Cybersecurity and Innovative Technology Journal, Vol.2, No.1, 2024, pp. 15-25
e-ISSN 3025-6682. DOI. 10.52889/citj.v2i1.333

Cybersecurity Vulnerabilities in Healthcare: A Threat to Patient Security

Submitted 11 November 2023, Revised 18 February 2024, Accepted 18 February 2024

William J. Triplett[1,2]*

[1]Department of Information Systems, Health Information Technology,
University of Maryland, Baltimore County, Baltimore, United States

[2]Department of Healthcare Technology, Cybersecurity Leadership,
Capitol Technology University, Laurel, United States

Corresponding Email: *wtriple1@umbc.edu

Abstract

Healthcare information systems hold significant importance; hence, their cybersecurity is crucial. Exposed networks make it easy for cybercriminals to launch cyberattacks and access healthcare data. Thus, concerns regarding cybersecurity and its link to healthcare privacy, confidential data, and medical devices are growing. Therefore, cybersecurity vulnerabilities in healthcare and patient security are significant issues. Healthcare information systems comprise correlated networks and play a vital role in treating and saving patients. However, advanced circulated ransomware attacks on hospitals prevent access to electronic health records for providing appropriate patient care, thus forcing doctors to turn to other facilities. These cyberattacks can leak patient data, and regaining control of information systems and patient data is highly expensive, thus resulting in extensive monetary losses. Cyberattacks aimed toward electronic medical records, information technology systems, and medical devices have corrupted the best systems across clinics and small offices with physicians, as well as merged health systems. There is an urgency to address cybersecurity vulnerabilities in healthcare; however, opinions differ regarding suitable measures for safeguarding patient data and ensuring infrastructural security. We aimed to reconcile these diverging hypotheses and provide an understanding of the current landscape and directions for further improvements by reviewing several studies on healthcare cybersecurity. We also interviewed healthcare professionals, cybersecurity experts, and administrators and distributed a survey questionnaire to healthcare organizations to gather quantitative data on existing cybersecurity measures and vulnerabilities. Our analyses show that healthcare organizations are vulnerable to a variety of threats, cyberattacks disrupt the health sector, cybersecurity vulnerabilities impact patient security, and implementations of cybersecurity measures are inconsistent across organizations. Owing to the sophisticated nature of cyberattacks, the healthcare industry must prioritize cybersecurity and provide the funding required to develop critical systems for safeguarding patients and their data. The study's findings underscore the need for standardized cybersecurity practices in healthcare to address inconsistencies in measures across organizations. Adequate and ongoing investment in cybersecurity infrastructure is imperative to counter increasingly sophisticated cyberattacks. Additionally, protecting patient data and maintaining trust within the healthcare sector are ethical imperatives that should guide industry actions. By embracing these implications, the healthcare industry can enhance patient security, financial stability, and ethical integrity.

Keywords: Cybersecurity, Confidential Data, Cyberattacks, Healthcare, Ransomware

INTRODUCTION

The healthcare sector is constantly challenged by malicious actors, resulting in novel vulnerabilities and increased significance of existing cybersecurity weaknesses (Javaid, Haleem, Singh, & Suman, 2023). We aimed to examine the cybersecurity vulnerabilities in the healthcare sector comprehensively, highlight the potential risks to patient security, and emphasize the need for robust measures to mitigate these vulnerabilities. Triplett (2022a) has stated that “healthcare organizations remain among the primary targets of these attacks.” According to Javaid et al. (2023), this situation has been exacerbated by the increasing dependence of healthcare providers on digital technology. Therefore, we aimed to elucidate the

nature of cybersecurity threats in the healthcare sector, particularly the risks they pose to healthcare providers. We comprehensively explored the most critical risks, examined their potential impacts, and determined the priorities for healthcare organizations to mitigate them. The healthcare sector faces numerous cybersecurity threats owing to the increasing digitization of healthcare systems and considerable value of electronic health records. Although enhanced patient care offers considerable advantages, some serious vulnerabilities remain, such as unauthorized access to sensitive patient data, data breaches, ransomware attacks, and other network vulnerabilities, which must be addressed.

Compared with detecting and deleting viruses, cybersecurity involves deploying and synchronizing resources across hospitals, information technology (IT) suppliers, medical devices, and industries to alleviate the dangers of cyberattacks. Therefore, cybersecurity requires collective commission and a collaborative effort from all stakeholders, as it is not exclusively an IT problem but an organizational issue that affects both enterprises and software. According to Triplett (2022b), “the increase of cybersecurity threats poses a significant risk to the healthcare industry, specifically, healthcare organizations, pharmaceutical companies, and clinics.” Such incidents can compromise patient privacy, cause financial losses, disrupt healthcare services, and, in worst-case scenarios, harm patients. The most significant cybersecurity risks to the healthcare sector include phishing attacks, malware infections, insider threats, and utilization of outdated software and hardware, which can result in data breaches, operational disruptions, and financial losses. The existing literature emphasizes the significance of comprehending these threats to develop effective cybersecurity strategies tailored to the healthcare sector. Coronado and Wong (2014) stated that “cybersecurity risk management is a huge responsibility, and everyone in the healthcare community should continue to keep this subject in mind as we collaborate on safeguarding our facilities to ensure optimal delivery of patient care.”

Generally, research has revolved around fundamental questions related to cybersecurity threats in the healthcare sector, including what are the most serious cybersecurity threats in this sector? How do these threats impact healthcare organizations? What measures have been implemented thus far and what are the pitfalls to be aware of?

Although healthcare systems worldwide have discovered the significant capabilities of digital technology for advancing clinical outcomes and changing care delivery, the healthcare sector faces greater cyber risks because of the fundamental weaknesses in its security posture (Martin, Martin, Hankin, Darzi, & Kinross, 2017). This is because most healthcare companies are unprepared to handle inevitable cyberattacks. This crisis can be devastating and has

prompted senior healthcare stakeholders to identify and adopt various strategies for combating the current limitations of existing systems. The healthcare sector is facing an increasing number of attacks, combined with the extremely restricted and significant nature of its data, which specifically influences the domain, thus making it susceptible and attractive to hackers. However, such attacks can have significant effects beyond monetary losses or operative interference as the quality of care can be affected, thus resulting in patient deaths (Abraham, Chatterjee, & Sims, 2019).

Thus, the healthcare sector faces numerous cybersecurity threats owing to the increasing digitization of healthcare systems and the considerable value of electronic health records. These threats include unauthorized access to sensitive patient data, data breaches, ransomware attacks, and network vulnerabilities. Lehto (2022) noted, "attackers can inflict damage or disrupt physical infrastructure by infiltrating the digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack." Additionally, the complexity of these threats continues to increase. Therefore, assessing and identifying the most critical cybersecurity risks is crucial for allowing healthcare organizations to allocate their resources effectively and prioritizing strategies for mitigating risks. Additionally, by prioritizing these risks based on their potential impact, organizations can allocate resources efficiently and address vulnerabilities through targeted measures (Smith, 2018). Numerous studies have contributed to the existing body of knowledge on cybersecurity risks in healthcare. For instance, researchers have explored the challenges and vulnerabilities encountered within healthcare systems and proposed strategies to safeguard them against cyber threats. Additionally, they have examined the effectiveness of existing cybersecurity approaches and identified their limitations. Lekshmi (2022) stated, "Even before the emergence of digital technology in the healthcare field, privacy breaches were a concern, but the increase in interconnectivity has opened multiple doorways for access."

We aimed to thoroughly review several noteworthy studies (Beavers & Pournouri, 2019; Hoffman, 2020; Thomas & Ngalamou, 2022) that have explored healthcare cybersecurity to provide a comprehensive understanding of the current landscape of healthcare cybersecurity and identify avenues for further exploration and improvements. Our review can enlighten the healthcare community and policymakers regarding cybersecurity threats and the necessity for implementing preventive measures. Amidst the vast field of cybersecurity, the healthcare industry constitutes distinctive security needs owing to the various regulatory requirements, the presence of sensitive patient data, and the use of life-sustaining medical devices, making it a prime target for cybercriminals. Hence, extensive research in this area is imperative. Although

there is a consensus regarding the urgency of addressing cybersecurity vulnerabilities in healthcare, the opinions regarding suitable measures for safeguarding patient data and ensuring infrastructural security differ. Therefore, we aimed to reconcile these diverging hypotheses and address the following research questions:

1. Why is healthcare susceptible? Private patient information, medical devices, and an access point are entries the attackers. Employees are not educated about online risks, and an excessively large number of devices are used for tracking or the diagnosis of patients.
2. Why is healthcare a major target? The substantial amounts of sensitive patient data possess a high monetary value. The targeted data include patients' protected health information, financial data, credit card data, banking data, personally identifying information, as well as medical research and innovation data involving patients.
3. What threats and costs are healthcare presently experiencing? Mobile data access, ransomware, lack of security education or procedures, poor software security measures, increasing costs of cyberattacks, and indirect costs of healthcare cybersecurity breaches are some examples.
4. What is the role of the healthcare sector involving cyberattacks? Protecting sensitive healthcare data and improving the security posture through awareness of cybersecurity risks.
5. How can the healthcare sector move forward? Limit staff access privileges, provide standard updates to systems, implement strong passwords and dual authentication procedures, and conduct employee training and education about common social engineering attacks.

METHOD

We comprehensively examined healthcare cyber risks through a mixed-method approach that combined qualitative and quantitative data. Generally, digital healthcare expertise is used transversely worldwide; however, healthcare data and equipment security are growing problem owing to the increased cybersecurity risks to medical devices because of their increasing dependence on digital systems (Camgöz Akdağ & Menekşe, 2023). Through in-depth interviews with healthcare professionals, cybersecurity experts, and administrators responsible for maintaining the security infrastructures of healthcare facilities, a qualitative component was employed. Additionally, a survey questionnaire was distributed to some healthcare organizations to gather quantitative data on existing cybersecurity measures and vulnerabilities. The in-depth interviews were semi-structured, allowing for flexibility in exploring specific areas of interest while ensuring consistency across interviews. By contrast, the survey was designed using validated scales and questions and focused on collecting quantitative data regarding cybersecurity practices, awareness, and vulnerabilities within healthcare

organizations.

The sample selection process employed stratified random sampling. Healthcare organizations were categorized based on their size, location, and type of care provided, such as hospitals, clinics, and long-term care facilities. A random sample of organizations within each category was then selected for inclusion in the study. This approach guaranteed a diverse representation of healthcare settings, facilitating a comprehensive understanding of cybersecurity vulnerabilities across the entire industry. However, as current cybersecurity frameworks offer a generic framework for all organizations, prioritizing the categories within the framework for individual healthcare organizations is critical for developing an effective security policy. The initial exploratory design involved using qualitative methods to identify the most critical risks and priorities for healthcare organizations. Subsequently, an explanatory design that leveraged the quantitative data was utilized to validate the qualitative findings and offered an in-depth analysis of the challenges. Additionally, a deductive approach was adopted to evaluate and enhance existing theoretical frameworks, fostering a robust understanding of healthcare cyber risks (Blanke & McGrady, 2016). The primary and secondary data collection methods allowed us to thoroughly examine the experiences, perceptions, and practices of healthcare professionals regarding cybersecurity. Preliminary data were collected through semi-structured interviews with cybersecurity experts in the healthcare sector and survey questionnaires administered to healthcare organizations. By contrast, secondary data were sourced from scholarly articles, government reports, and industry publications, which offered a broad perspective regarding the state of healthcare cybersecurity and the evolving threat landscape. Rigorous quality checks were performed to ensure data validity and reliability. Initial user acceptance testing of data and IT security controls was performed to ensure that the controls were operating well. Frequent offsite data backups were recommended, with strict controls for data encryption, access, and other best practices. Additionally, a hybrid data analysis approach was adopted, wherein qualitative data derived from the interviews were analyzed using thematic analysis, which facilitated the identification of recurring themes and patterns. In contrast, quantitative survey data were analyzed using descriptive and inferential statistics, which provided factual and comparative insights. Integrating these data analysis techniques helped facilitate a comprehensive understanding of healthcare cyber risks, thereby supporting the development of effective countermeasures against healthcare cyber risks. Currently, methodological cybersecurity countermeasures are employed to protect the privacy, integrity, and accessibility of data and information systems, particularly in the healthcare domain. Additionally, a multilayer attack model that provides a new viewpoint for attack and

threat identification and analysis has been proposed (Spanakis et al., 2020). Informed consent was diligently obtained from all participants to ensure voluntary involvement and confidentiality of their responses. Furthermore, the collected data are securely stored and accessible solely to the research team. Participants retain the right to withdraw from the study at any given time without any negative consequences. Additionally, this study conformed to the ethical guidelines set in the Declaration of Helsinki.

RESULTS AND DISCUSSION

The analysis of the collected data provided several significant insights into cybersecurity vulnerabilities in the healthcare sector. First, it revealed that healthcare organizations are vulnerable to a wide range of threats, both external, such as hacking and malware attacks, and internal, such as employee negligence. Cyberattacks have become increasingly disruptive to the health sector, particularly to hospitals, resulting in considerable damage by breaching patients' personal and professional information and significant revenue losses and fines (Bhosale, Nenova, & Iliev, 2021). Moreover, the analysis indicated that cybersecurity vulnerabilities substantially impact patient security, potentially resulting in compromised patient records, unauthorized access to medical devices, and disruption of healthcare services. Owing to perceptions of inadequate security, patients and practitioners may lose confidence in a healthcare provider’s ability to maintain patient privacy. Moreover, cyberattacks can result in operations systems being offline, leading to disruption of care because of software outages. In addition, the loss of access to health records may limit the provider’s ability to provide appropriate care, shelter, and medicine in times of need. Finally, damage to infrastructure, such as insurance and payment or utility systems, can also prevent people from accessing necessary medical care. The consequence of accessing patient records and medical devices, such as when a ransomware virus holds them hostage, deters the ability to care for patients effectively. Hackers’ access to private patient data not only opens the door for them to steal the information but also to either intentionally or unintentionally alter the data, which could lead to serious effects on patient health and outcomes.

Furthermore, the analysis revealed that there is a disparity in the implementation of cybersecurity measures among healthcare organizations, with certain organizations demonstrating higher levels of readiness.

The data analyses yielded significant findings regarding cybersecurity threats in the healthcare sector, including malware infections, phishing attacks, ransomware, and data breaches. The research questions were addressed, and the results offered valuable insights into the various types of vulnerabilities within the healthcare industry, along with the potential

threats they pose to patient security. Our study comprehensively examined past cyberattacks on healthcare organizations and analyzed current cybersecurity practices. The findings highlighted the critical gap between vulnerability awareness and the implementation of effective security measures, thereby emphasizing the need for a proactive and dynamic approach to healthcare cybersecurity that addresses both technological and human factors. To delve deeper into the research questions, we conducted statistical analysis to quantify the extent and severity of cybersecurity vulnerabilities in the healthcare sector. The results indicated that the prevalence of vulnerabilities was high as a considerable number of healthcare organizations lack sufficient safeguards to protect against cyber threats. This underscores the urgent need for enhanced cybersecurity measures and investments in robust defense systems.

Additionally, owing to the inherent weaknesses of the healthcare sector, it is susceptible to direct attacks and faces challenges in keeping patient information confidential, thus making it accessible to attackers (Alghamdi, 2022). Moreover, we highlighted the potential impacts of these threats on healthcare organizations, including financial losses, reputational damage, legal implications, and compromised patient safety. Furthermore, it was revealed that healthcare organizations face various challenges in effectively addressing cybersecurity threats. These challenges stem from limited resources, a lack of cybersecurity expertise, inadequate security controls, and the inherent complexity of healthcare systems. These findings emphasize the critical need for healthcare organizations to recognize and prioritize cybersecurity as a fundamental aspect of their operations. This indicates that, currently, only a few healthcare organizations can tackle these challenges owing to the scarcity of experts with critical cybersecurity skills. Furthermore, the demanding requirements to train new graduates with the credentials and abilities vital to healthcare cybersecurity were evaluated (Angafor, Yevseyeva, & He, 2020).

Additionally, the importance of sharing the cybersecurity responsibility among healthcare organizations, regulators, technology vendors, and all relevant stakeholders was elucidated. Such collaboration, information sharing, and partnerships with cybersecurity experts can enhance defense against cyber threats. Moreover, conducting training programs for healthcare personnel and regular security assessments can significantly bolster the resilience of healthcare systems. The cumulative merging of technology in the healthcare sector has improved diagnosis accuracy; however, cybersecurity improvements are still required (Argaw et al., 2020). Notably, a study (Smagulov & Smagulova, 2019) also identified the widespread vulnerabilities and associated risks within the healthcare industry. Our findings align with and expand on previous research in the field of healthcare cybersecurity, offer a comprehensive

understanding of the challenges faced by healthcare organizations in addressing cybersecurity threats, and substantiate the importance of addressing cybersecurity concerns in healthcare. Specifically, limited resources, lack of cybersecurity expertise, and inadequate security controls were identified as key challenges, thereby deepening the existing subject knowledge. Consequently, the pressing need to develop targeted interventions and policies that can effectively address these challenges and safeguard the data of healthcare organizations and patients was highlighted. Furthermore, examining cybersecurity is crucial and must be prioritized not just through preparedness but also through national security (Mishra, Alzoubi, Gill, & Anwar, 2022).

Moreover, our study builds upon the existing literature by delving into the specific challenges faced by healthcare organizations and the potential consequences of cyberattacks. The comparative analysis revealed common themes, such as the significance of employee training, encryption, and incident response plans for safeguarding patient information. However, this study further highlights the need for tailored cybersecurity measures that account for the unique characteristics and vulnerabilities of the healthcare industry. The implications of our study extend far beyond the scope of individual healthcare organizations, with the findings emphasizing the critical role of healthcare policymakers in developing comprehensive cybersecurity regulations and guidelines. By exploring the implications of inadequate cybersecurity measures, we aimed to raise awareness regarding their potential consequences and encourage policymakers to take proactive steps toward cybersecurity enhancement within the healthcare industry.

Although this study offered significant insights into the risks and priorities for healthcare cybersecurity, it has certain limitations. First, the findings were obtained through a comprehensive literature review, which inherently restricted the depth and scope of the analysis. Although we attempted to include a wide range of sources, some specific studies were excluded, which may have impacted the completeness and generalizability of the findings. Moreover, the absence of primary data collection limited the ability to offer firsthand insights into the specific challenges and experiences of healthcare organizations that have encountered cybersecurity threats. Additionally, it focused on a specific region and may not encompass the global landscape of cybersecurity vulnerabilities in healthcare. Furthermore, as with any self-reported data, there might be inherent biases or inaccuracies in the reported cybersecurity measures implemented by the surveyed healthcare organizations.

To overcome these limitations, future research should aim to conduct cross-regional and longitudinal studies that incorporate both quantitative and qualitative data. Longitudinal studies

would allow exploring the evolution of cybersecurity threats and the effectiveness of new countermeasures for mitigating them. Additionally, based on our findings, we recommend several avenues for future research. First, further investigations into the effectiveness of cybersecurity training programs for healthcare professionals could provide insights into the impact of education on enhancing cybersecurity practices within organizations and second, exploring the feasibility of adopting emerging technologies, such as blockchain, to improve the integrity and security of healthcare data warrants further attention. Blockchain technology can potentially enhance the trustworthiness and immutability of medical records, thereby reducing their vulnerability to cyberattacks. Finally, longitudinal studies can provide valuable insights into the long-term consequences of cyberattacks on healthcare organizations and the effectiveness of recovery strategies. There exist serious vulnerabilities in hospitals' technologies that are currently not addressed (Wasserman & Wasserman, 2022). To account for the evolving nature of cyber threats and adapt to emerging trends, future research must focus on developing comprehensive and resilient cybersecurity frameworks for the healthcare industry. Additionally, a mixed methods approach that combines a literature review with primary data collection through interviews, surveys, or case studies can be adopted, which can offer a more comprehensive understanding of the experiences and perceptions of healthcare organizations toward cybersecurity risks. Moreover, a broader sample size and inclusion of various types of healthcare organizations, such as hospitals, clinics, and private practices, can provide a more representative picture of cybersecurity in the healthcare sector.

CONCLUSION

This study extensively examined cybersecurity threats in healthcare, focusing on vulnerabilities and their impact on patient data and care continuity. Critical cyber risks were identified, offering a strategy for addressing them effectively. Triplett (2022) highlighted the significant risk posed by cybersecurity threats in the healthcare sector, emphasizing the need for organizations to identify weaknesses and develop comprehensive strategies, including risk assessment, personnel training, and contingency planning. Proactive measures to adapt to evolving cyber threats are essential. Although this study provides valuable insights, further research is needed to evaluate cybersecurity tools and practices, bridge the policy-implementation gap, and understand the psychological, financial, and operational effects of cyberattacks on patients and healthcare providers in the healthcare sector.

REFERENCES

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. doi:10.1016/j.bushor.2019.03.010.

Alghamdi, A. (2022). Cybersecurity threats to healthcare sectors during COVID-19 2nd International Conference on Computing and Information Technology (ICCIT) (pp. 87–92). IEEE Publications. doi:10.1109/ICCIT52419.2022.9711659.

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Bridging the cyber security skills gap: Using tabletop exercises to solve the CSSG crisis. In M. Ma, B. Fletcher & S. Göbel (Eds.), *Serious games* (pp. 117–131). Springer International Publishing. doi:10.1007/978-3-030-61814-8_10.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., . . . Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1), 146. doi:10.1186/s12911-020-01161-7.

Beavers, J., & Pournouri, S. (2019). Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions. In H. Jahankhani, S. Kendzierskyj & A. Jamal (Eds.), *Blockchain and clinical trial: Securing patient data* (pp. 249–267). Springer International Publishing. doi:10.1007/978-3-030-11289-9_11.

Bhosale, K. S., Nenova, M., & Iliev, G. (2021) *Sixth Junior Conference on Lighting (Lighting)*. A study of cyber attacks. In the healthcare sector, *2021*, 1–6.

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management*, *36*(1), 14–24. doi:10.1002/jhrm.21230.

Camgöz Akdağ, H., & Menekşe, A. (2023). Cybersecurity Framework prioritization for healthcare organizations using a novel interval-valued Pythagorean fuzzy CRITIC. In C. Kahraman & E. Haktanır (Eds.), *Intelligent systems in digital transformation: Theory and applications* (pp. 241–266). Springer International Publishing. doi:10.1007/978-3-031-16598-6_11.

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation and Technology*, Suppl, 26–30. doi:10.2345/0899-8205-48.s1.26.

Hoffman, S. A. E. (2020). Cybersecurity threats in healthcare organizations: Exposing vulnerabilities in the healthcare information infrastructure. *World Libraries*, *24*.

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. doi:10.1016/j.csa.2023.100016.

Lehto, M. (2022). Cyber-attacks against critical infrastructure. In M. Lehto & P. Neittaanmäki (Eds.), *Cyber security: Critical infrastructure protection* (pp. 3–42). Springer International Publishing. doi:10.1007/978-3-030-91293-2_1.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ*, *358*, j3179. doi:10.1136/bmj.j3179.

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*, *22*(2), 538. doi:10.3390/s22020538.

Smagulov, S., & Smagulova, V. (2019). Challenges of digital transformation in healthcare. *Intellect arch*, *8*, 12–32.

Smith, C. (2018). Cybersecurity implications in an interconnected healthcare system. *Frontiers of Health Services Management*, *35*(1), 37–40. doi:10.1097/HAP.0000000000000039.

Spanakis, E. G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., . . . Magalini, S. (2020). Cyber-attacks and threats for healthcare–a multi-layer thread analysis. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE Engineering in Medicine and Biology Society. Annual International Conference*. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society. Annual International Conference* 42nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). IEEE Publications, *2020*, 5705–5708. doi:10.1109/EMBC44109.2020.9176698.

Sunil Lekshmi, A. (2022), *Growing concern on healthcare cyberattacks and need for cybersecurity*.

Thomas, S., & Ngalamou, L. (2022). The impact of cybersecurity on healthcare. In K. Arai (Ed.), *Proceedings of the future technologies conference* (pp. 680–689). Springer International Publishing. doi:10.1007/978-3-030-89880-9_50.

Triplett, W. (2022b). Ransomware attacks on the healthcare industry. *Journal of Business, Technology and Leadership*, *4*(1), 1–13. doi:10.54845/btljournal.v4i1.31.

Triplett, W. J. Addressing cybersecurity leadership challenges in organizations. *Capitol technology university ProQuest dissertations publishing*. (2022a):30522018.

Triplett, W. J. (2022c). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586. doi:10.3390/jcp2030029.

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*, 862221. doi:10.3389/fdgth.2022.862221.