detect, respond to, and recover from cybersecurity incidents (NIST, 2018).

STAMP (Systems-Theoretic Accident Model and Processes) theory has also been applied to cybersecurity to identify and prevent cybersecurity incidents. This theory provides an analytical framework, which is very important in cybersecurity when attacks can come from various sources and target individual systems components for analyzing complicated interactions among system components and their environment. In cyber security, STAMP theory has been used in several studies. An example would be researched by Teixeira et al. (2016), which uses STAMP to analyze the cybersecurity risks associated with the Internet of Things IoT and identifies possible mitigation strategies. Another study was conducted in 2018 by Shi et al., using STAMP as a methodology to analyze cybersecurity risks linked to cloud computing and design an assessment of the effectiveness of various cybersecurity controls.

1.2 Purpose of Review

This review paper will examine implementing cyber risk theory and models in health care. The report will present an overview of different cybersecurity risk theories and models, including their strengths and weaknesses, and examine how they are being applied within the healthcare sector. A review of relevant literature from academic sources, books, and reports, as well as industry standards and guidelines related to cybersecurity in Healthcare, will be part of the scope of this paper. Furthermore, current cybersecurity issues in the healthcare sector as well as potential advantages of implementing cyber security risk theory and models, will be discussed in this paper. Overall, the paper aims to contribute to the understanding of cyber security risk theory and models to improve cybersecurity in Healthcare and explore possibilities for future research on this subject.

2. CYBERSECURITY RISK THEORY AND MODELS

Cybersecurity risk refers to the potential for harm or loss due to cybersecurity incidents or cyber-attacks on an organization's electronic assets, such as information systems, networks, and data. Such risk can result in a wide range of adverse effects, such as loss of income, reputational damage, intellectual property losses, and disruption of essential services (Cherdantseva et al., 2018). Cybersecurity risks have become increasingly prevalent and complex due to the expanding attack surface resulting from the widespread use of digital technologies and interconnected systems. Organizations of all sectors are highly vulnerable to cybercriminals, state-supported actors, and others who seek to harm them. The identification and assessment of the cyber risks, as well as the implementation of relevant security controls in order to minimize or manage those risks, will be essential for efficient cybersecurity risk management.

This requires a thorough understanding of an organization's resources, i.e., physical equipment, software, data, and human beings, as well as possible threats to this asset which it faces (NIST, 2018).

3. BENEFITS AND CHALLENGES OF IMPLEMENTING CYBERSECURITY RISK MODELS IN HEALTHCARE

Implementing cybersecurity risk models in healthcare can offer numerous benefits but poses some challenges. This section discusses both the benefits and the challenges. Firstly, implementing a cybersecurity risk model can help healthcare organizations identify potential risks and develop strategies to mitigate them to improve their security posture (Ahmed et al., 2021). Secondly, many healthcare organizations must implement security measures to protect patient data through HIPAA regulations. In order to help organizations, comply with these rules and avoid the possibility of sanctions, a cybersecurity risk model may be useful (Madden & Sisti, 2017).

Thirdly, the cybersecurity risk model can help healthcare organizations prioritize their security investments by considering the likelihood and impact of possible risks, allowing for more effective use of resources and cost efficiency (Kulshrestha & Sharma, 2020). Lastly, demonstrating that they take a firm stance on protecting essential information for patients can help healthcare providers gain trust with their customers through efficient cybersecurity measures (Madden & Sisti, 2017). On the other hand, implementing a cybersecurity risk model may pose some challenges. Firstly, cybersecurity risk models may be complex and require considerable technical expertise for their development and implementation, which is a challenge for health organizations with limited resources (Kulshrestha & Sharma, 2020). Secondly, changes in current procedures and practices might be needed to implement a cybersecurity risk model that could run into resistance from stakeholders used to the way things are done (Ahmed et al., 2021).

Thirdly, cyber security risk models depend on accurate and reliable data to assess the risks accurately. However, healthcare organizations can be challenged with data quality issues such as incomplete or inaccurate data (Kulshrestha & Sharma, 2020). Lastly, a lack of standardization in the cybersecurity risk models makes it challenging for healthcare organizations to compare and choose between different models (Ahmed et al., 2021). Implementing cybersecurity risk models in healthcare can give many benefits, such as improved security posture, compliance with rules, cost reduction, and increased patient trust. However, it also involves challenges, including complexity, change resistance, data quality problems, and lack of standardization. Healthcare organizations should carefully consider these factors when deciding whether to implement a cybersecurity risk model and choose the model that best meets their needs.

3.1 Case study

Hospital ABC is one of the largest hospitals in the United States of America. They have several departments with over two hundred locations across the Midwest. The leadership is concerned about delivering top-notch care services to their patient per the industry standard. Hospital ABC processes thousands of patient data across their locations daily. With the evolution of digital technology that supports telemedicine, employee collaborations using a centralized platform and populating the organization databases from Medical-Internet-of-Things. Over the years, the healthcare industry has been the target of threat actors, and CHN has lost millions of dollars in revenue due to data breaches. The cyber attackers exploit the vulnerable configuration of some technologies, lack policies and standards that can safely guide the CHN cybersecurity operations, installing and deploy legacy cybersecurity solutions that cannot be integrated into the security operation center. In the quest to provide seamless healthcare services to patients powered by numerous applications and solutions, these technologies have exposed the Hospital ABC infrastructure to numerous risks and made the infrastructure to be vulnerable.

In this paper, the security team will select a suitable cybersecurity risk theory to protect and prevent the Hospital ABC infrastructure using an approved cybersecurity model that supports the organization's cybersecurity policy, risk, governance, and compliance.

3.1.1 Cybersecurity Risk Theory and Model

Due to technological advancement and the adoption of Bring-Your-Own-Device at Hospital ABC, the security, and Information Technology teams must create a standard to monitor the organization's cybersecurity posture. Though numerous artificial intelligence models have been developed using machine learning algorithms to monitor the internal and external activities on the network to ensure that threats are detected in real-time, it was ineffective. To ensure that the cybersecurity risks of the hospital are dynamic and complex cyberspace are monitored, the security team at CHN adopts the System Theoretic Accident Model and Processes (STAMP). This theory will track the cyber-attacks from the system and accidents perspective. This model will apply cyber safety to view CHN cybersecurity by correlating the relationships between the applications, systems, and databases on the CHN network.

In the STAMP framework, the security team will define the cybersecurity scope of the organization and determine the factors that led to previous attacks. The security team will define and implement controls that will serve as the foundation of the STAMP model. The STAMP theory captures the organization's cybersecurity process, safety constraints, and hierarchical safety control structures. The critical part of the STAMP model is the safety constraint which focuses on enforcing relevant constraints to prevent Hospital ABC business processes from being exposed to risks. Hierarchical safety control focus on the organization's goals, policies, and constraints control commands (Savaş & Karataş, 2022).

The security team will evaluate and ensure that every communication channel within the hospital network, risk value, and likelihood of exposure is determined by the feedback from the measuring and reference channels. The measurement is conducted at the defined level of communication within the CHN network infrastructure. This model will be used to evaluate the conditions that can cause a process required for the effective and efficient functioning of CHN network assets to fail. The STAMP model will be used to conduct casual analysis based on the STAMP methodology to ensure that the security team can analyze the cybersecurity failure of network assets beyond a single point of failure should an attack occurs (Hamid & Stuart, 2016).

There is a need for the cyber risk model to be adopted by CHN to ensure that complex cyber risks are mitigated and controlled to prevent the business operation from shutting down, which might lead to a loss of revenue. The security must deploy and implement robust enterprise-based risk management solutions to analyze, identify, mitigate, and eliminate cyber risk within their tenant (Dreyling et al., 2021)

Adopting the Factor Analysis of Information Risk (FAIR) framework will allow the organization to optimize and implement cybersecurity controls to manage risk efficiently and effectively. The security team will collaborate with the Information Technology team to determine the cybersecurity risk within the hospital tenant and establish the reasons for the attack. The leadership will commit to appropriate investment to boost the organization's cybersecurity, which will identify the organization's cybersecurity gaps and ensure appropriate improvements (Wang et al., 2020). The security team adopted the FAIR-based cyber risk model mainly because the framework can be used to implement cyber resilience and conduct risk analyses within the defined cybersecurity framework. The FAIR model has been used to implement robust cybersecurity risk management to strengthen the organization's security using industry-approved standards.

The FAIR model will enable the leadership to analyze high-risk assets within the hospital network infrastructure. The risk within the organization will be correlated with the financial estimates for the risk identified by the security team (Bakare, 2020). The FAIR model will effectively compare the variance between the degree of risk tolerance to ensure appropriate risk management strategies are implemented. The FAIR risk models cannot be subjected to scoring or ranking of risk (high, medium, or low) but can be used to measure the financial investment on risk over time. Also, the model can be used to create a holistic organization cybersecurity risk profile for the organization.

3.1.2 CHN Cybersecurity Controls

The security team will implement cybersecurity controls to prevent the threat actors from stealing sensitive data from the hospital network infrastructure. This control mechanism will capture the physical and technical security of the hospital network. The security team will create policies and procedures to provide structure as a guide to stakeholders. The policies and procedures will ensure that the likelihood of an insider causing a data breach is prevented. This type of control is enforced at the administrative level.

The physical control will prevent unauthorized users from accessing hospital network infrastructure (data center, workstation areas, and physical biometric solution). The physical controls can be informed of a fence, fire sprinklers, and Closed-Circuit Camera Television. The security team will spend reasonable hours to ensure that appropriate technical and logical control is in place to limit the access of unauthorized users. This will determine what an employee can access at a point in time using role-level permission from the security team. To access the hospital tenant, the security team will enable multi-factor authentication for all BYOD and other Internet-of-Things that join the networks. The operational control will prevent a non-operational member of the hospital team from accessing business data meant for the leadership. Generally, these controls are implemented to prevent threat actors from accessing unauthorized resources within the hospital network. The Controls will be used to detect threats, prevent unauthorized access, delay any process that will make the hospital infrastructure vulnerable, correct risk situations with an adequate incidence response plan, and recover the compromised network assets by restoring backup whenever the network has been compromised.

3.1.3 Importance of Risk Assessment and Management in Healthcare Cybersecurity

Risk assessment and management are critical components of a comprehensive cybersecurity strategy in healthcare.

The importance of these practices can be seen in the following ways:

1. Identifying vulnerabilities: Risk assessment helps identify areas of weakness in a healthcare organization's IT infrastructure and processes. By identifying vulnerabilities, organizations can mitigate risks and reduce the likelihood of a cybersecurity incident (AbuKhousa et al., 2020).
2. Prioritizing resources: Risk management allows organizations to prioritize resources and investments based on the level of risk associated with each area of the organization. This ensures that resources are allocated where needed to prevent and respond to cybersecurity incidents (Marfori & Luy, 2019).
3. Meeting compliance requirements: Regulatory bodies often require risk assessment and management, such as HIPAA and HITECH. By meeting these requirements, healthcare organizations can avoid penalties and reputational damage associated with non-compliance (Chen et al., 2020).
4. Protecting patient data: Risk assessment and management help protect patient data from theft, loss, or unauthorized access. By proactively managing cybersecurity risks, healthcare organizations can better safeguard sensitive patient information (Jawadi & Sadoun, 2020).

5. In summary, risk assessment and management are critical components of an effective cybersecurity strategy in healthcare. Healthcare organizations can better manage cybersecurity risks and safeguard patient information by identifying vulnerabilities, prioritizing resources, meeting compliance requirements, and protecting patient data.

3.1.4 Strategies for Mitigating Cybersecurity Risks in Healthcare

Healthcare organizations are at risk of cybersecurity attacks that can compromise sensitive patient information, disrupt operations, and damage their reputation. For this reason, establishing effective cyber risk mitigation strategies by these organizations is essential. Here are some strategies that are effective:

1. Conduct regular risk assessments: Regular risk assessments can help identify vulnerabilities in an organization's systems and processes. By understanding the risks, healthcare organizations can develop and implement adequate security measures (Chen et al., 2020).
2. Develop and enforce policies and procedures: Clear policies and procedures are essential for managing cybersecurity risks. Healthcare organizations should have policies for password management, access controls, data encryption, and incident response (Jawadi & Sadoun, 2020).
3. Educate employees: Employees are often the weakest link in an organization's cybersecurity defenses. Therefore, it is essential to provide regular cybersecurity training to all employees to help them understand the risks and how to protect against them (Marfori & Luy, 2019).
4. Use encryption and other security technologies: Healthcare organizations should use encryption to protect sensitive data. They should also use other security technologies, such as firewalls, intrusion detection systems, and anti-malware software, to protect against cyber-attacks (AbuKhousa et al., 2020).
5. Conduct regular security audits: Regular security audits can help healthcare organizations identify weaknesses in their security defenses and take corrective action. Audits should be conducted by an independent third-party auditor (Chen et al., 2020).
6. In conclusion, healthcare organizations must take proactive steps to mitigate cybersecurity risks. Healthcare organizations can better protect patient information and prevent cyber-attacks by conducting regular risk assessments, developing and enforcing policies and procedures, educating employees, using encryption and other security technologies, and conducting regular security audits.

4. CONCLUSION

As health organizations increasingly rely upon digital technologies for storing and safeguarding sensitive patient data, cyber security risks are a critical concern. The potential for loss or damage caused by a cyber-attack on a healthcare organization is referred to as cybersecurity risk. Cyber-attacks may lead to significant consequences, such as the loss or theft of patients' data, damage to an organization's reputation, and even criminal sanctions. Healthcare organizations can use cybersecurity risk models to assess and manage cybersecurity risks. Some commonly used models include the NIST Cybersecurity Framework, Factor Analysis of Information Risk (FAIR), and Systems-Theoretic Accident Model and Processes (STAMP). These models can help healthcare organizations identify potential risks, assess the likelihood and impact of those risks, and develop strategies to mitigate them. There are many benefits to healthcare organizations using cybersecurity risk models. Improved data security, regulatory compliance, and customer confidence are also a result of these benefits. However, it is difficult to implement these models, given that healthcare institutions may not have the capacity or expertise to carry them out effectively.

However, healthcare organizations also face challenges in implementing cybersecurity risk models. Lack of resources, cultural resistance, and the changing threat landscape can also contribute to these challenges. Organizations must prioritize risk assessments and management to manage cybersecurity risks in healthcare effectively. This will include identifying weaknesses, assessing potential threats' likelihood and possible impact, and developing risk mitigation strategies.

4.1 Recommendation for Future Research and Practice

Future research and practice in cybersecurity in healthcare are crucial in ensuring that patient data remains secure and protected. One area of future research could be developing more sophisticated cybersecurity risk models. As the threat landscape evolves, healthcare organizations must continually update and improve their risk management strategies. This can be achieved by developing more sophisticated risk models to better account for new and emerging threats. Another area of focus for future research could be addressing the cybersecurity workforce shortage. Healthcare organizations need more cybersecurity professionals, making implementing effective cybersecurity risk management practices challenging. Future research could explore ways to address this shortage, such as developing training programs or leveraging technology to automate specific security tasks.

Understanding the impact of emerging technologies is also critical for future research in healthcare cybersecurity. As Healthcare evolves, new technologies such as telemedicine and the Internet of Things (IoT) are becoming increasingly important. Future research could explore the cybersecurity risks associated with these technologies and develop strategies to manage them. Increasing collaboration between healthcare organizations is another important area for future research. Cybersecurity threats are not limited to individual healthcare organizations; they can also impact entire healthcare systems. Future research could explore ways to increase collaboration between healthcare organizations to share threat intelligence better and develop more effective risk management strategies. Finally, conducting more empirical studies could also be a valuable focus for future research. While case studies can help illustrate the benefits and challenges of cybersecurity risk management in healthcare, more empirical studies are needed to better understand the efficacy of different risk management strategies. Future research could focus on conducting rigorous empirical studies to evaluate the effectiveness of different risk management strategies and identify best practices.

REFERENCES

1. AbuKhousa, E., Sherkat, N., & Saba, T. (2020). Risk assessment of healthcare information systems: A systematic review. Journal of Medical Systems, 44(7), 136.
2. Ahmed, M., Elkhodr, M., & Shahrestani, M. (2021). Cybersecurity in healthcare: A review of current trends, challenges, and solutions. Journal of Medical Systems, 45(4), 1-12.
3. A narrative review. Journal of Medical Internet Research, 19(9), e305.
4. Bakare, A. A. (2020). A Methodology for Cyberthreat ranking: Incorporating the NIST Cybersecurity Framework into FAIR Model (Doctoral dissertation, University of Cincinnati).
5. Carnegie Mellon University. (n.d.). OCTAVE. https://www.cert.org/octave/
6. FAIR Institute. (n.d.). Factor Analysis of Information Risk (FAIR). https://www.fairinstitute.org/
7. Cherdantseva, Y., Hilton, J., & Burnap, P. (2018). From cybersecurity to cybercrime: A review of the risk factors. International Journal of Cyber-Security and Digital Forensics, 7(2), 45-58.
8. Chen, X., Liu, Y., & Zhao, H. (2020). Review of healthcare information security risk management. Journal of Healthcare Engineering, 2020.

9. Dreyling, R., Jackson, E., & Pappel, I. (2021). Cyber security risk analysis for a virtual assistant G2C digital service using FAIR model. In 2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 33-40). IEEE.
10. Hamid, S. & Stuart, M. (2016). Cyber Safety: A System Theory Approach to Managing Cyber Security Risks - Applied to TJX Cyber Attack. http://web.mit.edu/smadnick/www/wp/2016-09.pdf
11. Identity Theft Resource Center. (2021). 2020 End-of-Year Data Breach Report. Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2021/01/2020-End-of-Year-Data-Breach-Report.pdf.
12. ISO/IEC. (2020). ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements. https://www.iso.org/standard/54534.html
13. Jawadi, W. M., & Sadoun, B. A. (2020). Healthcare information security and risk management. Journal of Medical Systems, 44(6), 105.
14. KPMG. (2019). Healthcare Cybersecurity: Protecting Patient Data. Retrieved from https://home.kpmg/us/en/home/insights/2019/03/healthcare-cybersecurity.html.
15. Kulshrestha, P., & Sharma, M. (2020). Cybersecurity risk assessment and management in healthcare organizations: A systematic review. Journal of Medical Systems, 44(6), 1-15.
16. Madden, M., & Sisti, D. A. (2017). Ethical and legal implications of the risks of cybersecurity in healthcare:
17. Marfori, M. L., & Luy, M. J. (2019). Hospital information security risk assessment: A case study. Journal of Cases on Information Technology, 21(3), 17-32.
18. Microsoft. (n.d.). Threat Modeling. https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling
19. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov/cyberframework.
20. The Open Group. (2019). FAIR™ (Factor Analysis of Information Risk) Cyber Risk Framework. Retrieved from https://www.opengroup.org/fair.
21. Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. International Cybersecurity Law Review, 3(1), 7-34.
22. Shi, W., Yang, L., Xu, J., & Yin, J. (2018). An STPA-based security risk assessment method for cloud computing. Future Generation Computer Systems, 82, 374-386. https://doi.org/10.1016/j.future.2017.12.008
23. Teixeira, T., Silva, J. P., & Mahler, C. F. (2016). STAMP-based security analysis of the Internet of Things. International Journal of Critical Infrastructure Protection, 14, 21-34. https://doi.org/10.1016/j.ijcip.2016.03.002
24. Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security, 89, 101659.