ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/iyad-m-ghonimat/23

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 4

Review Article

Cybersecurity Challenges in Healthcare Institutions and Approaches for Addressing this Concern

Iyad M Ghonimat[1]* and Rafeef A Ghonaimat[2]

[1]InternationalAmericanUniversity, USA

[2]Department of Internal medicine, Islamic hospital, Jordan

Citation: Ghonimat IM, Ghonaimat RA. Cybersecurity Challenges in Healthcare Institutions and Approaches for Addressing this Concern. *J Artif Intell Mach Learn & Data Sci 2024*, 1(4), 31-36. DOI: doi.org/10.51219/JAIMLD/iyad-m-ghonimat/23

Received: February 25, 2024; **Accepted:** February 29, 2024; **Published:** March 15, 2024

***Corresponding author:** Iyad M Ghonimat, International American University, USA, E-mail: ighonimat@gmail.com

ABSTRACT

Background: Cybersecurity is the practice of safeguarding systems, networks, and data from unauthorized access, use, disclosure, interruption, modification, or destruction. In healthcare, the significance of cybersecurity cannot be overstated, as healthcare institutions store and transmit sensitive patient data. Breaches in healthcare can result in severe consequences for patients, including unauthorized access to personal information, manipulation of medical records, service disruption, and financial loss.

Aim: This research aims to identify key cybersecurity challenges within healthcare organizations and propose comprehensive strategies to fortify cybersecurity measures. These measures are essential for safeguarding patient information and ensuring uninterrupted healthcare services in an increasingly digital healthcare landscape.

Method: This study thoroughly examines the cybersecurity threat landscape in the healthcare industry. It relies on extensive analysis of desktop search data, government reports, and incorporates relevant case studies and expert opinions.

Results: The research highlights the pressing need for healthcare organizations to possess a deep understanding of evolving cybersecurity risks. It underscores the importance of staying current with the latest healthcare cybersecurity solutions. Moreover, the study emphasizes that regular assessments of cybersecurity programs are imperative to ensure compliance with evolving risks and requirements.

Conclusion: Healthcare businesses must continually adapt and fortify their cybersecurity measures to effectively protect patient data and maintain the integrity of healthcare services.

Keywords: Cybersecurity threats, Healthcare industry, Ransomware

1. Introduction

In recent years, legislative measures have driven healthcare providers to embrace the concept of “meaningful use” by integrating networks into the delivery of healthcare services. This integration has led to the adoption of electronic-based systems, marking a significant transformation within healthcare organizations.

The emergence of cybercrime as a pressing concern traced back to the late 1970s, coinciding with the rapid growth of the computer information technology (IT) industry. What initially began as unsolicited electronic communications has evolved into a sophisticated landscape of malicious software, including viruses and malware. This technological evolution continues to advance in sophistication and coordination.

The healthcare sector, in particular, has become an attractive target for cybercriminals due to the abundance of sensitive personal and financial data housed within electronic health records. Yet, the integration of healthcare technology is a multifaceted endeavour that demands meticulous preparation and substantial time and financial investments to implement effectively.

Crucially, post-implementation, the regular updating of software is imperative to address emerging advancements and security vulnerabilities that hackers exploit. It is noteworthy that while many organizations allocate significant financial resources to achieve integration, they often overlook the importance of allocating sufficient time and resources for the ongoing maintenance and updating of software.

2.1. Problem statement

The increasing digitization of patient records and medical systems has elevated the vulnerability of patients' personal information and vital healthcare infrastructure. In the face of persistent and ever-evolving cyberattacks on healthcare providers, patients' personal data is continually jeopardized, while hospitals and clinics incur substantial financial losses[1].

In light of these pressing challenges, it is imperative to investigate the cybersecurity vulnerabilities within healthcare organizations and develop effective strategies to counteract these threats. This research seeks to identify the core cybersecurity issues within healthcare entities and put forth comprehensive measures to fortify cybersecurity defenses. The primary goals are to protect patient information, uphold privacy, ensure the safety of healthcare infrastructure, and guarantee uninterrupted access to essential healthcare services in an increasingly digital healthcare landscape.

2.2. Literature review

This literature review is structured to provide a comprehensive examination of the cybersecurity challenges faced by healthcare organizations. It is organized into distinct sections, each focusing on a critical dimension of this complex landscape. The first section highlights the impact of legislative measures, such as the ACA and HITECH, on healthcare technology adoption and the resultant vulnerabilities to cyber threats. The second section explores the profound repercussions of cybersecurity incidents on the healthcare sector and the ongoing transformation from a doctor-centric system to a technology-centred one. In addition, it discusses proactive measures essential for preserving data integrity and enhancing cybersecurity defences. Finally, the third section introduces the Internet of Things (IoT) and its relevance in healthcare, emphasizing the unique challenges posed by interconnected devices. Furthermore, it sheds light on the growing ransomware threat, elucidating its evolution and impact on individuals and organizations.

2.3. Legislation and digital transformation in healthcare

Kruse et al.[1] underscored the transformative impact of legislative measures such as the Patient Protection and Affordable Care Act (ACA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) on healthcare technology. These regulations incentivize healthcare providers to demonstrate "meaningful use" by integrating networks into service delivery. The shift to electronic-based systems in healthcare organizations, driven by these legislative measures, has inadvertently heightened vulnerability to cybercrime. The origins of cybercrime can be traced back to the late 1970s, coinciding with the emergence of the computer information technology (IT) industry. Initially, it manifested as unsolicited bulk messages and gradually evolved into malicious software, encompassing viruses and malware. The relentless advancement of technology is marked by increasing sophistication and coordination. The healthcare sector, harbouring sensitive personal and financial data within health records, becomes an attractive target for cybercriminals[1].

2.4. The Impact of cybersecurity incidents and proactive measures

Bésenyő and Kovács[3] emphasized the profound repercussions of cybersecurity incidents on the healthcare sector, encompassing hospitals, clinics, and various healthcare organizations. The global healthcare industry is undergoing substantial transformation, with technology increasingly taking centre stage. This shift is transitioning the sector from a predominantly doctor-centric system to one predominantly centred on technology. The integration of advanced technology is enabling more efficient and effective methods that enhance precision in medical services. However, this transformation necessitates heightened vigilance and advancements in addressing and mitigating cybersecurity risks[2].

In a separate study, [3]stressed the criticality of preserving data integrity, particularly patient data privacy. Healthcare organizations must prioritize the implementation of proactive measures to effectively mitigate, identify, and address cybersecurity threats. This may involve the adoption of effective strategies to combat cybercrime, routine risk assessments, and continuous cybersecurity training for personnel[3].

2.5 Internet of Things (IoT) and the Emergence of Ransomware

Saheed and Arowolo[4] introduced the concept of the Internet of Things (IoT) and its relevance in healthcare. IoT facilitates the connection of various objects to the Internet, enabling data sharing, intelligent identification, tracking, monitoring, and administration. The interconnectedness of various devices, ranging from smartphones to medical tools, poses unique cybersecurity challenges. Ensuring seamless connectivity while safeguarding data in an increasingly interconnected healthcare environment is a paramount concern[4].

In a recent study by[5], the susceptibility of computers to various forms of malicious software, including worms, malware, viruses, and spyware, was highlighted. Notably, ransomware has emerged as a pervasive menace, targeting both individuals and organizations. Ransomware attacks often coerce victims into purchasing decryption keys to recover their encrypted data, making financial gain a primary motivation for cybercriminals. These attacks have evolved to encrypt not only the victim's device but also network-based data accessible to the user. The assessment of malicious emails and contaminated text is a common vector for these attacks[5].

4. Methodology

4.1 Study Design

This review aimed to comprehensively analyze the cybersecurity threat landscape in healthcare, including types of threats and their impact, case studies, unique challenges, mitigation strategies, and future trends. The methodology employed for this review involved the following steps:

3.1.1. Literature search and selection criteria: A thorough search of relevant literature was conducted using reputable academic databases, including PubMed, IEEE Xplore, Google Scholar, and selected healthcare cybersecurity journals. The search encompassed articles published between 2017 and 2023, ensuring that recent research and incidents were included.

3.1.2. Data extraction and categorization: Information was systematically extracted from selected articles and categorized into distinct sections, including types and impacts of cybersecurity threats, recent incidents, unique challenges in healthcare cybersecurity, mitigation strategies, case studies, and future trends. Each section was analyzed separately to provide a comprehensive overview.

3.1.3. Synthesis and analysis: The extracted data were synthesized and analyzed to identify common themes, trends, and patterns across the literature. This analysis aimed to offer valuable insights into the evolving landscape of cybersecurity threats and solutions within the healthcare sector.

4. Findings and Discussion

4.1. Types and impact of cybersecurity threats in healthcare

Data breaches are the most prevalent cybersecurity events in the healthcare sector, involving illegal access to patient data, often referred to as data breaches. These breaches entail the intrusion of unauthorized individuals who gain access to sensitive patient information, including names, addresses, Social Security numbers, and medical records. Specific categories of data compromised in such events may include credit card numbers, medical records, and Social Security numbers[2].

Ransomware attacks are a significant cybersecurity problem commonly encountered in the healthcare sector. Malicious software, known as malware, is delivered into a computer network through a method called ransomware, employed as a means of assault. This malware uses encryption techniques to secure crucial data before demanding a ransom payment in exchange for its release[1].

Phishing attacks are fraudulent endeavors aimed at deceiving individuals into disclosing personal information, such as passwords and credit card details. These acts of aggression are carried out in a digital setting, often through popular communication channels like email and text messages.

Insider threats refer to cybersecurity dangers originating from within an organization. The term "insider threats" is used to define concerns related to employees who display either malicious intent or carelessness. Such employees have the potential to contribute to errors made by insiders[1].

4.2. Recent cybersecurity incidents in healthcare

In 2020, the University of Utah Health reported two different data breaches that affected patients' personal information and medical records. The first data breach at the University of Utah Health led to unauthorized access to some workers' email accounts. The second incident may have been caused by the discovery of malware on an employee's computer. Investigators believe that scam emails were the primary cause of the first data breach at the University of Utah Health. Phishing emails have been a longstanding tactic used by hackers. In a professional setting, a phishing email might appear to come from a trustworthy source, such as a third-party group doing business with the company or even an employee of the company. Hacking often involves providing directions to the targeted individual, asking them to enter their username and password to prove their identity and recover their login credentials. Malware typically infiltrates a computer when someone installs software. Hackers can also trick users into opening a dangerous attachment in an email, downloading a strange file, or clicking on a link that takes them to a malicious website.

After installing malware, a hacker gains unauthorized access to the computer system, making it easier for them to acquire private information without permission. Ultimately, someone infiltrated the University of Utah Health system and stole the personal information of more than 600,000 people[6].

In 2019, Methodist Hospitals reported a data breach that exposed patients' personal information to potential risks. The organization issued a press release in October 2019, with the purpose of alerting those affected and providing them with opportunities to enhance the security of their personal information. The breach, caused by phishing via email, specifically targeted the email accounts of employees. Suspicious behavior associated with staff email accounts came to the administrators' attention in June. Subsequently, the healthcare organization initiated an inquiry in collaboration with a team of investigators from an independent third party. The investigation concluded that a phishing scheme successfully stole sensitive information from two different employees on separate dates. Unauthorized access to an employee's email account was discovered on two consecutive occasions—the 12th of June and during the week of July 1 to July 8. Another email account was breached for approximately three months, starting on March 13 and continuing until June 12 of that year.

Finally, according to[2], "There has been a significant increase in cybersecurity incidents and data breaches over the past few years[7]. Below are the top ten data breaches (Table 1) that are under investigation by the Office of Civil Rights (U.S. Department of Health & Human Services, 2020 data, see references). The victim organizations are arranged in the order of most individuals affected by the data breach".

5.3. Unique challenges in healthcare cybersecurity

5.3.1. Data sensitivity and privacy concerns: Confidential patient information, including personal details such as names, addresses, Social Security numbers, and medical records, falls under the responsibility of healthcare facilities. These facilities are accountable for both preserving and transmitting this information. Numerous legislative and regulatory safeguards, such as the[8], are in place to protect the confidentiality of patient information. Healthcare institutions are mandated to assume the responsibility of safeguarding patient data from unauthorized access, utilization, or disclosure.

5.3.2. Human factors: Insider Threats and Training Gaps. Insider threats, often originating from employees with privileged access to patient information, pose a significant risk. these employees can inadvertently or maliciously compromise data security. inadequate training and awareness programs can exacerbate this risk, as employees may fall victim to deceptive practices such as clicking on malicious links or attachments in phishing emails. given the substantial workforce in healthcare organizations with privileged access, effective training and awareness initiatives are paramount.

Table 1: Top 10 data breaches under investigation.

No	Health Care Provider	State	Affected Persons	Breach Date	Nature of Breach
1	Regal Medical Group,	CA	3300638	Feb, 2023	Hacking
2	Lincare Holdings Inc.	FL	1737775	Oct, 2021	Hacking
3	Bapist Medical Centre	TX	1608549	July, 2022	Hacking
4	Eskenazi Health	IN	1515918	Oct, 2022	Hacking
5	Community Health Network, Inc. as an Affiliated Covered Entity	IN	1500000	Nov, 2022	Breach of Confidentiality
6	The Kroger Co.	OH	1474284	Feb, 2021	Hacking
7	St. Joseph's/Candler Health System, Inc.	GA	1400000	Aug, 2021	Hacking
8	North Broward Hospital District	FL	1351431	Jan, 2022	Hacking
9	University Medical Centre Southern Nevada	NV	1300000	Aug, 2021	Hacking
10	Texas Tech University Health Sciences Centre	TX	1290104	July, 2022	Hacking

5.4 Regulatory and compliance requirements

Healthcare companies must adhere to a complex web of rules and regulations governing data protection. HIPAA, among other regulations, outlines stringent requirements for safeguarding patient data. Compliance with these regulations is non-negotiable to protect patient privacy and avoid financial penalties.

5.5 Strategies for mitigating healthcare cybersecurity risks

In the digital healthcare era, effective cybersecurity rules and laws are critical for protecting health data. Effective cybersecurity solutions are required as cyber threats and attacks become more frequent, complex, and targeted. Cyberattacks on healthcare organizations can result in the loss of patient privacy, financial loss, legal and regulatory ramifications, and reputational damage.

It is a critical requirement for healthcare organizations to conduct routine risk assessments to identify and evaluate the cybersecurity risks they face. Following the identification of hazards, firms must implement appropriate controls to mitigate such risks. Another essential component in healthcare firms is identifying vulnerabilities, which can detect gaps in their information technology (IT) systems through the use of vulnerability assessments. Vulnerability assessments cover a wide range of technologies and procedures, including but not limited to penetration testing and network scanning, which can be used to evaluate and discover potential vulnerabilities.

Furthermore, prioritizing cybersecurity risks is crucial. Businesses should evaluate the likelihood of a threat materializing and the potential implications that a breach would impose on the firm. Several criteria must be considered when deciding the order of significance for risks. These variables include the level of sensitivity connected with the data at risk, the regulatory duties relevant to the firm, and the financial ramifications of implementing security measures. On the other hand, security policies and procedures contribute to the establishment of security rules and procedures, serving as the fundamental framework for implementing a strong cybersecurity program. The development of security policies and procedures is critical for clearly defining employees' individual roles and obligations and providing a thorough framework for the implementation of security measures that employees must follow. It is vital to evaluate and update security policies and processes regularly to ensure they align with current cybersecurity threats and legislation[2].

Incident response plans are essential for handling cybersecurity occurrences and minimizing their effects. Constructing incident response plans requires the clear demarcation of employee roles and responsibilities and the full description of the sequential actions that must be taken in the occurrence of a cybersecurity incident. It is crucial to regularly test incident response tactics to ensure their efficacy.

Moreover, the prevention of cyberattacks relies heavily on the implementation of staff training programs and the cultivation of awareness among workers. It is critical for healthcare organizations to equip their employees with extensive training on cybersecurity best practices. This education must cover fundamentals like recognizing and avoiding phishing attacks and creating secure passwords. To keep employees up-to-date on the latest cybersecurity threats, regular training is required.

Finally, as part of the technology role, firewalls and intrusion detection systems are critical security measures that play a critical role in protecting healthcare firms from cyberattacks. Firewalls are used to prevent unauthorized access to computer networks, whilst intrusion detection systems are used to detect and counteract malicious activity within those networks. Furthermore, Security Information and Event Management (SIEM) has the capability of gathering and scrutinizing logs emanating from various components of an IT infrastructure within a healthcare institution, with the goal of detecting potential security flaws. SIEM systems can provide warnings and reports, allowing security teams to respond to situations more quickly and efficiently[5].

Similarly, healthcare organizations can use threat intelligence to improve their security posture and incident response capabilities, and, of course, compliance and regulatory adherence (e.g., HIPAA compliance). Healthcare firms are required to follow a variety of cybersecurity standards and regulations, including the Health Insurance Portability and Accountability Act (HIPAA). These rules and regulations must be followed by healthcare institutions to protect patient data and avoid fines and penalties[5].

6. Case Studies and Best Practices

6.1. Successful cybersecurity implementation in healthcare organizations

There are many examples of healthcare organizations successfully implementing cybersecurity measures. The Health Sciences Building at the University of California, San Francisco

(UCSF) is a good example. A robust cybersecurity program now exists at UCSF Health, covering all the bases. Among these are the following: management of vendors and assessments of third-party risks; creation of security policies and procedures; creation of incident response plans; provision of employee training and awareness; use of firewalls and intrusion detection systems; implementation of Security Information and Event Management (SIEM); and establishment of a mechanism for detecting and responding to incidents.

6.2. Lessons learned from cybersecurity incidents

Incidents involving cybersecurity that occur in healthcare enterprises provide opportunities to gain useful insights and learn important lessons. One important takeaway from these incidents is the significance of putting in place a comprehensive cybersecurity program. It is also crucial to remember the relevance of providing workers with training on the most effective best practices for cybersecurity. Conducting incident response strategy .exercises on a regular basis is essential to verify their efficiency

6.3. Best practices for healthcare cybersecurity

Businesses within the healthcare industry have the opportunity to improve their cybersecurity posture by implementing a number of best practices. One of these recommended procedures is the conducting of regular risk assessments. Other practices include the identification and repair of vulnerabilities, as well as the implementation of security policies while also prioritizing the threats posed by cybersecurity attacks[9].

6.4. Future trends and challenges

The healthcare sector's primary concerns revolve around emerging cybersecurity threats. For instance, artificial intelligence (AI) might be employed to craft phishing emails that deceive users more effectively or create malware with enhanced evasion capabilities.

Likewise, quantum computing, an emerging field in computer science, has the potential to break numerous data encryption schemes. This could lead to unauthorized access to healthcare data or disrupt operations. The Internet of Medical Things (IoMT) pertains to internet-connected medical devices. IoMT devices can assist clinicians in patient tracking and treatment. However, it's essential to bear in mind that hackers may attempt to target these devices, potentially exploiting vulnerabilities in IoMT systems, leading to patient data theft or disruptions in hospital operations[4].

Additionally, healthcare cybersecurity technologies are continually evolving to safeguard healthcare facilities from cyber threats. Current healthcare cybersecurity advancements encompass a range of strategies. For example, the analysis of vast amounts of data for cyberattacks, known as "security analytics", can be instrumental. Network and data anomalies often serve as indicators of potential cyberattacks, and security analytics aid healthcare firms in detecting and addressing such anomalies. Machine learning, a subset of artificial intelligence, can apply innovative techniques to enhance safety. Machine learning can lead to the development of more effective malware monitoring systems capable of identifying novel threats. The concept of "zero trust" security emphasizes the lack of trust in anyone or anything regarding security matters. By implementing zero-trust security measures, healthcare firms can proactively prevent cyberattacks by strictly verifying user and device identities and authorizations before granting access to resources[10].

Furthermore, the ever-changing regulatory landscape necessitates the development of new cybersecurity solutions to assist healthcare businesses in safeguarding their systems against cyberattacks. Advances in healthcare cybersecurity encompass several key aspects. Security analytics leverage big data and analytics to detect and mitigate cyber threats. Security analytics in healthcare organizations focuse on identifying network and data abnormalities that may indicate potential cyberattacks. Machine learning, a form of artificial intelligence, has the potential to enhance security solutions. It enables malware detection systems to recognize and respond to emerging threats effectively. Zero trust security, which operates under the assumption that neither humans nor devices can be fully trusted, offers robust protection for healthcare firms. This approach carefully verifies user and device identities and authorizations before granting access to resources, thus fortifying defenses against hackers[2].

6. Conclusion

Due to the sensitive nature of patient information and the increasing integration of technology in the healthcare industry, healthcare enterprises encounter specific cybersecurity challenges. Various cybersecurity prevention techniques are available for healthcare organizations to employ. The solutions mentioned above adopt a comprehensive approach to addressing these security challenges. This approach encompasses risk assessment and management activities, such as identifying vulnerabilities, prioritizing risks, developing incident response plans, providing employee training and awareness, implementing firewalls and intrusion detection systems, utilizing Security Information and Event Management (SIEM) tools, managing vendors and assessing third-party risks, detecting and responding to incidents, and leveraging threat intelligence. Healthcare organizations must exhibit a profound awareness of the growing cybersecurity threats they face in addition to staying updated on the latest advancements in healthcare cybersecurity solutions. Lastly, healthcare institutions should routinely evaluate their cybersecurity programs to ensure alignment with the most current cybersecurity risks and legislation.

7. Acknowledgement

We would like to express our deepest gratitude to Prof. Zaher Kyle, Program Director at the International American University and Dr. Nour Obeidat, Director of Cancer Control Office, Director of Applied Research Unit at KHCC for their guidance and support.

8. Conflicts of Interest

Authors do not have any conflict of interest.

9. Funding

Not applicable

10. References

1. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Health Care, 2017;25: 1-10.
2. Bésenyo J, Kovács AM. Healthcare cybersecurity threat context and mitigation opportunities. Security Science Journal, 2023;4: 83-101.
3. Besenyo J, Krisztina Márton, Ryan Shaffer. Hospital attacks since 9/11: An analysis of terrorism targeting healthcare facilities and workers. Studies in Conflict & Terrorism, 2024;47: 36-59.
4. Saheed YK, Arowolo MO. Efficient cyber attack detection on the

Internet of medical Things-Smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access, 2021;9: 161546-161554.

5. Thamer N, Alubady R. A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. 1st Babylon International Conference on Information Technology And Science, 2021.

6. University of Utah Authors & Marketing and Communication. University of Utah Health data security announcement. University of Utah Health. 2020.

7. Abraham C, Chatterjee D, Sims, RR. Muddling through cybersecurity: Insights from the US healthcare industry. Business Horizons, 2019;62: 539-548.

8. CDC. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Centers for Disease Control and Prevention, 1996.

9. O’Brien N, Martin G, Grass E, Durkin M, Darzi A, Ghafur S. Cybersecurity in healthcare: Comparing cybersecurity maturity and experiences across global healthcare organizations (Preprint). Research Gate 2020.

10. Maurya AK, Kumar N, Agrawal A, Khan RA. Ransomware evolution, target and safety measures. IJCSE, 2018;6: 80-85.