Cybersecurity and Innovative Technology Journal, Vol.2, No.1, 2024, pp. 1-14
e-ISSN 3025-6682. DOI. 10.52889/citj.v2i1.338

The Growing Number of Cybersecurity Vulnerabilities Inside Healthcare Supply Chain

Submitted 10 December 2023, Revised 18 February 2024, Accepted 18 February 2024

Maurice L. McBride[1,2]*

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

[2]McBride Healthcare, Columbia, United States

Corresponding Email: *mmcbride@captechu.edu

Abstract

The healthcare supply chain is increasingly vulnerable to cybersecurity risks due to the integration of digital technology. The rise of digital records, telemedicine, and network connectivity has made it more susceptible to cyberattacks. The COVID-19 pandemic has further exacerbated this vulnerability, highlighting deficiencies in medical supplies, equipment, and services. The sector has implemented cybersecurity precautions, such as following HIPAA and GDPR, and collaborating with authorities and experts. However, the changing threat landscape necessitates continuous updates and changes. The study uses secondary data from the past three years to highlight the need for strong cybersecurity protocols to protect patient data, deliver services, and defend the supply chain from new threats. Future research should explore leveraging blockchain and AI-based cybersecurity, as well as strengthening government regulation, international cooperation, cybersecurity education, and patient empowerment.

Keywords: Healthcare, Cybersecurity, Privacy, Security, Supply Chain

INTRODUCTION

The healthcare industry has changed significantly as a result of the digital revolution. However, the healthcare industry is becoming a primary target for cyber-attacks due to the introduction of digital health records, telemedicine, and other technical improvements. These dangers do not exclude the healthcare supply chain, an essential part of the healthcare ecosystem. Various parties are involved in the healthcare supply chain, including patients, healthcare providers, and distributors. It includes procedures including manufacturing, distributing, and providing medical supplies and services. These businesses are becoming increasingly integrated via digital networks, which makes the healthcare supply chain more susceptible to cyberattacks.

Cybersecurity flaws may result in patient injury, interrupted healthcare services, or illegal access to private patient data. An assault on a hospital's supply chain, for example, would stop the flow of necessary medical supplies, which would have an impact on patient care. Analogously, a security breach in the network of a pharmaceutical corporation may result in unapproved entry to confidential information, including medication formulations or patient records. Concern should be expressed about the rising number of cybersecurity flaws in the healthcare supply chain. In addition to endangering patient privacy and safety, it has serious

financial ramifications. The healthcare industry had the highest average cost of a data breach in 2020, with an estimated $7.13 million (Wasserman & Wasserman, 2022).

In addition, the COVID-19 epidemic has made matters worse. Cyber threats now have new targets due to the fast adoption of telehealth services and the growing dependence on digital technology (He et al., 2020). Simultaneously, fraudsters are evolving in sophistication, using cutting-edge methods to take advantage of weaknesses in the healthcare supply chain. Strong cybersecurity safeguards are essential, as shown by the rise in cybersecurity vulnerabilities in the healthcare supply chain. It is critical to address these vulnerabilities as the healthcare industry embraces digital transformation in order to safeguard patient data, guarantee the provision of healthcare services, and maintain public confidence in the healthcare system.

Background

The evolution of healthcare cybersecurity is long and convoluted. There has been an increase in cybercrime and data breaches in the healthcare sector during the last decade. Patient data and the healthcare supply chain were both affected by these events, highlighting the sector's vulnerability and the urgent need for solid cybersecurity safeguards.

Historical Incidents of Cyber Threats

An increasing number of cybersecurity dangers have followed the healthcare industry's digital transformation. These dangers have changed, moving from nefarious hackers looking to make money to more crafty and focused assaults. An important turning point in this development was the ransomware outbreak known as WannaCry. The National Health Service (NHS) in England and Scotland was severely affected by the attack on May 12, 2017, a noteworthy cybersecurity incident (Skertic, 2021). The hack had a sizeable global effect on healthcare systems. A malicious virus known as WannaCry encrypted data on compromised machines, and the hackers requested a ransom to be paid before granting users access. It was the biggest cyberattack to impact England's National Health Service. At least 34% of trusts in England experienced significant disruptions due to the assault on the NHS. Thousands of surgeries and appointments had to be canceled as a result of the assault, which directly affected patient care. Six thousand nine hundred twelve appointments, including canceled procedures, were reported to NHS England as a direct consequence of the ransomware.

Nonetheless, it was calculated that around 19,000 appointments may have been impacted. NHS Digital said that, despite the extensive interruption, it thinks no patient data was lost or stolen. However, the incident showed how susceptible healthcare systems are to cyberattacks and how important it is to have robust cybersecurity protections (Yuryna Connolly et al., 2020). The National Health Service (NHS) has worked hard to strengthen its security posture after the

WannaCry assault. Actually, since 2017, it has only seen six successful ransomware assaults, as opposed to 203 in the three years before. Notwithstanding these advancements, the ongoing evolution and sophistication of cyber-attacks pose a severe danger to cybersecurity, which continues to be a top priority for healthcare systems globally (Yuryna Connolly et al., 2020).

In 2015, one of the biggest health insurance firms in the US, Anthem (now Elevance Health), was the target of a cyberattack. This was another significant breach. The Anthem breach significantly impacted the healthcare sector. Anthem, Inc. revealed in February 2015 that it had been breached by malevolent hackers, who may have taken over 37.5 million records, including personally identifiable information. Later, the figure was increased to 78.8 million individuals whose personal data was compromised (Cartwright, 2023). Names, birthdays, medical IDs, social security numbers, street addresses, email addresses, and work information, including salary data, were among the compromised data. The month before the data breach was detected, the data was taken over a few weeks. Since no medical data was exposed, Anthem was exempt from legal requirements to encrypt the material.

However, Anthem was the target of many civil class-action lawsuits, which were resolved for $115 million in 2017. Individuals whose data was compromised may have lifelong issues related to identity theft (Wilner et al., 2022). American International Group provided Anthem with insurance coverage of US$100 million against cyber-related issues. According to one source, the cost of alerting consumers to the hack may use up all this money. Anthem contacted cybersecurity company Mandiant to assess their security protocols and advised those whose information was pilfered to keep an eye on their accounts and exercise caution. The data theft typically aroused concerns over the theft of medical data. Strong cybersecurity safeguards are crucial, and this event served as a wake-up call for the healthcare sector. It raised awareness and could have resulted in changes to government data safety laws and security procedures.

Impact on the Healthcare Supply Chain

Cybersecurity risks significantly impact the healthcare supply chain. The movement of products, data, and services needed for patient care is called the supply chain. These items include hospital supplies, digital health solutions, and medications and medical equipment (Scott et al., 2020). Supply chain cyberattacks have the potential to impede the smooth movement of these vital commodities. There may be dire repercussions if the framework is breached. A cyberattack on the systems of a pharmaceutical firm, for instance, can cause delays in the manufacturing and delivery of pharmaceuticals, affecting patients' access to life-saving prescriptions. Similarly, a medical device firm may come under assault and lose critical equipment, endangering patients' lives (Paul et al., 2023). Wide-ranging repercussions may

result from these supply chain interruptions, including monetary losses and—more importantly—the safety of patients.

Additionally, throughout the epidemic, hackers have taken advantage of fresh openings by targeting front-line institutions like clinics and hospitals. The healthcare sector saw a sharp increase in ransomware assaults between 2020 and 2023. Maze, Conti, Netwalker, Revil, and Ryuk were the primary ransomware groups that targeted the healthcare industry (Neprash et al., 2022). In 2020, these organizations were responsible for 75% of all assaults on the industry. The supply chains set up to provide ransomware gangs and other threat actors access to credentials for healthcare networks witnessed a considerable decrease in the barrier to entry for assaults in the industry. As a result, there were more Initial Access Brokers (IABs), hackers that hunt for and compromise weak networks to sell access to the highest bidder, which may include ransomware gangs and their affiliates. Additionally, seven additional vulnerabilities were found that affect the PTC Axeda agent and jeopardize the security of medical devices and supply chains. Threat actors could be able to access data, change system settings, and remotely execute malware thanks to these vulnerabilities. These vulnerabilities could impact more than 150 devices across more than 100 companies.

Evolution of Cyber Threats and Industry Response

Cyber dangers have evolved in the healthcare sector in a way that is both substantial and alarming. Hospital computerization some years ago marked the beginning of the digital revolution in healthcare. One of the most targeted and lucrative industries that cyber criminals and cyber terrorists target these days is healthcare. Cybercriminals focus primarily on this site because of its valuable information, essential infrastructure status, and mobile services (Seh et al., 2020). The attack surface has grown due to the digitalization of healthcare procedures and records. Nowadays, a lot of sensitive patient data is stored in electronic health records (EHRs), which makes them attractive targets. Furthermore, the spread of Internet of Things (IoT) gadgets in the medical field, such as linked medical equipment and remote monitoring tools, has given hackers additional avenues of entrance (Scott et al., 2020).

As cyber risks continue to escalate, the healthcare sector has started to adjust. In order to safeguard patient data and guarantee continuity of service, hospitals, and other healthcare institutions have realized how critical it is to invest in cybersecurity safeguards. They have employed specialized cybersecurity staff, expanded their IT security expenditures, and deployed cutting-edge security measures. The Health Industry Cybersecurity Practices (HICP) 2023 Edition is a foundational publication that aims to provide best practices, raise awareness

of cybersecurity risks, and assist the healthcare industry in setting standards for mitigating the most relevant cybersecurity threats to the industry.

In addition, the sector has begun implementing cybersecurity standards and best practices. The United States, for example, requires security and privacy safeguards for patient data under the Health Insurance Portability and Accountability Act (HIPAA). Enhancing the cybersecurity posture of the act's covered companies and business partners is the industry's main priority. Therefore, bodies such as the HHS are in charge of enforcing the Privacy, Security, and Breach Notification Rules under HIPAA. Further international standards and laws have been developed, such as the General Data Protection Regulation (GDPR) in Europe, to safeguard patient privacy and data (Ducato, 2020). Cooperation has been essential to enhancing cybersecurity in the medical field. Public-private collaborations have been established to exchange creative ideas, best practices, and threat information. The healthcare sector has worked with governmental organizations and cybersecurity specialists to resolve weaknesses and create all-encompassing plans for protecting against cyberattacks.

Cybersecurity should be a top concern for healthcare companies regarding resources, technology, and operations. This entails expanding cybersecurity budgets, improving cybersecurity awareness and training initiatives, updating or replacing outdated systems, and conducting end-to-end security risk assessments. The healthcare sector has seen a notable increase in cyber risks, but the sector has responded with strength and initiative. Enhancing cybersecurity procedures, increasing public awareness, and putting policies in place to lessen the dangers brought on by these attacks are the main goals.

METHOD

In this study, a secondary data analysis methodology was utilized to look at cybersecurity flaws in the healthcare supply chain. Secondary data analysis is a relevant and helpful approach to answering research questions and entails reviewing and reevaluating data already obtained for various reasons.

Type of Data

Utilizing pre-existing data from reliable sources—such as reports, industry-specific databases, and scholarly journals—is the primary goal of the study. This information is pertinent, suitable, and necessary to address the research question since it sheds light on how cybersecurity is changing in the healthcare supply chain. Because healthcare data is sensitive and personal, using existing data may be especially helpful when gathering original data may prove difficult.

Data Collection Process

Current data was ensured by conducting a thorough evaluation of scholarly works that had been published in the previous three years before beginning the data-gathering procedure. Papers were gathered reputable places such as the National Library of Medicine, Science Direct, the Taylor & Francis Online, and other cybersecurity-related peer-reviewed journals. These resources provide a thorough summary of the situation of supply chain and healthcare cybersecurity. In addition, healthcare-related databases were used, concentrating on cybersecurity events, threat patterns, and supply chain best practices. By reviewing academic journals, industry documents, and reports, a dataset containing relevant data related to the study issue was assembled.

Data Analysis

Following data collection, data analysis method included many crucial processes, which began by content analyzing the collected literature and grouping the data into themes and subtopics. This made it possible for us to pinpoint prevalent cyber threat categories, weak points, and how they affect healthcare provision. Qualitative analysis was carried out to evaluate the quality of the data sources and ascertain their applicability to the study issue. This procedure included assessing the legitimacy and dependability of the chosen sources to make sure they were from respectable and authoritative organizations in the cybersecurity and healthcare fields. To improve the analysis, data synthesis methods, such as theme coding, was used, which required taking the most important conclusions and revelations from the chosen sources, contrasting and analyzing them, and spotting reoccurring themes and patterns. A comprehensive insight into the cybersecurity risks throughout the healthcare supply chain was created using qualitative data analysis techniques.

Justification of Approach

The method of secondary data analysis is key to obtaining data from various sources by depending on pre-existing data despite the delicate and intricate nature of cybersecurity in the healthcare industry. The data was ensured to accurately represent the current level of cybersecurity in the healthcare supply chain by using recent sources, all of which were published within the previous three years. Through a complete assessment of scholarly literature, reputable publications, and industry databases, a large dataset was compiled that enabled a holistic and empirical approach to the research topic. Much knowledge was gained from the method on typical cyber threat categories, weak points, and possible effects on healthcare delivery.

RESULTS AND DISCUSSION

The present situation of cybersecurity in the healthcare supply chain is a significant problem. The supply chain's security has emerged as one of the significant dangers in the healthcare industry, as the cyber threat environment is continually changing and becoming more dangerous.

Without a doubt, technological improvements in the healthcare sector have improved the accuracy of healthcare delivery. However, this technological revolution has also made the healthcare industry more vulnerable to a growing number of cybersecurity risks. According to Argaw et al. (2020), the healthcare sector is one of the most vulnerable industries to cyberattacks worldwide, as shown by the 2016 research from IBM and the Ponemon Institute. The primary cause of this increased danger is fraudsters' attraction to health data owing to its value.

Moreover, Argaw et al. (2020) assert that patient medical records have a wealth of sensitive information, including blood type, surgery history, diagnoses, and personal identifiers. Once this data is stolen, it is impossible to recover its privacy entirely, putting people at risk of identity theft and mental trauma. Beyond the effects on people, as the WannaCry ransomware assault on the UK's National Health System hospitals in 2017 showed, cyberattacks may impair hospital operations, jeopardize patient care, and cause severe delays in treatment (Argaw et al., 2020).

These can have long-lasting effects on healthcare organizations' finances and reputation, in addition to causing acute operational difficulties. With its interdisciplinary approach, the M8 Alliance has taken on a crucial initiative to address the cybersecurity dangers that hospitals worldwide are experiencing in this challenging environment. Through extensive scoping assessments, expert meetings, and teleconferences, the partnership hopes to provide valuable suggestions that hospitals may use to strengthen their defenses against cyberattacks.

Furthermore, Argaw et al. (2020) underscore that because the healthcare sector is vulnerable to cyberattacks, strong cybersecurity measures are desperately needed. The healthcare business is increasingly dependent on linked medical equipment and digital records. Therefore, protecting patient data and ensuring treatment is provided continuously are critical (Argaw et al., 2020). Research activities must keep concentrating on improving cybersecurity tactics, creating defenses, and encouraging multidisciplinary cooperation to ensure that healthcare is accurate, safe, and robust in the face of changing threats.

Alawida et al. (2022) provide a thorough analysis of the changing cybersecurity threats facing the healthcare industry, highlighting the crucial problems that may affect the healthcare

supply chain. The ongoing worries and new dangers that healthcare institutions must deal with are highlighted in their study. Ransomware is still dangerous since it may harm a brand's reputation, interrupt patient treatment, and have financial repercussions. According to survey findings, healthcare executives generally agree on the main dangers, which include insider threats, phishing attacks, ransomware, breaches involving partners or third parties, and data breaches (Alawida et al., 2022). Given how much the healthcare supply chain depends on the accuracy and accessibility of data and services, these risks have a significant impact on it.

These initiatives highlight the importance of healthcare research and data in the supply chain. According to Beaman et al. (2021), increasing the Ransomware-as-a-Service (RaaS) model will provide difficulties for healthcare institutions. Recent supply chain breaches show how threat actors are changing their tactics. The emphasis impacts the integrity of the supply chain on breaching cloud providers to get access to sensitive data (Alawida et al., 2022). Compromises using operational technology (OTOT) pose a growing risk, potentially creating vulnerabilities in the supply chain. Threat actors may take advantage of vendor upgrades or vulnerabilities in Primary Logic Controllers (PLCs) to exploit OTOT vulnerabilities, which might interrupt operations and jeopardize data integrity, thus affecting the healthcare supply chain (Wang et al., 2023).

Moreover, assaults on operational technology environments and supply chains demonstrate the attackers' ongoing evolution and improvement of their strategies (Sobb et al., 2020). For example, supply chain security gained national attention after the 2020 SolarWinds breach. According to Sathiya et al. (2023), over 80% of healthcare firms polled have a software supply chain risk management policy. However, the lack of cyber capabilities has persisted for years, and as a consequence, healthcare companies are still vulnerable to assaults. This emphasizes how the healthcare industry needs a robust cybersecurity workforce to meet these issues.

The need for safe and effective remote work is more significant than ever. Zhang (2023) claims that telehealth and remote patient monitoring have been more widely used in the healthcare industry, highlighting the need to reroute network traffic to cloud-based services. Protecting sensitive patient data and upholding the integrity of healthcare systems have become critical as healthcare professionals depend increasingly on digital platforms to provide treatment (Zhang, 2023). The hybrid work paradigm standard in healthcare environments emphasizes, even more how important it is to maintain strict security and privacy requirements while allowing greater access to essential apps. Strong cybersecurity protections are necessary

for healthcare personnel, who often operate remotely or in hybrid settings and need smooth access to patient data, diagnostic tools, and telemedicine platforms (Zhang, 2023).

Moreover, maintaining patient and stakeholder confidence while adhering to stringent privacy laws like HIPAA is a twin challenge for healthcare firms. Building this confidence requires transparency and accountability, essential components of a zero-trust strategy (Zhang, 2023). Healthcare providers may impose stringent access restrictions and guarantee that only authorized staff have access to patient data and essential systems by implementing a zero-trust architecture.

Neale et al. (2022) state that strict verification of all entities accessing sensitive data or systems is necessary when applying the zero-trust model to the supply chain. This lowers the attack surface and improves control over data access. Another crucial component is micro-segmentation, which makes sure that even if a single supply chain link is breached, the danger is limited and does not spread to harm the network as a whole. Within the context of cyberattacks, Adams (2023) highlights the significance of 'assuming breach' and concentrating on breach control. Hospitals may reduce interruptions to vital services and patient care by isolating impacted systems, restricting lateral movement, and using breach containment technologies like Zero Trust Segmentation (ZTS). Conducting regular cybersecurity audits is crucial in detecting weaknesses prior to their exploitation by malicious actors.

To fully understand the state of cybersecurity vulnerabilities within the healthcare supply chain, further crucial information is provided by (Ghadge et al., 2020). The authors provide a thorough rundown of all the cybersecurity threats that are common in the healthcare supply chain. Technology in the healthcare sector is advancing, and with it, so is the need for appropriate risk management procedures and evaluations of suppliers and outside service providers to reduce the possibility of supply chain exploitation. According to Ghadge et al. (2020), a Healthcare Delivery Organization (HDO) should include vendor and external supply chain risk assessments into its internal security policies since hacked networks might jeopardize systems. Strong cybersecurity protections are essential in the healthcare supply chain because of the sensitive data involved and the possible effects on patient care. Proactive cybersecurity is encouraged by Ghadge et al. (2020), who stress the value of regular risk assessments and the deployment of strong security measures. Their study gives essential insights for healthcare firms looking to improve their cybersecurity safeguards and substantially contributes to the knowledge of cybersecurity hazards in the healthcare supply chain.

The growing threat of supply chain assaults by third parties has increased recently, especially in 2021 through 2023, after the emergence of COVID-19. Because the healthcare

supply chain depends so heavily on outside parties, such as manufacturers of pharmaceuticals and suppliers of medical equipment, these assaults pose a severe threat to the suppliers or vendors that offer products and services to organizations. These kinds of assaults have the potential to seriously compromise patient data and safety inside the healthcare supply chain.

According to Sathiya et al. (2023), the COVID-19 pandemic uncovered fundamental vulnerabilities in healthcare supply chains, significantly hurting healthcare systems. These disturbances not only affect the accessibility of medicinal supplies but also heighten healthcare cybersecurity risks. An increase in potential targets for cyberattacks has resulted from the unexpected demand for digital healthcare technology during the pandemic. In their haste to implement digital solutions, healthcare companies often neglect security safeguards, leaving them vulnerable to assaults. Chain of Things (CoT) technology, which mixes IoT and blockchain, may make the healthcare supply chain more reliable and open to scrutiny. Concerns about the confidentiality of sensitive medical information may also be allayed in this way (Sathiya et al., 2023). By taking a comprehensive strategy, healthcare systems may become more resilient to disturbances and cyber attacks.

CONCLUSION

Maintaining the resilience and integrity of the healthcare supply chain depends critically on cybersecurity. The healthcare industry as a whole continues to be a profitable target for a variety of cyber threats, including nation-state threats, ransomware attacks, and supply chain breaches that are constantly becoming more sophisticated. To correctly manage these dangers, lawmakers, healthcare providers, and other stakeholders must understand how important it is to have robust cybersecurity safeguards in place. The recent supply chain hacks show that cybersecurity is not only an IT problem but also a crucial part of healthcare infrastructure. Due to increased connectivity, digital reliance, and the Internet of Medical Things (IoMT), the attack surface of the healthcare supply chain has risen. In this context, the risks not only include data breaches and disruptions in operations but also potential threats to patient care and life-saving medications.

Legislators, stakeholders, and healthcare professionals must act quickly to address the consequences of these revelations. First and foremost, healthcare organizations must make cybersecurity a central component of their business. Patient safety, service reliability, privacy, and confidentiality may all be compromised without a solid healthcare supply chain. Providers must spend money on incident response plans, cybersecurity measures, and awareness training to combat the expanding threats.

Policymakers are crucial for the development of the regulatory framework for healthcare cybersecurity. Legislation and regulations to enforce information security standards and report intrusions in the healthcare sector should be seriously considered. Policymakers also need to provide resources to healthcare cybersecurity R&D to stay ahead of emerging threats.

In addition, healthcare organizations need to interact closely with other stakeholders, such as suppliers, healthcare technology providers, and third-party service providers. Organizations involved in the healthcare supply chain should have adequate supply chain security policies, conduct regular cybersecurity assessments, and adhere to stringent security criteria in order to reduce risks in the supply chain.

The healthcare industry must understand how critical supply chain cybersecurity is to delivering high-quality patient care and safeguarding private patient information. Healthcare providers, legislators, and other stakeholders may work together to strengthen the cybersecurity posture of the healthcare supply chain and defend it against the increasing number of cyberattacks by adopting proactive measures and promoting a culture of security awareness.

SUGGESTIONS

The ever-changing landscape of cybersecurity risks in the healthcare industry highlights the need for ongoing research and development in several vital domains. These recommendations are pivotal in shaping the future of healthcare cybersecurity:

1. Development of Advanced Cybersecurity Solutions: The demand for innovative cybersecurity solutions is growing as cyber threats become more complex. The focus of future research should be on creating AI-based instruments that can anticipate and stop cyberattacks before they have a chance to do damage. It would be beneficial to investigate how blockchain technology may improve the security and accuracy of medical data. Using these cutting-edge technologies, the healthcare industry may strengthen its defenses against new dangers.

2. Role of Government in Regulating Cybersecurity in Healthcare: The environment around healthcare cybersecurity is significantly shaped by government rules. Subsequent investigations need to examine the efficacy of current governmental rules and provide suggestions for improving them. Finding a balance between operational effectiveness and regulatory compliance is a crucial issue that needs more research. The results may help design regulations that support robust cybersecurity procedures while guaranteeing the smooth operation of healthcare institutions.

3. Need for Global Cooperation to Address Cyber Threats: International cooperation is required since cyber dangers are not limited by physical location. Subsequent investigations need to examine avenues for worldwide collaboration, examining the function of global

institutions in enabling the sharing of cybersecurity best practices and threat information. Combined, these cooperative efforts may provide a substantial barrier against transnational threats.

4. Cybersecurity Education and Training: In light of the dearth of qualified cybersecurity specialists in the healthcare industry, future studies should concentrate on creating efficient curriculum and training initiatives. These courses could explore the proficiencies needed by cybersecurity experts in the healthcare industry and look at the best ways to teach cybersecurity knowledge. Providing workers with the necessary training and expertise is essential to protecting the industry against cyberattacks.

5. Patient's Role in Healthcare Cybersecurity: Healthcare technology end users include patients whose behavior has a significant impact on the security of these systems. Future studies should examine how to inform patients about cybersecurity and promote responsible online conduct. Healthcare firms may provide a more secure environment for their data and services by educating patients and offering help.

REFERENCES

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues after Covid-19: A survey. *Journal of King Saud University – Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/s12911-020-01161-7

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges, and future research directions. *Computers & Security*, *111*(1). https://doi.org/10.1016/j.cose.2021.102490

Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. *Journal of Clinical Monitoring and Computing, p. 37*. https://doi.org/10.1007/s10877-023-01013-5

Ducato, R. (2020). Data protection, scientific research, and the role of information. *Computer Law & Security Review*, *37*(105412). Science Direct. https://doi.org/10.1016/j.clsr.2020.105412

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223–240. https://doi.org/10.1108/scm-10-2018-0357

He, Y., Aliyu, A., Evans, M., & Luo, C. (2020). Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID-19: A Scoping Review (Preprint). *Journal of Medical Internet Research*, *23*(4). ncbi. https://doi.org/10.2196/21747

Neale, C., Kennedy, I., Price, B., Yu, Y., & Nuseibeh, B. (2022). The case for Zero Trust Digital Forensics. *Forensic Science International: Digital Investigation*, *40*, 301352. https://doi.org/10.1016/j.fsidi.2022.301352

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, *3*(12), e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express*, *9*(4). https://doi.org/10.1016/j.icte.2023.02.007

Sathiya, V., Nagalakshmi, K., Jeevamalar, J., Anand Babu, R., Karthi, R., Acevedo-Duque, Á., Lavanya, R., & Ramabalan, S. (2023). Reshaping healthcare supply chain using chain-of-things technology and key lessons experienced from the COVID-19 pandemic. *Socio-Economic Planning Sciences*, *85*(101510), 101510. https://doi.org/10.1016/j.seps.2023.101510

Scott, B. K., Miller, G. T., Fonda, S. J., Yeaw, R. E., Gaudaen, J. C., Pavliscsak, H. H., Quinn, M. T., & Pamplin, J. C. (2020). Advanced Digital Health Technologies for COVID-19 and Future Emergencies. *Telemedicine journal and e-health: the official journal of the American Telemedicine Association*, *26*(10), 1226–1233. https://doi.org/10.1089/tmj.2020.0140

Skertic, J. (2021). Cybersecurity Legislation and Ransomware Attacks in the United States, 2015-2019. *Doctor of Philosophy (PhD), Dissertation, Political Science & Geography, Old Dominion University*. https://doi.org/10.25777/c0vq-t159

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), 133. NCBI. https://doi.org/10.3390/healthcare8020133

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics*, *9*(11), 1864. mdpi. https://doi.org/10.3390/electronics9111864

Wang, Z., Zhang, Y., Chen, Y., Liu, H., Wang, B., & Wang, C. (2023). A Survey on Programmable Logic Controller Vulnerabilities, Attacks, Detections, and Forensics. *Processes*, *11*(3), 918. https://doi.org/10.3390/pr11030918

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

Wilner, A. S., Luce, H., Ouellet, E., Williams, O., & Costa, N. (2022). From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector. *International Journal:*

Canada's Journal of Global Policy Analysis, *76*(4), 002070202110679. https://doi.org/10.1177/00207020211067946

Yuryna Connolly, L., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: assessing severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa023

Zhang, Y. (2023). Privacy-Preserving with Zero Trust Computational Intelligent Hybrid Technique to English Education Model. *Applied Artificial Intelligence*, *37*(1). https://doi.org/10.1080/08839514.2023.2219560