Cybersecurity and Innovatove Technology Journal, Vol.3, No.2, 2025, pp. 58-67
e-ISSN 3025-6682. DOI: 10.53889/citj.v3i2.837

The Connection Between Hackers and Their Affinity Towards Healthcare

Submitted 27 June 2024, Revised 5 November 2024, Accepted 31 December 2025

Maurice L. McBride[1,2]*

[1]Department of Healthcare Technology, Healthcare Cybersecurity,
Capitol Technology University, Washington D.C., United States

[2]McBride Healthcare, Columbia, United States
Corresponding Email: *mmcbride@captechu.edu

Abstract

Cybercriminals target the healthcare sector because patient data can be traded illegally. These include ransomware attacks and medical record theft. This article analyzes the internal factors that make healthcare firms vulnerable to cybercrime. It also examines their complicated tactics for entering and profiting from these sectors. This paper examines healthcare cybersecurity case studies and current research. The goal is to help readers understand the main challenges of fighting different cyberattacks. The methodology part includes a thorough literature review and rigorous analysis of data from academic sources, industry publications, and cyber security incident databases. The numbers show the diverse threat actors targeting the healthcare business, their techniques, and the vulnerabilities of healthcare institutions to cyber attacks. The report concludes that healthcare cybersecurity is crucial. The guidelines presented are essential for healthcare cybersecurity.

Keywords: Healthcare Cyberthreats, Hackers, Access Controls, Identity Management, Patch Management

INTRODUCTION

In the overall digital world, the broadly applicable healthcare sector is a prime attractor of cyber criminals looking for flaws to exploit, even for making money or carrying out malicious acts (Keshta & Odeh, 2021). Medical records, insurance information, and PII all pose an incredible challenge to healthcare companies as there is a high risk of a data breach in these targeted areas, and ransomware attacks are also common (Rachit et al., 2021). Likewise, the fundamental importance of the healthcare industry and the capacity for such disruptions to have adverse effects on patient treatment and safety, cybercriminals add to their weight by laundering their activities (Thomasian & Adashi, 2021). The motivation of these hackers to break into healthcare is facilitated by various reasons that stem from the magnitude of medical data exchange on dark forums (Wenhua et al., 2023). These ransomware attacks can paralyze operations and clinical setups with payment extortion and the high level of IT vulnerabilities hence the in-built weaknesses existing in the complex healthcare system as well as medical devices which can be leveraged by hackers (van Boven et al., 2024). With the advent of the digital space over and the advancing medical sector adopting advanced technologies, the combat zone for hackers goes uphill and leads to another level of attack reaching out for abuse (Adil et al., 2024).

This detailed report will focus on the complicated psyche of cybercriminals attacking healthcare facilities, their various types and distributions of malware, and the hazardous repercussions of successful cyber-attacks. Figure 1 describes the various types of malware

capable of crippling the healthcare industry. By conducting a comprehensive analysis of actual cybersecurity incidents and the newest cybersecurity research, the paper in this document is worth reading for you because it is crafted to give the reader a holistic understanding of the formidable challenges presented by cybersecurity and the urgent need for decisive cybersecurity measures to protect healthcare organizations from cyber-attacks (Parker, 2023; Perwej et al., 2021).

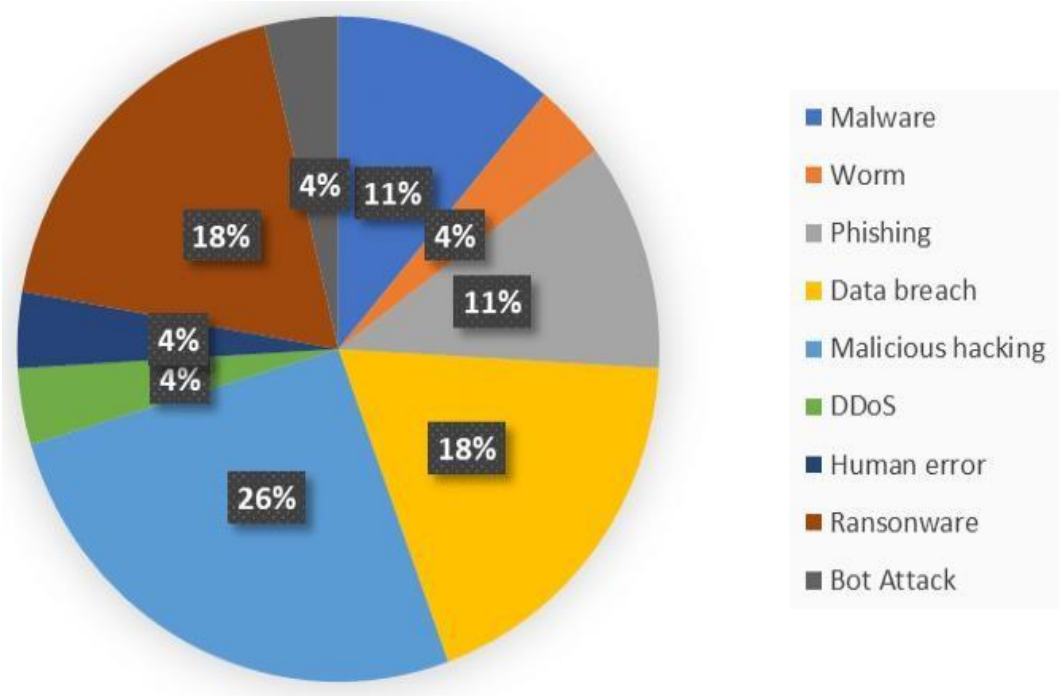

Figure 1 The Various Types of Malware Capable of Crippling the Healthcare Industry

The Allure of Healthcare Data

At the core of healthcare are the remarkable attributes of medical records, which contain personal and financial information that can be exploited by hackers. A recent publication in the Journal of the American Medical Informatics Association disclosed that a solitary medical record could fetch up to $1,000 on the illicit market, a significantly greater sum compared to credit card data (Van Uhm et al., 2021). This substantial amount highlights the lucrative nature of the healthcare data black market, where such information can be exploited for purposes such as identity theft, insurance fraud, and other illicit activities. Figure 2 describes the costly impact of malware by industry and Figure 3 describes the most recent healthcare breaches dating back to 2019 respectively.

Cybersecurity and Innovatove Technology Journal, Vol.3, No.2, 2025, pp. 58-67
e-ISSN 3025-6682. DOI: 10.53889/citj.v3i2.837

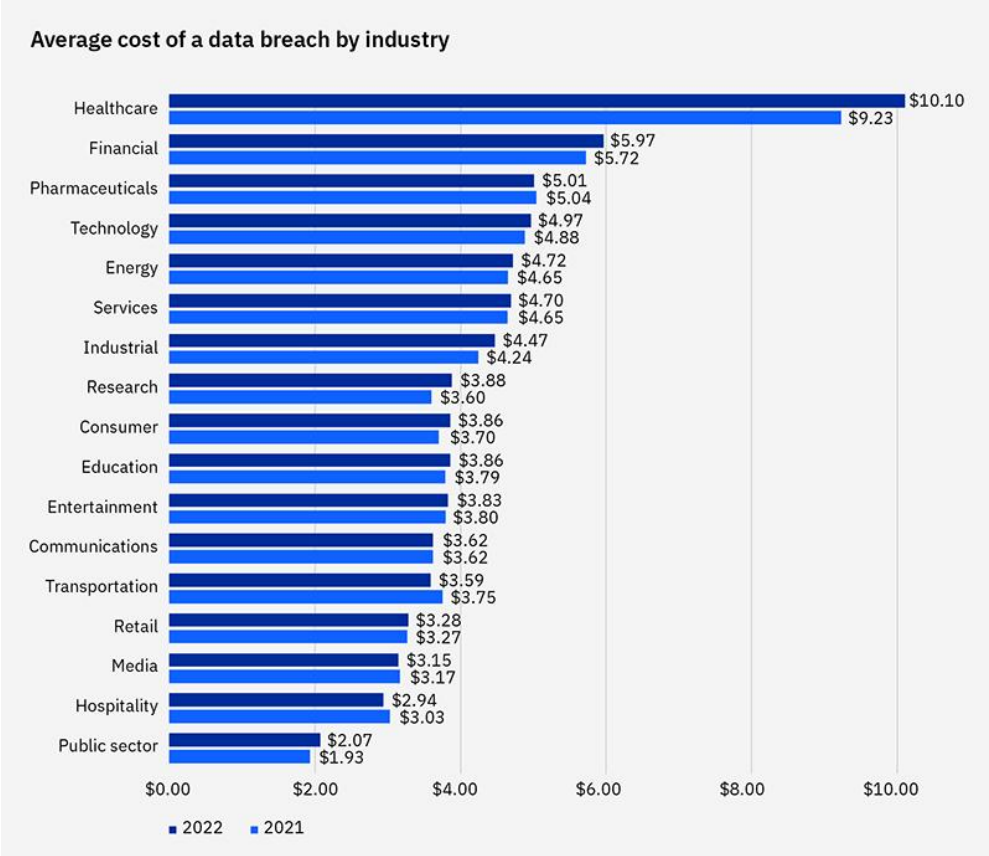

Figure 2 The Costly Impact of Malware by Industry

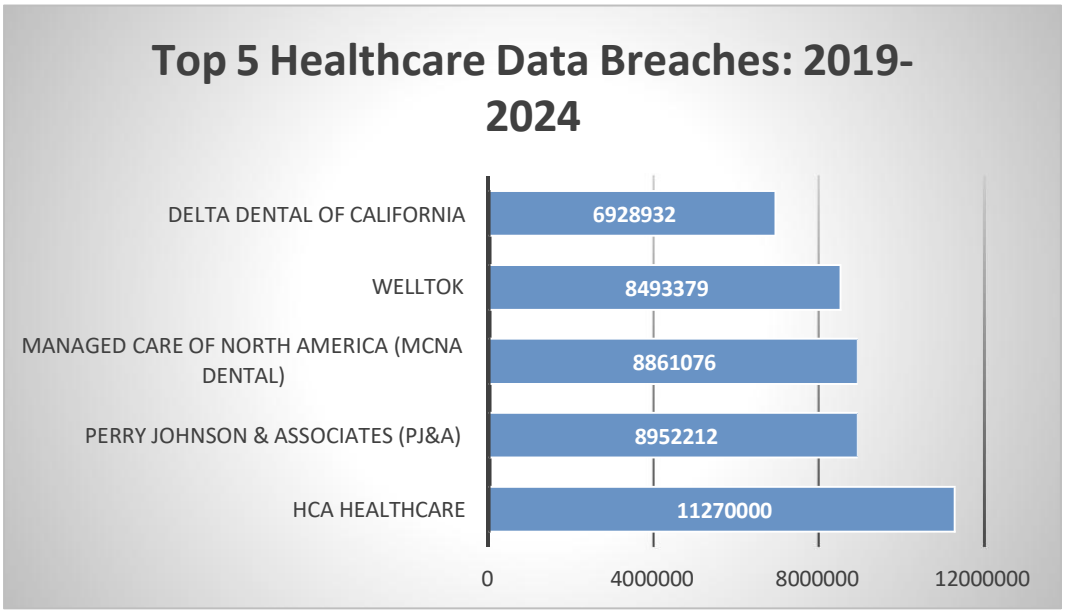

Figure 3 The Most Recent Healthcare Breaches Dating Back to 2019 Respectively

Ransomware: A Persistent Threat

Compounding this challenge is the healthcare industry's reliance on continuous access to patient data and medical systems, making it particularly vulnerable to ransomware attacks. Research published in the Journal of Medical Internet Research found that ransomware incidents in the healthcare sector increased by a staggering 94% between 2020 and 2021

(Schmitz-Berndt, 2023). Hackers can encrypt critical data and systems, effectively holding them hostage until a ransom is paid, exploiting the time-sensitive nature of healthcare operations and the potential for life-threatening consequences. Consequently, older systems of many healthcare organizations still exist, making them an easy target for hackers. An article published in the journal 'IEEE Access' showed that about 75% of medical devices running in the hospital are on unsupported operating systems. Therefore, they are very easy to exploit and gain access to the systems that have known vulnerabilities (Wasserman & Wasserman, 2022). The technology systems of medical facilities may be subject to different types of upgrading or replacement, which is a very complex and costly process, leaving hospitals and clinics open for cyber-attacks for a long time.

Regulatory Compliance: A Double-Edged Sword

The healthcare industry has a lot to do to comply with the stringent regulations of the law, such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S., and hackers will always find a way to exploit possible noncompliance. According to the JAMA study, the healthcare industry's average data breach cost was $7.13 million in 2020, and regulatory penalties comprised a great amount of this figure (Ke, et al., 2022). Hackers might throw their hats in the rig to exploit these weaknesses, as they are aware that the consequences of non-compliance with laws or damaging the reputation of the companies they're targeting can cost these organizations a fortune, which in turn can contribute to the necessity of paying ransoms or engaging in other expensive remediation efforts.

Remote Access: An Expanding Attack Surface

Lastly, the rapid growth in Remote Access Technologies and Telehealth Services in the healthcare industry has greatly expanded the chances for hackers to compromise. According to the research conducted by Van der Kleij et al. published in the International Journal of Medical Informatics, more than half of healthcare organizations faced cybersecurity issues while using remote access tools in 2021 (Van der Kleij et al. 2022). The improperly configured remote access points and privacy issues in telehealth platforms can be loopholes that enable cybercriminals to reach and penetrate the systems, stealing personal data. To counter these threats, healthcare organizations will need to prioritize cybersecurity among their topmost priorities through software updates, access controls, employee training, and the implementation of advanced security technologies. Partnerships created by mental health care providers, regulatory groups, and cyber security experts are essential to confront emerging threats and maintain the integrity and confidentiality of health data.

METHOD

Adopting a systematic and meticulous approach covering a thorough literature review and qualitative analysis, this study is aimed at examining the research on cyber criminals' punctual targeting of the healthcare sector (Perwej et al., 2021). The methodology involved the following steps: Firstly, it was conducted across various online databases, including Google Scholar, PubMed, IEEE Xplore, ACM Digital Library, and additional industry reports and cybersecurity incident databases using various search phrases related to the topic. The search terms applied featured complexes interlaced with words like "cybersecurity," "healthcare," "cybercriminals," "data breaches," "ransomware," and "cyberthreats," for all-encompassing and cogent research (Roumani, 2022). First, the initial search results have been examined regarding the overall relevance to the research topic and credibility of the sources along with the publication date (primary source from 2021 to 2024). Rigorous proportions of peer-reviewed journal articles, conference proceedings, government reports, and reports from respectable cybersecurity organizations have been delineated, which helped guarantee the material's reliability and quality (Kaur et al., 2021).

Furthermore, data from these selected sources were extracted and grouped according to the specific route of cybercrimes (i.e., motivation, methods, technique, case studies, and the impact of cybercrime on healthcare organizations) (Kelly et al., 2023). Employing qualitative analysis methods, like content analysis and thematic coding, was done so that patterns, trends, and insights that needed to be identified could facilitate the understanding of the intricacies that were at play (Keshta & Odeh, 2021). In their fourth part, the analysis of extracted data was synthesized and interpreted in an analytic process with rigor, which ultimately reached a detailed conclusion on hackers' preference to target the healthcare sector in their cyber-attacks, the possible consequences of successful attacks, and the challenges encountered by healthcare organizations in their defense against cyberthreats (Rachit et al., 2021). Finally, the correct referencing was carefully following the scholars' protocols and revealed the cited details in reference management software (e.g., Mendeley, Zotero) to complete the article (Thomasian & Adashi, 2021) using the highest academic standards of scholarly integrity (Wenhua et al., 2023).

RESULTS AND DISCUSSION

A detailed examination of the collected data revealed several key findings, including the healthcare sector's being cybercriminals' favorite target, their multi-dimensional motives, and the different strategies and tools they use in perpetrating their crimes (Adil et al., 2024). In the first place, it was revealed that the healthcare sector has as a target a multi-general threat, which counts nation-state actors, organized cybercriminal groups, hacktivist groups, and

individual hackers (Parker, 2023). Every side is fueled by individual drive, whether financial motives, espionage, ideological beliefs, or just the idea of overcoming security measures that are put down, and the threat spectrum's diversity is proliferating (van Boven et al., 2024). Unlike products sold through the dark web and black markets, patients' medical records and patient data found in medical records have very high economic value because of the sensitive nature of the information they contain (Perwej et al., 2021). This data can be sold to different unlawful actives, ranging from identity thieves to insurance fraudsters or even intelligence officers of state-owned interests who want to gather information; hence, cybercrime becomes a lucrative enterprise (Roumani, 2022).

Next, hackers using ransomware as their preferred way of attacking healthcare organizations have emerged as one of the significant challenges (Mikuleticet al., 2024). The pressure for healthcare providers to act quickly in urgent cases that can lead to patient harm is a significant factor that makes it easy for attackers to compel them to pay the ransom without hesitation, making this approach very profitable for such targets (Kaur et al., 2021). Hackers are perpetually looking for and exploiting IT healthcare systems, healthcare devices, and the proprietary nature of IoT technologies (Kelly et al., 2023). Legacy system infrastructure, an outdated software platform, and insufficient security measures provide attackers with a means of entry, hence the need for precise cyber security measures and regular updates to fight these threats (Keshta & Odeh, 2021). Lastly, pretexting strategies and social engineering techniques work well in helping hackers access healthcare systems and networks (Rachit et al., 2021). It is a common practice for cyber criminals to attack healthcare employees through emails or other messages sent to them with the primary intention of tricking them into revealing their usernames and passwords or infecting their systems with malware, compromising the human element as one aspect of possible security weakness in the medical security chain (Thomasian & Adashi, 2021).

Moreover, using inside actors, the criminal could intentionally mislead the patient information, or, on the other hand, they could be just negligent without committing a crime (Wenhua et al., 2023). The displeased staff or contractors with authority to access the sensitive systems and data can shortly help hack or obtain security leakage, which makes adopting all-encompassing access controls and employee training a big mandate (Adil et al., 2024). Cyber-attacks launched to successful ends on healthcare systems can have substantially negative impacts that involve leaking of patients' information, disruption of delivery of creditable medical services, losses of finances, image tarnish, and potential rights violations, which calls for immediate robust cyber protection measures and accident-response skills (Parker, 2023).

Last, results indicated that healthcare organizations have difficulties implementing secure measures as they have limited funds, constraints of legacy systems, and the momentum towards improvement of patient care is more than that in cybersecurity in return for operational efficiency and cybersecurity resilience (van Boven et al., 2024).

CONCLUSION

This all-encompassing study aggravates the fact that cybercriminals have a pronounced tendency toward healthcare institutions as weak spots, which prompts the healthcare sector to develop improved cybersecurity procedures (Perwej et al., 2021). Giving high value to medical data, individuals can acquire a bulk of money through ransomware attacks, capitalizing on the weak healthcare IT systems often present in medical device technologies, making healthcare organizations a wide range of thriving actors the core entities (Roumani, 2022). With an impressive range of techniques such as phishing simulations, social engineering, crushing through security gaps, and insider crimes, hackers use the military tactics needed to penetrate healthcare networks and expose sensitive data (Mikuleticet al., 2024). Penetration of successful cyber-attacks may take things to a different level: compromising the patient data, disrupting the primary medical services, bringing about financial losses, legal liabilities, and unfavorable reputational effects, which is the crucial reason the healthcare industry is so worried about cyberthreats (Kaur et al., 2021). There are still limitations, such as the need for more financial support, old-fashioned systems, and patient care being the priority over IT breaches (Kelly et al., 2023). Often, access to funding for cybersecurity advancements, inside outdated systems, and treating sick people as the top priority over cybersecurity fails as the major hurdles for the healthcare sector (Keshta & Odeh, 2021). It is vital to tackle these difficulties and implement robust cybersecurity procedures because it is essential to protect patient data guarantee uninterrupted healthcare service delivery and also reduce the risks associated with cyberthreats that are a continuous evolution (Rachit et al., 2021; Thomasian & Adashi, 2021).

SUGGESTIONS

To enhance cyber resilience and effectively address the affinity of cybercriminals for healthcare targets, a comprehensive and multifaceted approach is imperative (Wenhua et al., 2023). Increase Cybersecurity Investment: Healthcare organizations have to enact a high level of priority in the spending on cybersecurity and, thereby, invest an adequate amount of resources to execute effective security measures (Adil et al., 2024). These include obtaining state-of-the-art security technologies, designing relevant education programs, and integrating comprehensive incident response planning among employees (Parker, 2023). Adopt a Risk-Based Approach: Cybersecurity holds the highest risk in healthcare organizations. They have to

pay due attention to cybersecurity investments and fund adequate and strong defense mechanisms (van Boven et al., 2024). This includes acquiring the latest security systems technologies, arranging the all-encompassing employee training plan, and developing clear incident response procedures (Perwej et al., 2021). Implement Comprehensive Security Policies and Procedures: A complete set of security policies and methods addressing data protection, access control, and incident handling including the management of third parties should be an essential part of operations service (Roumani, 2022). These protocols and rules should be periodically assessed and technically refined in a dynamic atmosphere of cyber-danger development and methods of improvement (Mikuleticet al., 2024). Enhance Employee Awareness and Training: One of the strategies that must be implemented is the development of regular cybersecurity awareness and training programs for all healthcare employees (Kaur et al., 2021). They should indicate why only the observance of potential cyberthreats and quick reporting are irreplaceable, and they should spread knowledge about data storage and security rules (Kelly et al., 2023). Healthcare establishments can increase their general protection against cyber-attacks by promoting a cyber security-oriented culture (Keshta & Odeh, 2021). Strengthen Access Controls and Identity Management: Access controls and identification management systems are of utmost importance; they must secure data and system access to only registered personnel (Rachit et al., 2021). For example, multi-factor authentication, role-based access controls, and periodic auditing of privileged users mitigate malicious external forces and insider threats (Thomasian & Adashi, 2021). Prioritize Vulnerability Management and Patch Management: Identifying and remediating vulnerabilities in healthcare IT systems, medical devices, and IoT technologies is critical in ensuring robust protection against cyberthreats (Wenhua et al., 2023). It is, therefore, essential to develop a good riddance and mend process---periodical software updates and patching could contribute to minimizing Attack surfaces and counteracting known bugs and hiding places (Adil et al., 2024). Leverage Advanced Security Technologies: Implementing advanced IT security technologies like the next-generation intrusion prevention firewall, network-intrusion and security information and event management (SIEM) solutions, and endpoint protection platforms not only helps poorly detect and combat cyberthreats but also provides an end-to-end barrier to the cyber-attacks (Parker, 2023).

Through the implementation of such a set of recommendations that are aimed at enhancing cyber resilience, mitigating cybercrime risks, and protecting both patient data and the continuation of crucial medical services in an advanced technology and networked world, healthcare companies can eliminate the probability of malicious cyber-attacks and preserve the

confidentiality of vital data and business sustainability (van Boven et al., 2024; Perwej et al., 2021).

REFERENCES

Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare Internet of Things: Security Threats, Challenges and Future Research Directions. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2024.3360289

Cyber-Attacks by Type. Download Scientific Diagram. (n.d.). Retrieved March 15, 2024, from https://www.researchgate.net/figure/Cyber-Attacks-by-Type_fig2_359155431

Healthcare Data Breach Statistics. (n.d.). Retrieved March 14, 2024, from https://www.hipaajournal.com/healthcare-data-breach-statistics/

Kaur, M., Singh, D., Kumar, V., Gupta, B. B., & Abd El-Latif, A. A. (2021). Secure and energy efficient-based E-health care framework for green internet of things. *IEEE Transactions on Green Communications and Networking*, *5*(3), 1223-1231. https://doi.org/10.1109/TGCN.2021.3081616

Ke, J., Wang, W., & Foutz, N. Z. (2022). Heterogeneous consumer response and mitigation toward healthcare data breach: Insights from location big data. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4029103

Kelly, B., Quinn, C., Lawlor, A., Killeen, R., & Burrell, J. (2023). Cybersecurity in Healthcare. *Trends of Artificial Intelligence and Big Data for E-Health*, 213-231. https://doi.org/10.1007/978-3-031-11199-0_11

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, *22*(2), 177-183. https://doi.org/10.1016/j.eij.2020.07.003

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers & Security*, *136*, 103489. https://doi.org/10.1016/j.cose.2023.103489

Parker, M. (2023). Managing threats to health data and information: toward security. In *Health Information Exchange* (pp. 149-196). Academic Press. https://doi.org/10.1016/B978-0-323-90802-3.00016-2

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710. https://dx.doi.org/10.18535/ijsrm/v9i12.ec04

Rachit, Bhatt, S. & Ragiri, P.R. Security trends in Internet of Things: a survey. *SN Appl. Sci.* **3**, 121 (2021). https://doi.org/10.1007/s42452-021-04156-9

Roumani, Y. (2022). Detection time of data breaches. *Computers & Security*, *112*, 102508. https://doi.org/10.1016/j.cose.2021.102508

Schmitz-Berndt, S. (2023). Defining the reporting threshold for a cybersecurity incident under the NIS directive and the NIS 2 directive. *Journal of Cybersecurity*, *9*(1). https://doi.org/10.1093/cybsec/tyad009

The Cost of Cyberattacks in Healthcare in 2023 - Intraprise Health. (n.d.). Retrieved March 15, 2024, from https://intraprisehealth.com/the-cost-of-cyberattacks-in-healthcare

Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the internet of medical things. *Health Policy and Technology*, *10*(3), 100549. https://doi.org/10.1016/j.hlpt.2021.100549

van Boven, L. S., Kusters, R. W., Tin, D., van Osch, F. H., De Cauwer, H., Ketelings, L., & Barten, D. G. (2024). Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. *Annals of emergency medicine*, *83*(1), 46-56. https://doi.org/10.1016/j.annemergmed.2023.04.025

Van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. *Computers & Security*, *113*, 102535. https://doi.org/10.1016/j.cose.2021.102535

Van Uhm, D., South, N., & Wyatt, T. (2021). Connections between trades and trafficking in wildlife and drugs. *Trends in Organized Crime*, *24*(4), 425-446. https://doi.org/10.1007/s12117-021-09416-z

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

Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, *12*(3), 546. https://doi.org/10.3390/electronics12030546