Telecom Business Review
16 (1) 2023, 51-58
http://publishingindia.com/tbr/

Cyber Risk and Mitigation Associated with Healthcare Industry

Ankit Anand*, Irina Leonova**

*Technology Consultant, EY. Email: anandankit842@gmail.com

** Faculty of Social Sciences, Lobachevsky University, 603950 Nizhny Novgorod, Russia. Email: irina_leonova@list.ru

***Abstract*—**Incidences of cyber fraud are increasing in multiple industrial sectors making cybersecurity a prime area of concern. In certain industries such as healthcare, the concern becomes stronger as it is directly related to our health and well-being. The expansion of portable gadgets like smartphones and USB devices, as well as the enormous number of connected medical devices, are widening the attack surface. With the advancement in the cyber world on the daily basis, the risk in the healthcare industry has not been explored much. Hence, this research paper talks about some of the security concerns, their effects, applications, and risk-reduction strategies related to the healthcare sector. To attain the objectives, a qualitative approach has been adopted wherein various studies related to the cyber risk associated with the healthcare domain have been analyzed. The implications of this paper for designing and developing security solutions in the healthcare sector that will benefit society at large are discussed for security practitioners. By offering several remedies to the hazards that have been identified as being connected to the cyber world in the healthcare industry, this study adds to the body of literature.

***Keywords*—**Cybersecurity, Risk, Healthcare, Cyber Mitigation

I. INTRODUCTION

A. Background

In today's era, organizations need an action plan way before the risk becomes a threat, given that attackers are constantly seeking the weakest link in a system's defense, security measures can give organizations a way to assess and comprehend the system's security status (Coventry & Branley, 2018). The healthcare industry has experienced an increase in security breaches in recent years. According to a Verizon data study, 85% of malware that targets the medical industry is ransomware, and the frequency of breaches in this industry has increased dramatically from the previous year.

B. Objective

Due to the quantity and frequency of personal data archived and stored along with crumbling architecture, especially in community clinics, along with the complexities imposed by the high endpoint count, the healthcare sector faces some distinct issues (Jalali & Kaiser, 2018). The healthcare sector should strengthen its security measures to protect its priceless assets because it is generally less secure than other sectors (Kruse et al., 2017). Security metrics can be used to compare an organization's performance to that of its competitors in the market and notify stakeholders of observations and patterns within the organization (Savola et al., 2015). The risk in the healthcare sector hasn't been extensively studied despite everyday advances in the cyber world. So, this research study discusses several security challenges relating to the healthcare sector, their effects, use cases, and mitigation strategies for the risk factor. Addressing these cybersecurity challenges is crucial in the healthcare sector, especially considering the rapid shift to a digital business model where organizations need to adapt a new approach to risk management and security practices (Dutta, 2020).

There are two ramifications for the study's findings. At first it places a focus on awareness of the cyber risk related to the healthcare sector. However, it also points out the gap and vulnerable areas that need to be filled and, as a result, future study directions. The demand for healthcare is not adequately addressed by studies on healthcare facilities. To address the issue of managing risk exposures within the medical industry, there aren't enough study

resources in this field. This paper has been arranged in the below format: - i) Section I: Introduction, ii) Section II: Literature Review, iii) Section III: Research Questions and Framework, v) Section IV: Result and Analysis, v) Section V: Discussion, vi) Section VI: Limitation of Study and Future Area, vii) Section VII: Conclusion.

II. LITERATURE REVIEW

Attacks on medical devices, services, and infrastructure that could jeopardize patient safety are the biggest threat to the healthcare industry (Perakslis, 2014). Healthcare providers must ensure accessibility and consistency in their services, but hackers are always searching for ways to breach systems and pose a threat to these attributes. The value of the personal data held by the healthcare sector and the ease with which the subject can be accessed attract hackers (Martin et al., 2017).

Healthcare cybersecurity problems are not completely unique, but they have grown prevalent especially with the development of medical AI research in radiology and have been named to be among the biggest hazards to the industry in 2021. Findings have suggested general strategies for enhancing security through both detection and prevention tactics, as well as ways that technology might boost security while reducing risks (Kelly et al., 2023). Most of the known vulnerabilities that threaten the healthcare industry also affect other sectors, but because patient safety is at stake, the impact of a compromise is much greater. When it comes to the security, reliability, and accessibility of confidential documents, few authors have identified certain security assaults that are directed towards healthcare systems (Priya et al., 2018). The impact of emerging telecom communication standards like 5G on healthcare, as discussed in 'Revolutionizing Healthcare With 5G' (Gupta & Ghosh, 2019), presents additional considerations for cybersecurity and risk mitigation in the healthcare industry.

In order to comprehend the nature of cyber-attacks against the healthcare industry, few researchers have used a modern hospital ecosphere as a scenario for the Iot and smart security risk identification, with a focus on first recognizing the threats that harm the health sector, why they did so, and how they carry out the operations (Jimo, Abdullah & Jamal, 2023).

Also, recommendations for technical and non-technical actions that would aid in securing and ensuring privacy throughout the healthcare sector using IoE systems are made using the findings from the DREAD threat model.

The information, network, and storage gathering phase are the three phases the investigators describe security breaches. There are many wireless devices attached to healthcare systems, but while these tools support clinicians and other healthcare providers in providing successful quality of healthcare, they also widen the attack surface ("Securing Wi-Fi Access for Healthcare," 2023). Cybersecurity education for all staff in healthcare organizations must be improved using online resources, simulation, and gaming to provide insights into the scope of cyberattacks and their influence on staff welfare. Together with recommendations for future policy and practice, (Niki et al., 2022) have outlined the role that national educators, policymakers, and multilateral organizations had in accomplishing this goal.

Ransomware is a class of software that is commonly referred to as a modern-day type of blackmail that encrypts user data in order to extort payment as stated (Mago & Fransisco Madyira, 2018; Mansfield-Devine, 2016). Ransomware has become one of the most prevalent types of assaults towards the medic sector in the last few years. Attacks like WannaCry is one such example of ransomware attack that used SMB vulnerability (Server Message Block). Due to its simplicity of usage, portability of ransomware kits, and distributed currency as ransomware, Bitcoin has become increasingly popular among hackers (Brewer, 2016; Al-rimy et al., 2018). Below are the parameters because of which the healthcare system has been prone to data and security breaches:

A. Ancient Architecture

It is well known that medic companies, in particular community hospitals, use outdated infrastructure that are vulnerable to cyberattacks. Organizations must have a plan of action to preserve business workflow if their critical services are compromised due to cyberattacks since the threat landscape is always altering (Padmanabhan, 2017). Due to the enormous amount of sensitive data that health institutions store, privacy and security are key issues (Zackery et al., 2022). Numerous research papers have proposed the deployment of cloud computing in the medical industry as a means of mitigating the critical issues brought on by aging facilities. Nevertheless, some organizations are reticent to embrace the cloud model due to security and privacy concerns raised by cloud services (Bamiah et al., 2012; Iyengar et al., 2018; Sahi et al., 2018; Liu et al., 2017).

B. Medical Instruments

Nowadays, formerly unconnected medical gadgets are online to facilitate medic data sharing and speed up the delivery of results. These medical gadgets will undoubtedly also increase the attack surface and create Network vulnerabilities (Williams & Woodward, 2015). Diagnostic gadgets are now networked to servers, allowing doctors to rapidly transmit data on findings like scanning reports. Malware may, meanwhile, spread through one infected machine into another as a function of this, it can probably reach the wider medical servers. Attackers might use susceptible medical equipment as an initial point when attacking the hospital system (Schwartz et al., 2018).

C. Security Pattern

Effective security skilling is generally considered to be among the finest intrusion detection systems due to the fact that individuals are susceptible to social manipulation that may therefore turn into the fragile link on a system for intruders to access. Passcode disclosure was found to be prevalent in the medical industry as a result of doctors and other healthcare professionals' frequent motivation to provide exceptional care to patients and their potential to view access controls like secure passcode as a barrier instead of as a safety precaution (Koppel et al., 2015).

D. Compliance with Legal and Regulatory Committees

To protect the data they store, hospital management must make sure the proper security procedures are in place, which limit access to only those who are authorized.

E. Security Measures

Researchers are more interested in security metrics as a technique to quantify security measures that advocates indecision-making. In a recent analysis by Thycotic, the majority of enterprises lack cybersecurity measures, making it challenging to access and monitor the effectiveness of their security measures. Several researchers have published several articles & papers on security metrics, yet they were predominantly operational aspect focused and did not take into account the environment of medical Informatics infrastructure (Campbell, 2014; Jansen, 2009).

The security measures that might be used to address the cybersecurity issues outlined are presented in the following subsections, along with an explanation of how the use of these measurements could help in safety enhancement of IT infrastructures.

1) IOC

Data that could be used to identify fraudulent behavior which has taken place on a network or system is known as an indicator of compromise (Sainz, 2019). The knowledge gained from these security lapses can be applied to stop such assaults whenever such a situation arises. Companies can benefit from detecting symptoms of intrusion that can aid in promptly identifying occurrences that the monitoring systems may have missed.

2) IOA (Indicators of Attack)

Latitudinally moving could indicate that an intruder has infiltrated the system and is progressing through susceptible sites until they achieve their goal, according to the Indicator of Attack (IOA) (Purvine et al., 2016). A significant increase in bandwidth and incoming traffic may signal a Distributed Denial of Service (DDoS) attack or data espionage (Kiruthika Devi et al., 2012). The presence of numerous hosts interacting on non-standard ports with external networks suggests that sophisticated attackers are attempting to conceal their activities.

3) Penetration Testing

Due to the inherent expenditures, organizations typically conduct penetration assessments every two years or every quarter, but the threat landscape can swiftly shift and render such tests obsolete. Companies have created more recent penetration testing tools that work within the network to close this gap.

4) VAPT Testing (Red and Blue Team)

In the optimization phases following the deployment of new security programmes, Network penetration and vulnerability analysis could also be utilized. Businesses can increase the efficiency of their security procedures by implementing safety measures to assess whether they are applying the results of assessments and evaluations.

The cyber-risks to the healthcare sector are addressed in this research paper, along with potential countermeasures for Healthcare Technology systems. It also highlights a quick review of security measurements after analyzing cyber-attacks' impact. The suggested indicators may also be employed in other areas to enhance the system's safety. Due to the vulnerability of cyberattacks, assaults posed

to patients' security should be thoroughly monitored. Implementing appropriate mitigation measures will help IT security if these indicators are measured appropriately.

III. RESEARCH METHODOLOGY

A thorough investigation was carried out using the search terms "Cyber Risk or Healthcare" and "Cyber OR Risk OR Security'' and "Cyber OR Security OR Healthcare" and "Industry OR Risk OR Healthcare OR Assessment," among others, on Web of Science, Google Scholar, Scopus, and ScienceDirect (Risk Assessment OR vulnerability Assessment OR Healthcare OR Assessment). Publications, reports, press journals, whitepapers, and other web databases were used to collect the information for this research. The contextual significance of the compiled literature was also considered. The goal of this paper is to categorize the metrics that can be used to classify security challenges, cyber risks in the healthcare sector and spread awareness on the measures one can adopt in strengthening the defense procedures and inculcating hyperactive culture of information security among these organizations. The lack of focus the scientific community has given the issue of cyber risk in the health industry is highlighted in this research. It emphasizes the necessity of additional research into the exploratory research of risk associated with cyber, particularly with relation to specific categories and subcategories of functional data breaches.

Day by day, the amount of medics and doctors that require data access about their patients has increased drastically. To deliver high-quality patient care and prevent duplication, the necessity for network devices in the healthcare ecosystem has become a must. While connecting these systems has several advantages, it also brings problems in the aspect of the security of the CIA triad of the data (Smith, 2018).

The paper proposes to address the following research questions:

- What are various cyber-risks affecting the healthcare industry?
- How is the healthcare industry impacted by cyber risks?
- What are the measures and solutions to address these cyber risks?

IV. RESULT AND ANALYSIS

Use In this section, we have analyzed four major challenges – cyberattacks that the healthcare domain has been facing. Later we also discussed the use cases to avoid these.

A. Phishing

Phishing is the practice of placing dangerous URLs within emails that appear to be normal but are actually malicious. To urge recipients to open the links, these emails frequently make references to recognized medical conditions.

1) Use Cases

CEO Fraud is one example of phishing which exploits the name of the corporation's CEO by deceiving staff to provide personal data or execute fund transfers. At Upsher-Smith Laboratories, the hackers immediately forced the supervisor to wire $50 million across nine accounts toward the "CEO's accounts"-those accounts belonged to the hackers (Kirda & Kruegel, 2005).

2) Impact

It was discovered that the bank account belonged to the hackers. Despite the operation being terminated at $39 million, the damages had already been done. Indeed, the business was unable to recoup the funds.

3) Solution

Phishing may be avoided if the organization has clear guidelines and adequate cyber awareness. Any URLs must be closely examined by people to make sure they don't lead to any strange or suspicious domains. Additionally, people must be cautious of impersonal welcomes, foul language, and misspelled terms (Roy & Debbarma, 2020).

B. Attacks by Ransomware

During a ransomware attack, malware is injected into the networks to infect and conceal personal information unless a ransom fee is paid. Its prominence is caused by hackers' understanding of how crucial it is for the medical industry to prevent operational challenges.

1) Use Cases

An instance of a ransomware assault is called SamSam (Falco et al., 2018) that secretly snoops for a long period after being infected. SamSam targets particular organizations by exploiting their weaknesses. After SamSam eliminates or makes it impossible for the victim to access his own data, the ransomware's developers demand a ransom.

2) Impact

SamSam was allegedly used by two Iranian cybercriminals targeting more than 200 businesses and organizations in Canada, including hospitals, local governments, and governmental authorities. The assaults are believed to have cost USD 30 million.

3) Solution

With sandboxing, advanced multilayered protection against the full range of email-borne threats is provided by a secure email gateway solution. A web application firewall (WAF) helps to secure online applications by screening and monitoring HTTP traffic to and from a web service. A vital element of security, it acts as the initial line of defense against cyberattacks (Jamil et al., 2019; Roy & Debbarma, 2020).

C. DDoS Attacks

This attack involves flooding a targeted network with fraudulent sync packets in an effort to take it offline. A significant number of endpoints and IOT devices that have been coerced into joining a botnet via malware infection are used in this planned attack.

1) Use Cases

The 2015 GitHub Attack (Bhattacharjee et al., 2019) was one of the largest DDoS attacks that exploited GitHub, an online software configuration management site used by millions of developers. Botnets were not used in the GitHub attack because server DDoS was employed. Rather, the attackers capitalised on the amplifying effect of the client-side database caching system.

2) Impact

For several days, this politically motivated attack continued. With a latency of 20 minutes and a throughput of 1.35 terabits/second, this DDoS attack prevented the majority of prime users from accessing the website. More than 35k repositories were compromised. Two GitHub projects that were attempting to circumvent Chinese government censorship were the target of the DDoS attack, which originated in China. It's thought that the attack was intended to put pressure on GitHub to stop supporting these kinds of projects.

3) Solution

Network security must be maintained in order to thwart any DDoS attack attempt. Controlling the maximum range requires the ability to identify a DDoS quickly because an attack only affects the maximum range if the hacker has enough time to gather requests. To protect businesses against DDoS attacks, one can rely on network security measures like firewalls and intrusion detection systems, antivirus and anti-malware software, endpoint security, web security tools, and network segmentation protocols (Roy & Debbarma, 2020).

D. Data Breaches

The Medical Industry has a high proportion of security breaches (Joseph, 2018). According to reports, there were 1.76 safety incursions per day on an average in the healthcare sector in 2020.

1) Use Cases

A cyber-attack was reported by Norwood Clinic ("The 10 biggest cyberattacks in healthcare in the 1st quarter of 2022," 2022) in Alabama wherein the attacker got access to database that stored details of patient like their SSN-Social Security Number, birthdates however it did not include any financial data which may include debit or credit card numbers.

2) Impact

The healthcare organization based in Alabama acknowledged that 228,000-patient data was compromised in this cyber-attack. In response, Norwood Clinic hired cybersecurity professionals to examine its servers and has been working to strengthen its data security. Credit monitoring and identity theft protection was also offered by the Clinic.

3) Solution

Risk and gap analyses should be done on current infrastructure to provide security rankings (Jamil et al., 2019). Also, Healthcare stakeholders such as security personnel should work in tandem to improve the security stances of all service providers. Briefings or the use of free cybersecurity materials can be used to enhance cyber awareness training. The other solution can be implementation of Multi-Factor Authentication which is one of the simplest controls enough to prevent an attack.

V. DISCUSSION

To find the major challenges faced by the Healthcare Industry, we have researched reports and news articles from 2000 to 2023. We have also referred to the reports

published by various companies like Center for Internet Security, working on resolving malware attacks in and around the world.

According to a recent survey, global cybercrime rose by 38% for 2022 compared to 2021, with India's healthcare system being one of the most frequently attacked. These attack statistics, as per CheckPoint Research (CPR) (Global cyberattacks rise, 2023) were fueled by lesser, more nimble attackers and malware groups, who concentrated on attacking collaborative technologies used in work-from-home environments, attacking educational institutions who transitioned to e-learning after COVID-19.

Given the potential impact of cyberattacks on healthcare, it is crucial to study this issue to better understand the threat's nature and develop strategies for prevention and response. Thus, this research helps develop more effective security measures and raise awareness among healthcare providers and the public about the importance of cybersecurity in healthcare.

VI. IMPLICATIONS

The objective of the research study is to focus on security issues associated with the healthcare industry, its impact, use cases and solutions to mitigate the risk factor. This study is useful to the healthcare institutions to get awareness on various risk factors while they implement security solutions. This article promotes various stakeholders such as security personnel and management team to work in tandem to provide the best security solution to their patients.

VII. LIMITATIONS AND FUTURE RELEVANCE

The study's major limitation is its focus on only documents that contained the keyword "health," which could have unnecessarily constrained the range. But we chose this keyword approach to better understand the present level of cyber risk in the healthcare sector, especially during the epidemic. The weakness of this research may also be its strength.

This assessment criterion identifies information gaps in the healthcare industry and offers opportunities for further investigation into data breaches. Researchers could start by reading up on data breaches in all other sectors and putting the most efficient procedures into practice in healthcare institutions. Furthermore, it encourages creative organizational solutions utilizing the knowledge of professionals and consultants.

VIII. CONCLUSION

This research paper explores the security concerns & vulnerabilities that the healthcare industry is currently facing and has also listed a few reasons why it is vulnerable to cyberattacks. Healthcare is not the only domain affected by cyberattacks, but because patient safety and privacy are at stake, the impact is immense. Cyberattacks in healthcare can have significant consequences for individuals, organizations, and society as a whole. Cyberattacks can result in the theft or alteration of patient data, which can lead to serious harm for patients. It can cause healthcare providers to lose access to critical systems and data, which can disrupt patient care. It can expose sensitive patient information, which can violate patient privacy and lead to a loss of trust in healthcare providers.

There was discussion of the culture of security to be implemented, ancient architectural patterns followed by the healthcare institution, and medical equipment vulnerabilities. We have also discussed recent examples of cyberattacks that have caused hefty loss such as Phishing, ransomware, data breaches and DDos Attack. We have also divided the parameters into eight groups so that decision-makers can calculate the security of the systems and make well-informed decisions.

To strengthen the integrity of these systems, a cybersecurity parameter suggestion was produced, Penetration testing, IOC, VAPT teaming (Red & Blue), Risk analysis, IOA and Intelligence driven security were the metrics categories that grouped the parameters using were. In order to give a more comprehensive picture of the system security of information systems, which includes pharmaceutical products as well as other related systems, future research will measure and aggregate these indications.

REFERENCES

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144-166. doi:https://doi.org/10.1016/J.COSE.2018.01.001

Dutt, N. S. (2020). Building the next-gen cyber security operating model in a digital eco-system. *Telecom Business Review, 13*(1), 65-68. Retrieved from http://publishingindia.com/TBR/65/building-the-next-gen-

cyber-security-operating-model-in-a-digital-eco-system/10907/16252/

Gupta, P., & Ghosh, M. (2019). Revolutionizing healthcare with 5G. *Telecom Business Review, 12*(1), 41-45. doi:http://www.publishingindia.com/GetBrochure.aspx?query=UERGQnJvY2h1cmVzfC81NTc2LnBkZnwvNTU3Ni5wZGY=

Bamiah, M., Brohi, S., Chuprat, S., & Ab Manan, J. L. (2012). A study on significance of adopting cloud computing paradigm in healthcare sector. *Proceedings of 2012 International Conference on Cloud Computing Technologies, Applications and Management, ICCCTAM 2012*, 65-68. doi:https://doi.org/10.1109/ICCCTAM.2012.6488073

Horawalavithana, Bhattacharjee, A., Liu, R., Choudhury, N., Hall, L. O., & Iamnitchi, A. (2019). *Mentions of Security Vulnerabilities on Reddit, Twitter and GitHub* (pp. 200-207). doi:https://doi.org/10.1145/3350546.3352519

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security*, *2016*(9), 5-9. doi:https://doi.org/10.1016/S1353-4858(16)30086-1

Campbell, G. (2014). *Measures and metrics in corporate security* (pp. 1-145). Elseiver. doi:https://doi.org/10.1016/C2013-0-15979-X

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48-52. doi:https://doi.org/10.1016/J.MATURITAS.2018.04.008

Falco, G., Viswanathan, A., Caldera, C., & Shrobe, H. (2018). A Master Attack methodology for an AI-based automated attack planner for smart cities. *IEEE Access*, *6*, 48360-48373. doi:https://doi.org/10.1109/ACCESS.2018.2867556

Global Cyberattacks Rise 38% with Healthcare Most Targeted in India (2023, January 12). *Business Standard*. Retrieved from https://www.business-standard.com/article/technology/global-cyberattacks-rise-38-with-healthcare-most-targeted-in-india-report-123011200899_1.html

Iyengar, A., Kundu, A., & Pallis, G. (2018). Healthcare informatics and privacy. *IEEE Internet Computing*, *22*(2), 29-31. doi:https://doi.org/10.1109/MIC.2018.022021660

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5). doi:https://doi.org/10.2196/10059

Jamil, A., Asif, K., Ghulam, Z., Nazir, M. K., Mudassar Alam, S., & Ashraf, R. (2019). MPMPA: A mitigation and prevention model for social engineering based phishing attacks on Facebook. *Proceedings - 2018 IEEE International Conference on Big Data, Big Data 2018*, 5040-5048. doi:https://doi.org/10.1109/BIGDATA.2018.8622505

Jansen, W. (2009). Directions in Security Metrics Research. 15-16. *National Institute of Standards and Technology.* doi:https://doi.org/10.6028/NIST.IR.7564

Jimo, S., Abdullah, T., & Jamal, A. (2023). IoE security risk analysis in a modern hospital ecosystem. *Advanced Sciences and Technologies for Security Applications*, 451-467. doi:https://doi.org/10.1007/978-3-031-20160-8_26

Joseph, R. C. (2018). Data breaches: Public sector perspectives. *IT Professional*, *20*(4), 57-64. doi:https://doi.org/10.1109/MITP.2017.265105441

Kelly, B. S., Quinn, C., Belton, N., Lawlor, A., Killeen, R. P., & Burrell, J. (2023). Cybersecurity considerations for radiology departments involved with artificial intelligence. *European Radiology,* 213-231. doi:https://doi.org/10.1007/S00330-023-09860-1

Kirda, E., & Kruegel, C. (2005). Protecting users against phishing attacks with AntiPhish. *Proceedings - International Computer Software and Applications Conference*, *1*, 517-524. doi:https://doi.org/10.1109/COMPSAC.2005.126

Kiruthika Devi, B. S., Preetha, G., & Mercy Shalinie, S. (2012). DDoS detection using host-network based metrics and mitigation in experimental testbed. *International Conference on Recent Trends in Information Technology, ICRTIT*, 423-427. doi:https://doi.org/10.1109/ICRTIT.2012.6206744

Koppel, R., Smith, S., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: You want my password or a dead patient? *Itch*, *208*, 215-220. doi:https://doi.org/10.3233/978-1-61499-488-6-215

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care: Official Journal of the European Society for Engineering and Medicine*, *25*(1), 1-10. doi:https://doi.org/10.3233/THC-161263

Liu, W., Zhu, S. S., Mundie, T., & Krieger, U. (2017). Advanced block-chain architecture for e-health systems. *International Conference on E-Health Networking, Applications and Services*,

2017-December, 37-42. doi:https://doi.org/10.1109/HEALTHCOM.2017.8210847

Mago, M., & Fransisco Madyira, F. (2018). Ransomware software: Case of WannaCry. *International Research Journal of Advanced Engineering and Science*, *3*(1), 258-261. Retrieved from https://irjaes.com/wp-content/uploads/2020/10/IRJAES-V3N1P608Y18.pdf

Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8-17. doi:https://doi.org/10.1016/S1353-4858(16)30096-4

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we? *BMJ (Clinical Research Ed.)*, *358*. doi:https://doi.org/10.1136/BMJ.J3179

Niki, O., Saira, G., Arvind, S., & Mike, D. (2022). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *Digital Health*, *8*, 1-3. doi:https://doi.org/10.1177/20552076221104665

Perakslis, E. D. (2014). Cybersecurity in health care. *The New England Journal of Medicine*, *371*(5), 395–397. https://doi.org/10.1056/NEJMP1404358

Priya, R., Sivasankaran, S., Ravisasthiri, P., & Sivachandiran, S. (2018). A survey on security attacks in electronic healthcare systems. *Proceedings of the 2017 IEEE International Conference on Communication and Signal Processing, ICCSP 2017*, *2018-January*, 691-694. https://doi.org/10.1109/ICCSP.2017.8286448

Purvine, E., Johnson, J. R., & Lo, C. (2016). A graph-based impact metric for mitigating lateral movement cyber-attacks. *SafeConfig 2016 - Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Co-Located with CCS 2016*, 45-52. doi:https://doi.org/10.1145/2994475.2994476

Roy, S. D., & Debbarma, S. (2020). Detection and mitigation of cyber-attacks on AGC systems of low inertia power grid. *IEEE Systems Journal*, *14*(2), 2023-2031. doi:https://doi.org/10.1109/JSYST.2019.2943921

Sahi, M. A., Abbas, H., Saleem, K., Yang, X., Derhab, A., Orgun, M. A., Iqbal, W., Rashid, I., & Yaseen, A. (2018). Privacy preservation in e-Healthcare environments: state of the art and future directions. *IEEE Access*, *6*, 464-478. doi:https://doi.org/10.1109/ACCESS.2017.2767561

Sainz, I. (2019). Diseñar para divergencias y convergencias. Enfoques del DCG para los procesos de lectura por placer en la Red. *Exploraciones, Intercambios y Relaciones Entre El Diseño y La Tecnología*, 57-79. doi:https://doi.org/10.16/CSS/JQUERY.DATATABLES.MIN.CSS

Savola, R. M., Savolainen, P., Evesti, A., Abie, H., & Sihvonen, M. (2015). Risk-driven security metrics development for an e-health IoT application. *2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference*, 1-6. doi:https://doi.org/10.1109/ISSA.2015.7335061

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., Petrozzino, C., & Zuk, M. (2018). The evolving state of medical device cybersecurity. *Biomedical Instrumentation & Technology*, *52*(2), 103-111. doi:https://doi.org/10.2345/0899-8205-52.2.103

Securing Wi-Fi Access for Healthcare. (2023). Retrieved November 10, 2023, from https://www.fortinet.com/blog/industry-trends/securing-wi-fi-access-for-healthcare

Smith, C. (2018). Cybersecurity Implications in an Interconnected Healthcare System. *Frontiers of Health Services Management*, *35*(1), 37-40. doi:https://doi.org/10.1097/HAP.0000000000000039

The 10 biggest cyberattacks in healthcare in the 1st quarter of 2022. (2022). Retrieved November 10, 2023, from https://www.chiefhealthcareexecutive.com/view/the-10-biggest-healthcare-cybersecurity-attacks-in-the-1st-quarter-of-2022

Padmanabhan, P. (2017). The NHS ransomware event and security challenges for the U.S healthcare system. *CIO*. Retrieved November 10, 2023, from https://www.cio.com/article/229994/the-nhs-ransomware-event-and-security-challenges-for-the-u-s-healthcare-system.html

Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices (Auckland, N.Z.)*, *8*, 305. doi:https://doi.org/10.2147/MDER.S50048

Zackery, A., Zolfagharzadeh, M. M., & Hamidi, M. (2022). Policy Implications of the concept of technological catch-up for the management of healthcare sector in developing countries. *Journal of Health Management*, *25*(2), 144-155. doi:https://doi.org/10.1177/09720634221076964