Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies

Elham Abdullah Al-Qarni
Department of Computing and Information Technology
University of Bisha
Bisha-Saudi Arabia

***Abstract*—Cyberattacks on several businesses, including those in the healthcare, finance, and industrial sectors, have significantly increased in recent years. Due to inadequate security measures, antiquated practices, and sensitive data, including usernames, passwords, and medical records, the healthcare sector has emerged as a top target for cybercriminals. Cybersecurity has not gotten enough attention in the healthcare sector, despite being crucial for patient safety and a hospital's reputation. In order to prevent data breaches that could jeopardize the privacy of patients' information, hospitals must deploy the proper IT security measures. This research article reviews many scholarly publications that look at ransomware attacks and other cyberattacks on hospitals between 2014 and 2020. The report summarizes the most recent defensive measures put forth in scholarly works that can be used in the healthcare industry. Additionally, the report provides a general review of the effects of cyberattacks and the steps hospitals have taken to manage and recover from these disasters. The study shows that cyberattacks on hospitals have serious repercussions and emphasizes the significance of giving cybersecurity a priority in the healthcare sector. To combat cyberattacks, hospitals must have clear policies and backup plans, constantly upgrade their systems, and instruct employees on how to spot and handle online threats. The article comes to the conclusion that putting in place suitable cybersecurity safeguards can reduce the harm brought on by system failures, reputational damage, and other associated problems.**

Keywords*—*Cybersecurity; healthcare industry; malware; ransomware; DoS; DDoS

I. INTRODUCTION

The healthcare sector is very concerned about security, especially on the internet, where cyberattacks are becoming more common and sophisticated. Access control violations, assaults that inject and execute malware, and denial of service (DoS) attacks are some of the most frequent threats to healthcare security. In contrast to Distributed Denial of Service (DDoS) assaults, which employ numerous hosts to attack a system, DoS attacks include a single source that floods the target system with requests. This makes it difficult to pinpoint the attack's origin. Patients may suffer as a result of these attacks, and healthcare organizations may suffer reputational damage [1].

Another major threat to the healthcare sector is malware, which virtually always comes in new varieties. Ransomware is one malware family that healthcare institutions are becoming worried about. Ransomware was listed second on a list of cybersecurity dangers to healthcare companies in a poll by the Healthcare Information and Management Systems Society (HIMSS), with 17% of respondents reporting having been the victim of a ransomware attack [2].

Healthcare businesses have been the subject of several high-profile cyberattacks in recent years. For instance, a ransomware assault that affected the Irish Health Service Executive (HSE) in 2021 severely disrupted healthcare services [3]. Similar to this, over 150 nations were impacted by the WannaCry ransomware assault in 2017, which forced the UK's National Health Service (NHS) to reschedule procedures and cancel appointments [4].

Healthcare institutions must put robust cybersecurity safeguards in place to stop cyberattacks and safeguard sensitive patient data. Many healthcare institutions, however, continue to lack adequate security protocols, leaving them open to intrusions. Only 44% of healthcare businesses, according to a study by the Ponemon Institute, have a thorough security policy in place [5].

Based on responses from 167 healthcare cybersecurity specialists, Fig. 1 shows the survey's ranking of cyberattacks in 2021. The author's method involved doing a content assessment of scientific papers from 2014 to 2020 that discussed malware, DoS, and social engineering attacks on hospitals.

There are five sections in the paper. Hospitals that experienced cyberattacks from 2014 to 2020 are covered in Section II. Hospitals can apply the measures discussed in Section III to lessen or prevent a cyberattack. Results and discussion are presented in Section IV, and the paper is wrapped up in Section V.

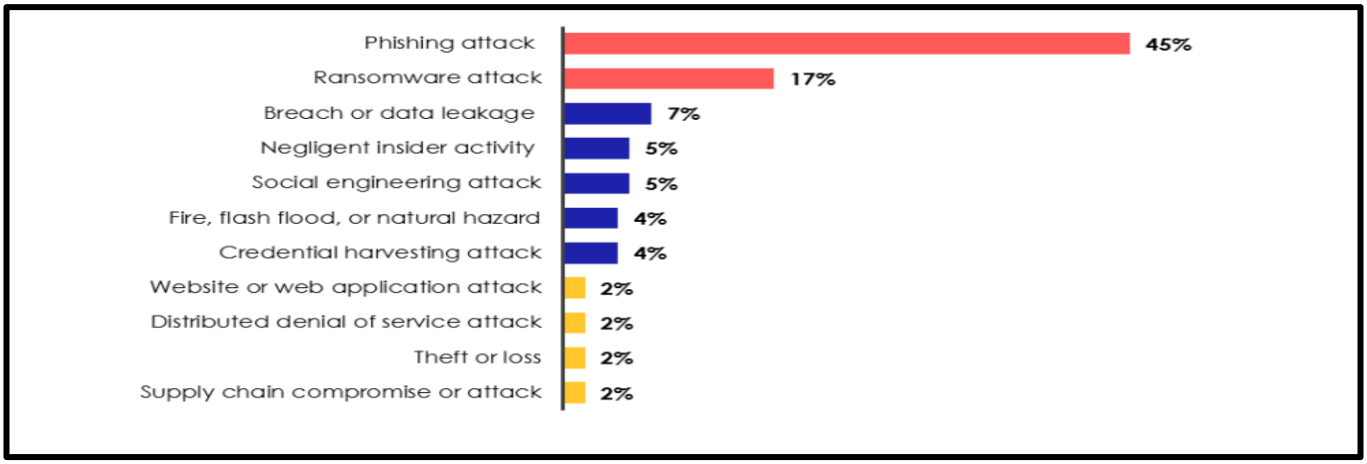

Fig. 1. A list of the most significant cyberattacks for 2021 [2].

II. Cybersecurity in Healthcare Systems

In this section, we'll talk about a number of hospitals that experienced cyberattacks, the steps we took to deal with the situation, and the effects of the attacks.

Table I gives a summary of cyberattacks on hospitals, including ransomware and distributed denial of service (DDoS), as well as the results. For instance, on March 20, 2014, a DDoS attack targeted Boston Hospital, causing a network outage that lasted two weeks and adversely disrupting hospital operations. In 2016, ransomware that used social engineering techniques struck Lukas Hospital and Hollywood Presbyterian Medical, disrupting the systems and making patient data unusable. In 2020, ransomware attacks affected three hospitals, one each in the Czech Republic, the United States, and London. Boston Children's Hospital had the longest attack duration, lasting 14 days, while Champaign-Urbana Public Health District had the shortest, lasting only four days.

The table shows that the effects are harsh regardless of the attack strategies and tactics used by cybercriminals. Therefore, if cybersecurity was given top priority in the healthcare sector, system failures, reputational damage, and other related problems might be lessened.

Table II lists the methods that hackers use to attack the healthcare sector as well as the defenses used by hospitals to fend against and recover from attacks. All of these institutions, which were targets of various cyberattacks, including those at Boston Hospital, Lukas Hospital, Brno Hospital, and Hancock Hospital, followed the same course of action: they shut down their systems to limit the harm. The table demonstrates that hospitals did not have defined strategies or backup plans to deal with intrusions, demonstrating a disregard for cybersecurity. For instance, Brno Hospital continued to run Windows XP into 2020. This emphasizes how important it is for healthcare businesses to address cybersecurity and implement preventative steps to lessen and eliminate online dangers.

Information on the ransom payments made by hospitals to hackers to recover access to their systems is shown in Table III. In comparison to attempting to restore compromised information technology systems without the decryption key needed to remove the infection, paying the ransom may be less detrimental to operations and profit margins. Boston Hospital spent the most to restore its systems, close to $600,000, and Champaign-Urbana Public Health District spent the second-most, $350,000. The least amount was paid by Hollywood Presbyterian Medical, at $17,000. Although paying a ransom may incur financial costs, it is preferable to endangering lives, tarnishing one's image, or disclosing private information. Hospitals should put patients' safety first, even if doing so would inspire hackers to undertake additional cyberattacks. It is crucial that hospitals.

Fig. 2 illustrates how cyberattacks are divided into three distinct attack categories.

1) Injection attack: A web application may be "injected" with malicious data by an attacker, affecting the way it operates by directing it to execute certain commands. Injection is one of the early varieties of web-based attacks. Malware is an illustration of an injection attack. According to [6], malware is any computer code written with the purpose of gaining unauthorized access to digital devices and IT infrastructures. This is done by breaching the security measures protecting them and taking advantage of security flaws. Three distinct malware subtypes were discernible:

a) SamSam: Initially appearing in late 2015, a ransomware malware, primarily targets the healthcare sector. SamSam specializes in using RDP, FTP, and Java-based web server vulnerabilities to access the victims' machines [7].

b) Locky: It is a ransomware family that uses a hybrid cryptosystem and was launched in 2016. Its mechanism of operation involves scanning the victim's drives, such as network drives, for particular file types to encrypt them using RSA and AES [8].

c) Netwalker: Also known as Mailto, is a type of attack where the attacker uses the victim's network to encrypt all Windows-based devices. The attacker can use either phishing emails or executable files that travel throughout networks to carry out his attack [9].

TABLE I. EXAMPLE OF HOSPITALS EXPOSED TO CYBER-ATTACKS

Targeted system/ Region, Year	**Cyber Attack Category**	**Result**	**Source**
Boston Children's Hospital/ Boston, 2014	DDoS	For a period of two weeks, the hospital's network was inactive, seriously disrupting everyday operations and leading to the closure of the fundraising website.	[21]
Lukas Hospital/ Germany, 2016	Social engineering & Malware	High-risk surgeries were postponed by the hospital while they evaluated and sanitized their infected servers and computer systems.	[19] & [21]
Hancock regional hospital/ United States, 2018	Malware (SamSam)	The backup files are permanently destroyed.	[19]
Hollywood Presbyterian Medical Center/ Los Angeles, 2016	Malware (Locky) & phishing	Staff employees were unable to access patient information, X-rays, and other devices during the attack and were unable to use backup systems to restore the data.	[22]
Champaign-Urbana Public Health District/ United States, 2020	Malware (NetWalker)	In order to provide updates on COVID-19, the organization blocked its website and used its Facebook page instead.	[27]
Brno University Hospital/ Czech Republic, 2020	Ransomware	The hospital's IT network was completely shut down as a result of a significant service disruption, preventing personnel from accessing patient records, X-rays, and other devices. Handwritten notes and transfer procedures had to be used by the hospital, which may have compromised patient safety and slowed down operations. Two further hospital departments had to be shut down as a result, including the motherhood department and the children's hospital.	[17]
Hammersmith Medicines Study/ London, 2020	Ransomware	Birth dates, insurance numbers, and passport information were among the many private details stolen from patient records.	[17]

TABLE II. METHODS OF CYBER-ATTACK ON HOSPITALS AND RESPONSES TO CYBERATTACKS

Hospital	**Attack method**	**Response**	**Source**
Boston Children's Hospital	The hospital network was targeted by hackers who attempted to breach it by focusing on "exposed ports and services," as well as launching a phishing email campaign that specifically targeted hospital employees.	The hospital took the measure of stopping all web-facing programs, including email services, to effectively close all firewall entry points and prevent staff members from accidentally clicking on a malicious link.	[18]
Lukas Hospital	Technique for social engineering	All systems have been turned off. Backups were used to restore systems.	[19] & [20]
Hancock regional hospital	The hackers utilized the Microsoft Remote Desktop Protocol to infiltrate the administrative account of a hardware vendor.	Turn off all desktop and network systems.	[19]
Hollywood Presbyterian Medical	NAN	Pay a ransom	[20]
Champaign-Urbana Public Health District	NAN	Employees exchanged information using their systems and networks.	[23]
Brno University Hospital	Exploiting vulnerability in the WindowsXP operating system.	Shut down the entire information technology network	[17]
Hammersmith Medicines Study	Use of the ransomware-as-a-service model.	NAN	[17]

TABLE III. AMOUNTS PAID BY HOSPITALS TO RESTORE THEIR SYSTEMS

Hospital	**Financial Cost**	**Source**
Boston Children's Hospital	$300,000 - $600,000	[18] & [24]
Hancock regional Hospital	$50,000	[25]
Hollywood Presbyterian Medical	$17,000	[20]
Champaign-Urbana Public Health District	$350,000	[26]
Hammersmith Medicines Study	No ransom was paid	[17] & [27]

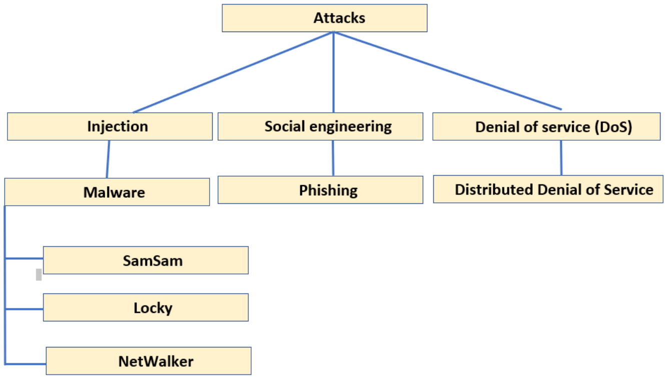

Fig. 2. Cybersecurity attacks classification.

2) Social engineering: It is a method where an attacker uses interpersonal interactions to prey on psychological flaws in the victim to persuade them to divulge critical information to the attacker [10]. Phishing is a type of social engineering that hackers employ to trick their victims into divulging sensitive information like usernames, passwords, bank account details, etc. This is accomplished by tricking the user into clicking on a link to a false website or downloading a malicious program.

3) Denial of service attack: It is a type of cyberattack that mostly focuses on consuming resources, including memory or computing power. Both wireless and cable connections can be used to carry out this assault [11]. A particular kind of DoS assault that targets websites is known as a distributed denial-of-service attack. To assault a single victim, an attacker uses malicious script that has been placed on several other computers. The website is intended to become inoperable [12].

III. Mitigation Strategies

As indicated in Fig. 3, we will cover risk classifications and the most recent techniques hospitals can use to lessen the effects of cyberattacks in this section.

According to [13], risk is the potential for loss or harm if an attacker exploits a security hole. An operational risk associated with online activities that threatens information assets, resources for information and communication technology, and technological assets and may cause material damage to an organization's tangible and intangible assets, business interruption, or reputational harm is another comprehensive definition of cybersecurity risk [14]. Risk reduction and risk avoidance are two alternatives provided by risk mitigation strategies. Preventative measures are used in mitigation strategies to lessen the possibility or impact of a cyberattack. These tactics are focused on locating and addressing any weak spots and security risks in the organization's rules and information. Risk-mitigation measures can include putting in place infiltration detection systems and protection barriers, as well as updating software and hardware often and training staff on best practices for cyber security.

A. A Proactive Incident Response (IR)

Planning and preparation, detection, analysis, and evaluation, containment and eradication, recovery, and post-incident activities are the six steps that make up this procedure. The firm must first establish its security policy and incident response capability. This involves putting together a team to manage incidents and acquiring the necessary tools and supplies. In the second stage, an event is automatically detected using tools like network- or host-based intrusion detection systems or manually using manual requirements like alerting users to problems. In the third stage following the incident, the incident response team analyzes and verifies the incident. Implementation of containment strategies, such as sandboxing, occurs in the fourth stage. In stage five, the administrator will check that the systems are operating normally and correct any issues to prevent future occurrences. After an incident, a meeting should be held as the final step. The purpose of this meeting is to advance technology and gain knowledge [15].

B. Secure Architecture based on Blockchain Technology and Artificial Intelligence

Five layers make up the suggested architecture for a safe system based on artificial intelligence and blockchain technology. The first layer, referred to as the "data layer, gathers information from patient sensors, including temperature and heartbeat. Additionally, malware samples are gathered in this layer and sent to the malware analysis layer. Tools like Pestudio and Process Explorer are used in the second layer, known as malware analysis, to examine the malware. The second layer's harmless samples are included in the third layer's intelligence, which checks them for security flaws using artificial intelligence techniques like support vector machines (SVM) and random forests (RF). Data transferred from Layer 3 is safely stored in Layer 4, the Blockchain layer. Hospitals, pharmacies, laboratories, and ambulances are examples of healthcare data recipients at the applications layer (layer three) [16].

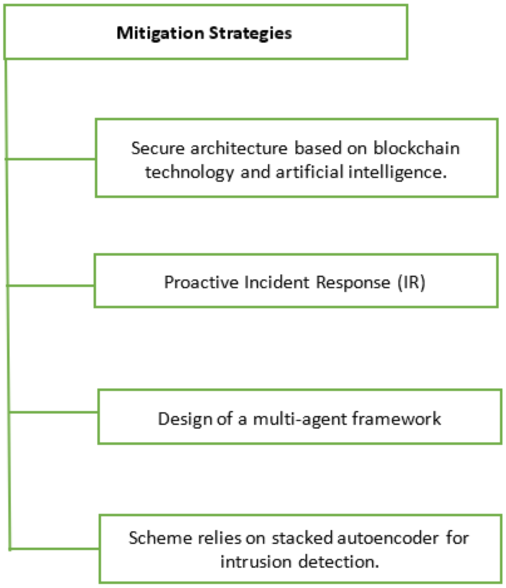
Mitigation Strategies
Secure architecture based on blockchain technology and artificial intelligence.
Proactive Incident Response (IR)
Design of a multi-agent framework
Scheme relies on stacked autoencoder for intrusion detection.

Fig. 3. Proposed strategies to mitigate cyber-attacks.

C. Design of a Multi-Agent Framework

The framework is created in two steps. First, five system agents need to be made. Patient, nurse, doctor, ambient, and database agents. The next step is to provide a tiered architecture that classifies agents according to their data storage and power capabilities. The wireless sensor network platform was utilized in this framework [16].

D. Scheme Relies on Stacked Autoencoder for Intrusion Detection

Scheme's framework for intrusion detection uses stacked autoencoders. Data pre-processing, feature extraction, and intrusion behavior determination make up the method' three steps. Infiltration behavior is defined at the Data Pre-Processing phase. A stacked autoencoder is used in the feature extraction stage to get parameter weights for various features. The XGBoost algorithm is used in the Intrusion Behavior Determination stage to determine if a behavior is normal or intrusive.

IV. Results and Discussion

As healthcare companies become more popular targets for hackers, cyberattacks against hospitals are on the rise, according to the evaluation of scholarly articles done for this research paper. Because of its outmoded practices, weak security measures, and sensitive data, the healthcare sector is a prime target for hackers. These attacks can have serious effects, including harm to patients, harm to the reputation of healthcare organizations, and monetary losses.

The study also outlines a number of research papers' protection against cyberattacks and solutions that healthcare institutions might use. These tactics comprise staff training, routine system updates, and the application of cutting-edge security tools like intrusion detection systems and firewalls. According to the study, hospitals should prioritize cybersecurity and have detailed strategies and backup plans to deal with intrusions.

Hospitals are vulnerable to attacks because of insufficient security standards, according to the assessment of scholarly studies. The majority of healthcare firms do not have a thorough security strategy, which shows a disregard for cybersecurity. The study recommends that healthcare institutions take proactive steps to safeguard sensitive patient data and lessen the effects of system errors, reputational damage, and other related problems.

V. Conclusions and Future Works

This study concludes by emphasizing the urgent necessity for healthcare institutions to address cybersecurity in order to prevent data breaches that could jeopardize patient information. Hospital cyberattacks can have serious repercussions, so healthcare companies need to create clear policies and backup plans to cope with these situations. The report provides a summary of hospital cyberattacks from 2014 through 2020, including ransomware assaults, and offers many tactics hospitals might employ to lessen or prevent a hack.

Future studies can concentrate on creating innovative techniques and tools to defend healthcare companies against cyberattacks. For instance, research may look into how to employ machine learning and artificial intelligence to detect and stop cyberattacks on hospitals. Additionally, studies might look into how cyberattacks affect patient security and consider the moral ramifications of data breaches in the healthcare sector.

Overall, the importance of cybersecurity in the healthcare sector is highlighted in this research study, and healthcare companies must take proactive steps to safeguard sensitive patient data. Healthcare institutions must emphasize cybersecurity given the increase in cyberattacks on hospitals in order to limit losses from system failures, reputational damage, and other associated problems.

Acknowledgment

The author wishes to express her deep appreciation and respect to Salahaldin M.A. Abuabdou for inspiring and motivating her to write this paper.

References

[1] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

[2] Healthcare Information and Management Systems Society, "2021 HIMSS Healthcare Cybersecurity Survey Report," 2022. [Online]. Available: https://www.himss.org/resources/2021-himss-healthcare-cybersecurity-survey-report. [Accessed: 18-Apr-2023].

[3] M. O'Brien, "Ireland’s Health Service Executive hit by ransomware attack," The Guardian, 14 May 2021. [Online]. Available: https://www.theguardian.com/world/2021/may/14/irelands-health-service-executive-hit-by-ransomware-attack. [Accessed: 18-Apr-2023].

[4] A. Osborn, "NHS cyber-attack: GPs and hospitals hit by ransomware," BBC News, 12 May 2017. [Online]. Available: https://www.bbc.com/news/health-39899646. [Accessed: 18-Apr-2023].

[5] Ponemon Institute, "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data," 2016. [Online]. Available: https://www.ponemon.org/library/2016-ponemon-institute-benchmark-study-on-privacy-security-of-healthcare-data. [Accessed: 18-Apr-2023].

[6] M. Ashawa and T. Morris, "Understanding and Mitigating Malware Attacks," in Proceedings of the 11th International Conference on Cyber Warfare and Security (ICCWS 2019), vol. 1, pp. 1-10, 2019.

[7] V. Arora, A. Varshney, A. Arora, and N. Shukla, "Assessment of SamSam Ransomware Attack on Healthcare Sector and Way Forward," Journal of Information Privacy and Security, vol. 15, no. 1, pp. 1-12, 2019.

[8] S. Almashhadani, T. Almarshad, and A. Al-Salman, "Ransomware: The Past, Present, and Future," in Proceedings of the 3rd International Conference on Computer Applications & Information Security (ICCAIS 2019), vol. 1, pp. 1-6, 2019.

[9] Gómez-Hernández, J. A., García-Teodoro, P., & Díaz-Verdejo, J. E. (2022). Analysis of Netwalker Ransomware: Detection, Prevention and Recovery. Computers & Security, 106, 102556.

[10] W. Wang, Y. Zeng, X. Zhang, X. Xu, Y. Xiang and X. Shen, "A Survey on Social Engineering Attacks and Defenses in Online Social Networks," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1342-1372, Secondquarter 2020, doi: 10.1109/COMST.2020.2974247.

[11] Singh, R., Singh, S., & Saini, D. (2019). Denial of Service Attacks: Impact, Detection, and Mitigation Techniques. Journal of Network and Computer Applications, 135, 62-80. https://doi.org/10.1016/j.jnca.2019.02.015.

[12] Singh, A., Kumar, A., & Tyagi, S. (2020). A Comparative Analysis of Detection and Mitigation Techniques against Distributed Denial of Service Attacks. In Proceedings of the International Conference on Smart Technologies in Computing and Communication (pp. 259-269).

Springer.

[13] Kandasamy, P., Perumal, M., & Naresh, R. (2022). Cybersecurity Risks and Their Mitigation Strategies for Healthcare Industry. In Cybersecurity and Privacy Issues in Industry 4.0 (pp. 19-37). Springer, Singapore.

[14] Strupczewski, A. (2021). Cybersecurity Risk Management in the Healthcare Industry. In Handbook of Research on Information Security and Cyber Threats in the Fourth Industrial Revolution (pp. 103-116). IGI Global.

[15] Y. He, X. Lu, Y. Yao, W. Zhang and W. Tang, "A Cyber Security Incident Response System with Automated Forensics and Orchestration," in IEEE Access, vol. 10, pp. 113773-113786, 2022, doi: 10.1109/ACCESS.2022.3140703.

[16] Alabdulatif, A., Ahmad, A., Khan, M. K., Azeem, A., Al-Khateeb, A., & Al-Salman, A. (2022). A secure architecture based on blockchain technology and artificial intelligence for healthcare applications. Future Generation Computer Systems, 127, 487-495. https://doi.org/10.1016/j.future.2021.09.0.

[17] Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A., & Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic. Journal of Advanced Transportation, 2021, 1–19. doi: 10.1155/2021/6627264.

[18] Wilner, A. S., Luce, H., Ouellet, E., Williams, O., & Costa, N. (2021). From public health to cyber hygiene: Cybersecurity and Canada’s healthcare sector. International Journal: Canada’s Journal of Global Policy Analysis, 76(4), 522–543. doi: 10.1177/00207020211067946.

[19] 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), 146. doi: 10.1186/s12911-020-01161-7.

[20] Paul III, D. P., Spence, N., Bhardwa, N., & PH, C. D. (2018). Healthcare facilities: another target for ransomware attacks.

[21] Cox, J. (2018, January 19). The Cyber Attack—From the POV of the CEO. Hancock Regional Hospital. https://www.hancockregionalhospital.org/2018/01/cyber-attack-pov-ceo/

[22] Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52. doi: 10.1016/j.maturitas.2018.04.008.

[23] Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K.-K. R., & Al-Qirim, N. (2022). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. Digital Communications and Networks, S2352864822001274. doi: 10.1016/j.dcan.2022.06.005.

[24] Ghayoomi, H., Laskey, K., Miller-Hooks, E., Hooks, C., & Tariverdi, M. (2021). Assessing resilience of hospitals to cyberattack. DIGITAL HEALTH, 7, 205520762110593. https://doi.org/10.1177/20552076211059366.

[25] Burrell, D. N., Aridi, A. S., McLester, Q., Shufutinsky, A., Nobles, C., Dawson, M., & Muller, S. R. (2021). Exploring System Thinking Leadership Approaches to the Healthcare Cybersecurity Environment. International Journal of Extreme Automation and Connectivity in Healthcare (IJEACH), 3(2), 20–32. https://doi.org/10.4018/IJEACH.2021070103.

[26] Strasburg, J., & Hinshaw, D. (2020). Cybercriminals Sweep In to Take Advantage of Coronavirus. The Wall Street Journal, 24.

[27] Mahadevan, P. (2020). Cybercrime Threats during the COVID-19 pandemic. Global Initiative Against Transnational Organized Crime, Switzerlan.