Unravelling the Web of Issues and Challenges in Healthcare Cybersecurity for a Secure Tomorrow

Aisyah Muhd Azri Baptist

Faculty of Accountancy, Universiti Teknologi MARA, Selangor Branch

Puncak Alam Campus, Malaysia

Farhanah Abdul Halim

Faculty of Accountancy, Universiti Teknologi MARA, Selangor Branch

Puncak Alam Campus, Malaysia

Siti Fatimah Abdillah

Faculty of Accountancy, Universiti Teknologi MARA, Selangor Branch

Puncak Alam Campus, Malaysia

Intan Waheedah Othman (Corresponding author)

Faculty of Accountancy, Universiti Teknologi MARA, Selangor Branch

Puncak Alam Campus, Malaysia

E-mail: waheedah87@uitm.edu.my

Nurul Jannah Abdullah

Sapura Energy Berhad, Jalan Tasik, Mines Wellness City

Seri Kembangan, Malaysia

Received: September 28, 2023   Accepted: November 1, 2023   Published: November 14, 2023

doi:10.5296/ber.v13i4.21341   URL: https://doi.org/10.5296/ber.v13i4.21341

Abstract

Cybersecurity is becoming increasingly crucial specifically for healthcare organizations. The advent of digital technologies such as telemedicine, the Internet of Medical Things (IoMT), and cloud-based solutions has brought about transformative advancements in patient care and administrative processes. However, with this progress comes an array of cyber threats that can have adversarial consequences if managed ineffectively. Driven by the growing concerns within the realm of cybersecurity, this paper delves into the issues and challenges faced by healthcare organizations in the deployment of cyber technologies. The research aims to dissect the multifaceted issues and challenges that contribute to compromised cybersecurity measures, resulting in potential data and system breaches. The study seeks to offer valuable insights, thereby paving the way for informed strategies and solutions to enhance cyber defenses and mitigate risks of unauthorized access and data breaches.

Keywords: Cybersecurity, Cyber risk, Cyberattack, Data breach, Healthcare

1. Introduction

Significant events such as the COVID-19 pandemic have accelerated technology adoption among corporate entities. Digital transformation, driven by emerging cyber technologies such as artificial intelligence, big data and data analytics, blockchain, cloud computing, the Internet of Things (IoT), and the industrial Internet of Things (IIoT), has now become a priority for businesses to embrace. However, along with the extensive benefits accompanying this transformation, cybersecurity has grown into a significant challenge for companies.

Cybersecurity is the practice of protecting data, computer systems and networks from unauthorized access or criminal use (Li & Liu, 2021). It involves the process of safeguarding data by preventing, detecting, and addressing cyber-attacks (Bozkus & Caliyurt, 2018). Cybersecurity is crucial as it protects organizations from cyber threats and helps to prevent attacks by malicious actors that may result in data breaches, unauthorized information disclosure, theft of, or damage to hardware, software, or data. The surge in cybersecurity-related incidents, especially those involving data security breaches, has a catastrophic impact on many industries. It was reported that cyber-attack cases demonstrated an increasing trend with a 38% rise in worldwide attacks in 2022 compared to 2021 (Anderson, 2023). The global cost of cybercrime which is projected to reach $10.5 trillion by 2025 (Ene, 2023) emphasizes that cybersecurity transcends national boundaries and requires global attention.

Cybersecurity is becoming increasingly crucial specifically for healthcare organizations. The advent of digital technologies such as telemedicine, the Internet of Medical Things (IoMT), and cloud-based solutions has brought about transformative advancements in patient care and administrative processes. However, with this progress comes an array of cyber threats that can have adversarial consequences if managed ineffectively.

Healthcare organizations offer a diverse range of health services, handle massive sensitive data and maintain extensive networks where enormous volumes of data are continually exchanged (Kruse et al., 2017; Abraham et al., 2019). The management of such extensive data, and reliance on various external services and providers offer cybercriminals an avenue to exploit specific vulnerabilities within the cybertechnology, thereby compromising the integrity of the healthcare company's supply and customer chain. The spectrum of cyber risks encompasses ransomware attacks, identity theft, and data breaches, posing persistent challenges for these organizations (Coronado & Wong, 2014; Tully et al., 2020). These cyber risks not only compromise patient privacy but can also disrupt medical operations, leading to potentially life-threatening situations.

The HIPAA Journal (2016) revealed that the healthcare industry constituted 88% of all ransomware attacks within US industries. Additionally, data breaches have afflicted over 90% of healthcare facilities in the US (Ponemon Institute, 2016). Further reinforcing this trend, a global report on cyberattacks by industry highlights that the healthcare sector witnessed a substantial 74% growth in cyberattacks in 2022 compared to the preceding year. This is followed by the government/military sector that emerged as the second most targeted, experiencing a 46% growth compared to the previous year (Anderson, 2023).

An effective cyber risk management is crucial as it allows an organization to comprehend, prioritize, and proactively manage cyber risks by implementing controls in a timely manner, mitigating potential effects on business timelines, quality, or costs (Cremer et al., 2022). The risk management strategy entails implementing robust cybersecurity measures such as incorporating data encryption, vulnerability assessments and access control to safeguard sensitive patient data and ensure the integrity of healthcare systems. Nonetheless, some organizations tend to neglect these critical preventive strategies, thereby exposing themselves to the risk of cybersecurity breaches.

The most challenging aspect of cybersecurity is realizing that hackers are one step ahead of businesses. They search for security flaws that employees are likely to overlook. The development of new technologies, particularly cloud and mobile, is accelerating exponentially. In this dynamic landscape, cybersecurity experts must remain in a vigilant state of awareness to anticipate and block hackers' efforts since they adapt to new technologies quickly (Javaid et al., 2023). Whilst security solutions are crucial for identifying and preventing malware, they are generally reactive rather than proactive.

Driven by the growing concerns within the realm of cybersecurity, this paper delves into the issues and challenges faced by healthcare organizations in the deployment of cyber technologies. The research aims to dissect the multifaceted issues and challenges that contribute to compromised cybersecurity measures, resulting in potential data and system breaches. The study seeks to offer valuable insights, thereby paving the way for informed strategies and solutions to enhance cyber defenses and mitigate risks of unauthorized access and data breaches.

2. Issues and Challenges in Cybersecurity Management

2.1 Complex Healthcare Data Ecosystem

An efficient healthcare system helps to ensure availability of medical services, smooth operation of medical systems and equipment, effective management of diverse types of data, safeguarding of patient data’s confidentiality and integrity, and compliance with industry regulations. In this context, healthcare cybersecurity holds paramount importance as it is not only a best practice, but also a legal requirement. The Health Insurance Portability and Accountability Act (HIPAA) in the United States, for instance, mandates that healthcare organizations safeguard patient data and maintain its confidentiality. Failure to comply with HIPAAA not only leads to legal consequences but also damages the organization's reputation and patient trust.

Nevertheless, navigating a complex ecosystem stands as a significant issue for the healthcare industry in effectively managing cybersecurity risks. The complexity of healthcare systems, which comprise of a myriad of interconnected devices, networks, databases, and applications poses hurdles for healthcare organizations in detecting and mitigating cybersecurity threats. This complexity further complicates the task of safeguarding the entire infrastructure, thus rendering healthcare organizations more susceptible to cyberattacks (DiPietro,2017).

The data ecosystem complexity can create vulnerabilities at various touchpoints within the healthcare system, as employees often handle sensitive data. In 2016, the Athens Orthopedic Clinic in the United States encountered a data breach incident stemming from an unaddressed vulnerability within their electronic medical record (EMR) system. This breach resulted in the unauthorized exposure of personal and medical data belonging to over 200,000 individuals, culminating in a penalty of $1.5 million for the clinic due to its failure to comply with HIPAA regulations. This breach had far-reaching consequences, opening avenues for potential identity theft, fraud, and various financial crimes. It further eroded patients' trust in the clinic, which has caused reputational damage for the business. (Alder, 2019).

2.2 Data Breaches

Cyber data breaches have evolved into one of the most serious concerns within the healthcare sector that cause catastrophic financial implications (Meisner, 2017). Data breach is classified into two main types: internal data breach and external data breach (Reddy et al., 2022). Internal data breach encompasses issues such as poor infrastructure, software vulnerabilities, and unauthorized database access. Conversely, external data breaches involve issues such as hacking, ransomware attacks, and theft.

In 2016, healthcare was ranked ninth on the list of most targeted industries for cyberattacks and fifth in terms of data breaches (Security Scorecard, 2016, p. 5). The problem with data breaches arises when hackers steal patient information, selling it on the dark web to individuals who then exploit it for illicit purposes such as drug trading, financial scams, and fraudulent insurance claims (Bathia & Agarwal, 2023). These crimes arise from malicious activities such as employee misuse of access, external agents utilizing stolen login details or devices, social engineering tactics or hacking through malware deployment to exploit weak credentials or system vulnerabilities (Meisner, 2017).

Healthcare data breaches have exposed 385 million patient records in the US from 2010 to 2022, with individual patient records being counted multiple times (Bryant, 2019). Smaller healthcare organizations are particularly vulnerable to data breaches and cyberattacks due to their limited resources and weaker cyber defences. These organisations often face the dilemma of allocating substantial funds for security measures while lacking immediate access to emergency security advisors in the event of a breach (Reddy et al., 2021). Cybercrime targeting personal data may lead to substantial financial losses for the victims (Meisner et al., 2017).

2.3 Medical Devices and System Vulnerabilities

Medical devices such as insulin pumps, intracardiac defibrillators, mobile cardiac telemetry, pacemakers, and intrathecal pain pumps and their interconnected nature present an additional concern to healthcare organizations as they are vulnerable to cyberattacks (Rodriguez, 2022). Medical devices often lack security monitoring, as they operate on a range of software and hardware platforms that make oversight using a single tool challenging. Companies that fail to implement proper certificate validation in their implementations would result in insecure network communication. Cybercriminals can exploit vulnerabilities in the supply chain and compromise medical devices to steal data, including personally identifiable information (PII), intellectual property, research findings, data from drug trials, financial information, and medical records, and then monetize the data in a variety of ways (Trend Micro, 2018). Based on findings from the Medical IoT Survey (2022), medical facilities with more than 75% of connected medical devices face a 24% higher risk of cyberattack than practices with less than 50% of connected devices (Capers, 2022). Individuals with malicious intent can breach these devices and instruct them to provide inaccurate readings, administer drug overdoses, or otherwise endanger the health of patients (Federal Bureau of Investigation, 2022).

Implantable and programmable medical devices, such as insulin pumps and pacemakers, have been targeted in cyberattacks (Kapoor et al., 2019). For instance, insulin pumps provide diabetic patients with continuous protein insulin delivery. A hacker can infiltrate the device's wireless connectivity and gain illicit access via a tiny radio transmitter, enabling them to manipulate the device's settings and operations. The hacker can secretly administer substantial doses of insulin to patients, without their awareness or consent. This can have serious consequences for the victimized patients, resulting in severe hypoglycaemia that can lead to functional brain damage.

Exploitation of medical devices has a negative implication on the operational processes, patient safety, data confidentiality, and data integrity of healthcare facilities (Federal Bureau of Investigation,2022). Failure to address these issues promptly will gradually intensify the adverse impact they have on the landscape of medical devices and systems in the healthcare industry.

2.4 Insider Threats

Insider threat is a serious challenge when managing cybersecurity risks. Insider threats can range from unintentional actions, such as carelessness, to malicious actions that cause destruction. Insider threats are those involving individuals within a healthcare organization, such as employees, but also contractors and business associates that have been provided with access to healthcare assets, networks and systems (Lee, 2022). A common form of insider threat is patient data theft. Other forms of insider threat include convenience and curiosity, such as unauthorized access to information unrelated to the provision of healthcare and circumvention of security measures to facilitate work (Lee, 2022).

The challenge lies in detecting the malicious activities of insiders, given that they hold authorized access and operate within the confines of their established boundaries. Unlike external threats that need to breach security measures, insiders can exploit vulnerabilities from within. Insiders may have knowledge of the network setup, defense system and vulnerabilities, making them better equipped to exploit weaknesses without raising suspicion (Saxena et al., 2020). It might be difficult to spot an insider threat among authorized users since their behavior may seem legitimate and blend in with everyday activity. Balancing the need for access privileges with the risk of insider threats becomes a delicate task for organizations.

A study revealed that 60% of healthcare organizations had encountered breaches originating from third-party vendors or business associates, highlighting a deficiency in effectively managing these relationships (Alder, 2023). Another case is the WannaCry ransomware attack in 2017, which significantly impacted healthcare institutions worldwide, including the UK's National Health Service (NHS). The rapid spread of this attack resulted from unpatched systems and a lack of cybersecurity proficiency among staff members. This dire situation forced the NHS to cancel appointments and delay surgeries, demonstrating how a cybersecurity breach can exert serious repercussions on healthcare operations.

Several instances of insider threat cases stem from unintended actions, notably human errors (Lee, 2022). These actions encompass scenarios like inadvertently clicking on a phishing link in an email or mistakenly inputting inaccurate information into Electronic Health Records. Insiders would then steal sensitive data for financial gain, leak information to competitors, or disrupt critical systems. The consequences of insider threats can be severe, leading to financial losses, reputational damage, legal liabilities, and erosion of patient trust. Rebuilding trust and mitigating the impact of insider threats can be challenging and time-consuming.

2.5 Legacy System Vulnerabilities

Obsolete legacy systems are another issue which increases the exposure of cyberattack in the healthcare sector (Abed & Griffths,2019). A legacy system in healthcare pertains to outdated clinical technology, applications, or hardware that have become functionally and connectively obsolete (Abu Bakar et al., 2021). Medical devices operating on an outdated legacy system might harbor vulnerabilities, thereby increasing the susceptibility to severe cyberattacks (Tervoort et al., 2020).

The predicament associated with obsolete legacy systems emerges as medical practitioners and personnels strive with executing their duties on systems prone to crash, connectivity problems, or overwhelming complexity, rendering them nearly inoperable (Ahmed et al., 2019). This issue extends to external IT providers, who are similarly constrained by these legacy systems due to limited resources for effective digital transformation initiatives. Moreover, equipment currently in use lacks vendor support and encounter challenges in implementing software patches, largely due to its outdated nature (Tervoort et al., 2020).

Obsolete legacy systems are exposed to malware and ransomware attacks, exerting impact on the core healthcare system, such as Electronical Health Records (EHRs), Picture Archiving and Communication Systems (PACS), and Laboratory Information Systems. This, in turn, leads to treatment providers being unable to access patient information at the point of care, creating widespread disruptions within the organization and severely compromising patient safety (Abed & Griffths,2019). Consequently, the healthcare organization could potentially lose its proficient legacy system users. Healthcare employees are not only frustrated by slow response times, glitches, error notifications, and frequent system failures but they are also rendered less productive and may jeopardize the quality of patient care.

3. Obstacles in Effective Cybersecurity Management

3.1 Limited Funding

Resource limitations, specifically budgetary, staffing, and time constraints, present a significant hurdle for healthcare organizations aiming to invest in and implement effective cybersecurity technologies. The Ponemon Institute's study in 2019 revealed that 79% of healthcare organizations experienced data breaches in the preceding two years, with 45% attributing these breaches to lack of funding as a key impediment to prevention. These challenges are particularly pronounced among smaller healthcare organizations that often lack the necessary budget to implement basic cybersecurity measures, such as encryption and two-factor authentication (PWC, 2021).

The rise of telemedicine, the Internet of Medical Things (IoMT), and cloud-based solutions brings both convenience and complexity. While these technologies enhance patient care and streamline processes, ensuring the security of these interconnected systems is an ongoing challenge. There exists a tendency to prioritize patient care over cybersecurity, which often translates to insufficient time and resources dedicated to reinforcing cybersecurity initiatives. This is corroborated by the finding that numerous healthcare providers strived with the complex balance between addressing COVID-19 and sustaining cybersecurity, ultimately heightening their vulnerability to cyberattacks (Muthuppalaniappan & Stevenson, 2021).

3.2 Lack of Cybersecurity Expertise

Whilst having to secure sufficient financial allocation for cybersecurity, the challenge remains in the recruitment of qualified cybersecurity experts. Healthcare providers might lack the requisite knowledge or skill set to implement effective cybersecurity measures. The shortage of cybersecurity specialists in the healthcare industry exacerbates the issue, possibly due to salary disparities, making it difficult for healthcare organizations to secure qualified personnel (HIPAA Journal, 2023).

Based on the survey by the Healthcare Information and Management Systems Society (HIMSS), a mere 25% of healthcare organizations had a dedicated cybersecurity professional within their workforce. Yaraghi et al. (2018) emphasize that lack of cybersecurity expertise is a significant factor of data breach litigation which is viewed as negligence on the part of the healthcare organization. This may cause huge fines for violating data protection regulations, eventually leading to significant financial and reputational damages for the organization.

4. Recommendations for Effective Cybersecurity Management in Healthcare Industry

Cybersecurity is a critical issue that requires attention amidst the widespread adoption of digital technologies within healthcare organizations aimed at enhancing healthcare delivery and operational efficiency. Ensuring the security of these cyber technologies is an ongoing challenge. Within this context, the Theory of Planned Behaviour (TPB) emerges as a strategic solution, offering invaluable approaches to navigate cybersecurity concerns specific to the healthcare domain.

TPB is a psychological model developed by Ajzen (1991) that can be applied to explain and predict human behavior in deploying cybersecurity practices within healthcare organizations. TPB comprises three key variables which include attitude, subjective norm, and perceived behavioral control. Specifically, attitude is connected to beliefs which produce a favorable or unfavorable attitude towards behavior. Subjective norms refer to an individual’s perception of the social pressure to perform or not perform a particular behavior. Perceived behavioral control refers to an individual’s perception of their ability to perform a behavior (Icek Ajzen, 2019). In general, when a person has a stronger attitude, subjective norm, and perceived behavioral control towards a certain behavior, their intention to engage in that behavior is likely to be higher.

As the digital transformation continues to reshape the healthcare sector, it becomes paramount to effectively address cybersecurity challenges. By creating an environment based on the TPB model where cybersecurity is valued, understood, and integrated, healthcare organizations can significantly enhance their ability to protect patient data, maintain compliance, and effectively respond to cyber threats.

4.1 Investing in Cybersecurity Assessment Tool (CSAT) Programs

In the context of TPB, attitude encompasses an individual’s perception of the importance of following security protocols and best practices to protect confidential data (Alanazi et al., 2022). By fostering a culture that emphasizes the importance of cybersecurity and making it a priority, healthcare organizations can positively influence employees’ attitudes towards embracing cybersecurity. This is where the attitude is connected to beliefs where it may influence the healthcare industry’s intention to implement cybersecurity measures.

In shaping the attitude and culture towards adopting cybersecurity strategic approach, it is crucial that healthcare organizations allocate sufficient amount of funds for investment in cybersecurity assessment tool (CSAT) programs. CSAT is a specialized software or set of software tools designed to analyze the security status of an organization's digital infrastructure, systems, networks, and applications. CSAT can help organizations track their implementation of cybersecurity best practices, besides identifying weaknesses, and potential risks that could be exploited by cyber attackers. By conducting thorough assessments, organizations can proactively address security gaps and enhance their overall cybersecurity defenses.

4.2 Establishing Cybersecurity Control Framework

The subjective norm component of the TPB entails the perception of whether superiors or employees support and encourage adherence to security protocols (Yeng et al., 2022). The top management plays a pivotal role to actively support cybersecurity initiatives (Jalali & Kaiser, 2018). The management's dedication to cybersecurity may strengthen the belief that these security measures hold significance and warrant adherence. Fostering positive peer influence is also important and can be facilitated through internal communication channels, showcasing instances where colleagues' adherence to cybersecurity protocols has prevented security incidents.

Establishing subjective norms within healthcare organizations is vital for the development of a dynamic cybersecurity framework tailored to safeguard the complex healthcare ecosystems. Such a framework has far-reaching implications, including enhancing efficiency, resilience, privacy, and information security (Boudko & Abie, 2019). To establish these subjective norms effectively, healthcare organizations need to implement strong policies that promote security. These policies should encompass a range of aspects, from access control to data encryption. Healthcare organizations should also proactively collaborate with industry-leading technology experts and standard bodies. These experts can offer valuable insights into emerging threats and best practices. Standards bodies, such as NIST (National Institute of Standards and Technology) and ISO (International Organization for Standardization), can help create, develop, and coordinate standards, policies, or procedures that align with the specific needs and intricacies of healthcare environments.

4.3 Training

Perceived behavioral control of the TPB refers to an individual’s confidence in their ability to recognize and avoid security threats. Employees often serve as the first line of defense against cyberattacks, and their awareness and actions can significantly impact an organization's security posture. Employee training is therefore important which should empower staff to not only understand cybersecurity best practices but also to identify, report, and address security threats promptly (He et al., 2020). Training should be designed in a way that not only expands employees' knowledge, but also motivates them to develop compliant behaviors.

The management should also facilitate by streamlining the security implementation process as much as possible. It is crucial to ensure that employees can easily comprehend and adhere to security protocols (Nifakos et al., 2021). This may entail providing clear step-by-step guides, user-friendly tools, and implementing automation wherever applicable. Equipping healthcare personnel with awareness programs, training courses and information sharing on the nature of cybersecurity attacks may improve employees’ acceptance towards the need for managing cyber risks, hence determining the success of the overall cybersecurity strategy (Basel, 2021).

5. Conclusion

The complex interplay between digital transformation and cybersecurity within the healthcare sector poses significant challenges and implications. The rapid adoption and the integration of cyber technologies have resulted in transformative advancements while simultaneously amplifying vulnerabilities. The surge in cybersecurity-related incidents, including data breaches and cyberattacks, underscores the urgent need for robust protective measures. The realm of cybersecurity transcends organizational boundaries, necessitating collaboration among healthcare professionals, IT consultants, government agencies and vendors. A proactive approach that encompasses risk management, strong policies, and an empowered workforce is vital in the face of cyber threats.

The complexities of healthcare systems, ranging from interconnected medical devices to diverse data ecosystems, contribute to the vulnerability of the sector. Insider threats and the exploitation of legacy systems pose additional challenges, underscoring the need for effective cybersecurity strategies. However, constraints such as limited resources and expertise can hinder effective implementation.

A comprehensive approach is necessary to address the challenges of cybersecurity in healthcare organizations. Integrating the Theory of Planned Behavior (TPB) into cybersecurity strategies offers a structured framework to shape attitudes, address subjective norms, and enhance perceived behavioral control. By applying TPB principles in the context of healthcare cybersecurity, organizations may gain understanding of the factors that influence behavioral change among healthcare personnel, analyzing the effectiveness of training programs, and uncovering methods to facilitate a cultural shift toward cybersecurity awareness (Nifakos et al., 2021; Alanazi et al., 2022). This empowers organizations to foster a culture of cybersecurity awareness and preparedness. This approach goes beyond mere compliance and seeks to instill a proactive mindset among healthcare personnel, ultimately strengthening the overall cybersecurity posture of healthcare organizations.

As the digital transformation continues to revolutionize healthcare, future studies could concentrate on enhancing health data privacy frameworks. Research may involve exploring innovative methods for preserving patient confidentiality, secure data sharing, and the intersection of blockchain technology with healthcare data management.

In conclusion, healthcare organizations can create strategies to encourage cybersecurity best practices among their staff members by using the theory of planned behavior. This can assist in developing a culture of security and lowering the danger of cybersecurity threats in the healthcare sector.

Acknowledgments

The authors express their gratitude for the financial and administrative assistance provided by the Faculty of Accountancy, Universiti Teknologi MARA Cawangan Selangor, Malaysia.

Authors contributions

Not applicable.

Funding

Not applicable.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Macrothink Institute.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

Open access

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

References

Abed, S. F., & Griffiths, G. (2019). *Legacy applications: A healthcare cybersecurity nightmare*. Bridgehead. [Online] Available: https://www.bridgeheadsoftware.com/wp-content/uploads/2019/02/Legacy_Applications_Cybersecurity_Nightmare_BridgeHead_Whitepaper.pdf

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

Abu Bakar, H., Razali, R., & Jambari, D. I. (2021). Legacy systems modernisation for citizen-centric digital government: A conceptual model. *Sustainability, 13*(23), 13112. https://doi.org/10.3390/su132313112

Ahmed, Y., Naqvi, S., & Josephs, M. (2019). *Cybersecurity metrics for enhanced protection of healthcare IT systems.* Proceedings of the International Symposium on Medical Information and Communication Technology. pp. 1-9. https://doi.org/10.1109/ISMICT.2019.8744003

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior, 136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Alder, S. (2023). Healthcare organizations most common victims in 3rd party data breaches. *HIPAA Journal.* [Online] Available: https://www.hipaajournal.com/healthcare-most-common-victim-in-3rd-party-data-breaches/#:~:text=Healthcare%20organizations%20were%20the%20most,%2C%20and%20government%20(14%25).

Alder, S. (2023). Survey highlights ongoing healthcare cybersecurity challenges. *HIPAA Journal*. [Online] Available: https://www.hipaajournal.com/survey-highlights-ongoing-healthcare-cybersecurity-challenges/

Alder, S. (2019). Athens orthopedic clinic pays $1.5 million HIPAA penalty after 2016 data breach. *HIPAA Journal*. [Online] Available: https://www.hipaajournal.com/athens-orthopedic-clinic-pays-1-5-million-hipaa-penaltyafter-2016-data-breach-9882/

Alder, S (2016). Healthcare industry accounts for 88% of ransomware attacks. *HIPAA Journal*. [Online] Available: https://www.hipaajournal.com/healthcare-industry-accounts-88-ransomware-attacks-3519/

Anderson, J. L. (2023, January 20). *Global cyberattacks increased 38% in 2022.* Security Magazine. [Online] Available: https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022

Bhatia, K., & Agarwal, S. (2023). A critical study of cybercrime: It's impact during covid-19. *Journal of Survey in Fisheries Sciences, 10*(4S), 3111-3121.

Boudko, S., & Abie, H. (2019). *Adaptive cybersecurity framework for healthcare internet of things.* Proceedings of the International Symposium on Medical Information and Communication Technology. pp. 1-6. https://doi.org/10.1109/ISMICT.2019.8743905

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal, 33*(4), 360-376.

https://doi.org/10.1108/MAJ-02-2018-1804

Branley-Bell, D., Coventry, L., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff. *Annals of Disaster Risk Sciences*, *3*(1), 1-14. https://doi.org/10.51381/adrs.v3i1.51

Bryant, M. (2019, February 15). *Cybersecurity, privacy top healthcare leader concerns Healthcaredive*. [Online] Available: https://www.healthcaredive.com/news/cybersecurity-privacy-top-healthcare-leader-concerns/548541/

Capers, Z. (2022, November 29). *More healthcare devices means more cyberattacks - How weak medical IOT security threatens patient care*. Capterra. [Online] Available: https://www.capterra.com/resources/medical-internet-of-things-iot-security/

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice, 47*(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6

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

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

DiPietro, M. (2017). Addressing cybersecurity in healthcare: Building a strong foundation for current and future threats. *Journal of Healthcare Information Management, 31*(4), 8-14.

Ene, C. (2023, February 22). *10.5 trillion reasons why we need a united response to cyber risk, Forbes.* [Online] Available: https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=42b04e1d3b0c

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of covid-19: Scoping review. *Journal of Medical Internet Research, 23*(4), e21747. https://doi.org/10.2196/21747

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital, 21*(2), 203-213. https://doi.org/10.1108/JIC-05-2019-0112

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: a systematic, organizational perspective. *Journal of Medical Internet Research, 20*(5), e10059. https://doi.org/10.2196/10059

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications, 100016*, 1-13. https://doi.org/10.1016/j.csa.2023.100016

Kapoor, A., Vora, A., Yadav, R. (2019). Cardiac devices and cyber attacks: How far are they real? How to overcome? *Indian Heart Journal, 71*(6), 427-430. https://doi.org/10.1016/j.ihj.2020.02.001

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, 25*(1), 1-10. https://doi.org/10.3233/THC-161263

Lee, I. (2022). Analysis of insider threats in the healthcare industry: A text mining approach. *Information, 13*, 404. https://doi.org/10.3390/info13090404

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

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

Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. *Copernican Journal of Finance & Accounting, 6*(3), 63-73. https://doi.org/10.12775/CJFA.2017.017

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *International Journal for Quality in Health Care, 33*(1), mzaa117. https://doi.org/10.1093/intqhc/mzaa117

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. https://doi.org/10.3390/s21155119

Ponemon, L. (2016, May 12). *Nearly 90 percent of healthcare organizations suffer data breaches, new ponemon study shows*. Ponemon Institute. [Online] Available: https://www.ponemon.org/news-updates/blog/security/nearly-90-percent-of-healthcare-organizations-suffer-data-breaches-new-ponemon-study-shows.html

PWC. (2021). *Global top health industry issues 2021*. [Online] Available: https://www.pwc.es/es/publicaciones/sanidad/pwc-global-top-health-industry-issues-2021.pdf

Reddy, J., Elsayed, N., Elsayed, Z., & Ozer, M. (2022). *Data breaches in healthcare security systems, cryptography and security*. [Online] Available: https://arxiv.org/pdf/2111.00582.pdf

Rodriguez, S. (2022, December 2). *Weak connected medical device security increases cyberattack threats*. Health IT Security. [Online] Available: https://healthitsecurity.com/news/weak-connected-medical-device-security-increases-cyberattack-threats

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K. K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics, 9*(9), 1460. https://doi.org/10.3390/electronics9091460

Tervoort, T., De Oliveira, M. T., Pieters, W., Van Gelder, P., Olabarriaga, S. D., & Marquering, H. (2020). Solutions for mitigating cybersecurity risks caused by legacy software in medical devices: A scoping review. *IEEE Access, 8*, 84352-84361. https://doi.org/10.1109/ACCESS.2020.2984376

Trend Micro (2018). *Exposed medical devices and supply chain attacks in today's connected hospitals*. [Online] Available: https://documents.trendmicro.com/assets/rpt/exec-series-exposed-medical-devices-and-supply-chain-attacks-in-todays-connected-hospitals.pdf

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health Security, 18*(3), 228-231. https://doi.org/10.1089/hs.2019.0123

Yaraghi, N., Du, A. Y., Sharman, R., & Gopal, R. (2018). An empirical analysis of data breach litigation. *Journal of Management Information Systems, 35*(1), 228-259.

Yeng, P. K., Fauzi, M. A., & Yang, B. (2022). A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information, 13*(7), 335. https://doi.org/10.3390/info13070335