Impact of Cybersecurity Measures in the Healthcare Sector: A Comprehensive Review of Contemporary Approaches and Emerging Trends

Sapna Kumari[1], Priyadarshini Pattanaik[2]

[1]Student of Department of IT Security Management, Arden University, Dessauer Str. 3-5, 10963 Berlin, Germany. Email: sapna.ukot@gmail.com
[2]Faculty of Computer Science and Informatics, Berlin School of Business & Innovation (BSBI), Berlin, Germany

---***---

Abstract - The digital transformation of the healthcare sector has revolutionized operational efficiency and patient care, yet concurrently exposed healthcare organizations to unprecedented cybersecurity risks, jeopardizing patient confidentiality and organizational integrity. This study undertakes a comprehensive investigation into contemporary cybersecurity strategies and emerging trends within the healthcare industry. Through a meticulous examination of published literature from reputable databases, including PubMed/MEDLINE, CINAHL, and Web of Science, critical patterns and vulnerabilities are discerned, underlining the escalating frequency and severity of cyber threats such as ransomware and phishing attacks. Emphasizing the pivotal role of organizational cyber resilience governance and policies, the study identifies a notable gap in standardized cybersecurity risk assessment methodologies, signaling the urgent need for innovative approaches. In response to identified challenges, the research proposes the development of novel methodologies to fortify cybersecurity defenses and protect patient data. Leveraging cutting-edge technologies such as blockchain and artificial intelligence, the study advocates for proactive measures to mitigate emerging threats and ensure data security and patient privacy in healthcare environments. Moreover, the integration of end-to-end security measures and the adoption of DevOps methodologies are highlighted as promising avenues for enhancing cybersecurity resilience. Results from a systematic literature review underscore the imperative for ongoing research and collaboration to address cybersecurity challenges in healthcare effectively. By offering insights into key cybersecurity features, technologies, and responsibilities within the healthcare sector, this study aims to inform stakeholders and policymakers, facilitating the implementation of robust cybersecurity measures. Furthermore, the study presents key findings regarding the current state of cybersecurity in healthcare, including challenges faced and potential solutions identified through the research process. Ultimately, through concerted efforts and the utilization of innovative strategies, healthcare organizations can navigate the evolving cybersecurity landscape, safeguarding patient information and upholding the integrity of healthcare systems.

Key Words: Healthcare cybersecurity, Internet of Things, blockchain, artificial intelligence, patient data protection, Cyber threats, innovative approaches

1. INTRODUCTION

Protecting the privacy of patient data and enabling the effective management of medical operations depend significantly on the security of our healthcare systems. The more digital technology is being integrated into healthcare, the greater the industry is exposed to cyberattacks. As a result, cybersecurity plays an essential part in safeguarding our networks, systems, and programs from online threats, stopping illegal access, and avoiding the disturbing consequences caused by data breaches. It is about building a strong defense to maintain our healthcare landscape safe and sound. The security of our healthcare systems is critical to ensuring that our medical procedures are carried out efficiently and that patients' personal information remains private. It all comes down to ensuring that personal information is secure and that our medical processes proceed as usual. The risk of cyber accidents has significantly increased as more digital technology has been integrated into our healthcare systems [1].

The risk of cyber-attacks has significantly increased as our healthcare systems use more digital technology. for protecting our systems, and all the networking systems from cyber-attacks, and avoiding all illegal access, along with different scenarios of data breaches, the significance of cybersecurity cannot be emphasized. It's an essential step in protecting the privacy and confidentiality of our healthcare system. It is about building a strong defense to maintain our healthcare landscape safe and sound. Since the healthcare industry has valuable data and frequently insufficient defenses, it is a prime target for cybercrime. Cybersecurity incidents, which include ransomware attacks and health information theft, risk patient privacy, cause disruption to healthcare systems, and maybe even put lives at risk. Despite its pivotal role in patient safety, the historical deficiency of cybersecurity in healthcare necessitates a transformative shift [2].

To provide a complete and efficient cybersecurity solution intended for the healthcare sector, this transition includes changes in human behaviour, advances in technology, and procedure modifications. To address the difficulties the healthcare industry suffers in maintaining patient safety when faced with the threat of cyberattacks, a concerted effort has been made to smoothly implement the latest developments in cybersecurity and innovative technologies into practice. This proactive approach strives to furnish a more secure and robust solution. Also, enforcing and making new regulations, and rules to create a legal system to monitor and direct healthcare organizations to prioritize and make efforts to protect patient safety and well-being can significantly impact the preventative measure [3] [18].

Healthcare organizations maintain sensitive databases containing patient data, medical history, personal information, and transaction history. If these databases were to fall into the wrong hands, patients could be seriously at risk of identity theft, medical fraud, and data misuse. Transaction details could also be compromised, with potential legal repercussions that could harm medical institutions. Cybersecurity can therefore offer a safeguard system to prevent any fallout and put patient privacy at risk to counteract this security breach. [10].

- **Medical Device Security:** Cybersecurity can be an effective means of ensuring more secure use of medical equipment. Malware and cyberattacks with unauthorized access might threaten patient safety, so medical devices must be handled securely [4] [27].
- **Operational Continuity:** The uninterrupted functioning of healthcare operations depends on a secure and dependable system that operates without any delays. Cybersecurity can be leveraged to manage and supply a dependable system that functions effectively, as delays in patient care or even pose a threat to life [4].

Privacy breaches were a concern before the era of digital health records, but new vulnerabilities are introduced by the current interconnectivity of records. Modern records provide several entry points for possible access, enabling remote entry (unlike the protected paper records in hospitals).

Therefore, it becomes crucial to establish awareness and training programs specific to healthcare professionals. Emphasizing human efforts in enhancing system security is crucial, as human behaviour plays a significant role in defending against cyberattacks and responding to them. This involves executing strong security protocols, following standards, and actively reducing the possibility of security breaches, particularly considering the enormous value of data, such as medical records and financial transactions handled by healthcare facilities. Adopting end-to-end encryption techniques and incorporating AI advancements are critical to strengthening cybersecurity [11] [6].

Hospital and security records, for example, often contain a significant amount of private information, including names, dates of birth, social security numbers, addresses, and credit card information. Because healthcare data has more value on the black market than data from other industries, hackers are drawn to healthcare organizations. Interestingly, electronic health records (EHRs) are worth tens to hundreds of times more on black market exchanges than credit card data. Cybersecurity incidents increase the financial difficulties the healthcare industry is already facing, dealing with higher expenses and narrower profit margins when compared to other industries. Cybersecurity is a serious threat to patient safety in addition to worries about patient privacy and the financial burden on the healthcare industry. The complex consequences of insufficient cybersecurity in healthcare organizations are highlighted by the fact that cybersecurity protocols could be compromised, compromising the health of patients [11].

1.1 Major Cybersecurity Breaches in Healthcare

1.1.1 Cyberattack Disrupts US Hospital Systems (August 4, 2023)

The study by [12] investigated a ransomware attack associated with a record-breaking cybersecurity compromise that occurred in the U.S., healthcare organizations were affected, peaking with frequency in August 2023. A targeted attack is carried out by the ransomware group BlackCat or in other words, 'daylight' which interrupted hospital computer systems and forced emergency rooms to shut down due to closure while ambulances got diverted. This massive threat led to over 1500 hospitals and healthcare clinics being attacked including leading health systems such as Community Health Systems Universal Health Services and HCA Healthcare.

Critical interventions in healthcare provision such as surgeries, treatments, and appointments will be disrupted. The threat to compromise confidential patient data that includes personal information, medical records as well as billing details. Large financial losses were incurred through ransom payment, loss of earnings, and repair damages costs. Potential adverse harm to patients, complications, and deaths due to late or inappropriate care. Major losses and deterioration of reputation, credibility for hospitals as well as their applied leadership [12].

1.2 NHS Ransomware Attack (August 11, 2022)

An attack organized by the Quantum group in August 2022 was one of the biggest security ransomware attacks that threatened at National Health Service (NHS) operation in December. This assault impacted over 200 medical facilities and clinics, resulting in disruptions to the patient care of more than a hundred patients while cancelling appointments, surgeries, and therapies. In the attack, quantum used a phishing email to trick staff into opening an infectious attachment that encrypted vital files. The amount that the criminals demanded was £10 million in bitcoin, and they threatened to erase all info by deleting it from their hard drives unless the ransom was paid within 48 hours [8].

Cancellation of appointments, surgeries, and treatments due to interruption in critical healthcare services. Leaking of sensitive data about patients, such as names, addresses medical history, and test results. Significant financial losses resulting from ransom demands, foregone revenue, and recovery costs. Risk to patient safety, complications, and death associated with the delay or inappropriate care delivery. Sustained damage to the reputation and trust of healthcare entities, institutions, staff, and providers [8].

This research aims to draw focus on the present cyber security issues facing the healthcare sector and to suggest current strategies for protecting infrastructure and data. This study also aims to provide recommendations for best security practices and address new cybersecurity trends in the healthcare industry. The main objectives of this paper are mentioned as follows.

1) To investigate cybersecurity and the role it plays in healthcare.
2) To explore key cybersecurity features and technologies for the healthcare industry.
3) To investigate various cybersecurity responsibilities in the healthcare industry.
4) To pinpoint important cybersecurity applications in the healthcare industry.
5) To develop effective strategies for mitigating cyber security threats within the healthcare industry.

Research Questions

R01: What are the cyber security challenges of the healthcare sector?
R02: What are the current approaches and applications of cyber security in the healthcare sector?
R03: What are the new methods that can be used to ensure the security of data and privacy of patients in the healthcare sector?
Section 1 offers a concise introduction to cybersecurity and its role in healthcare. It provides a comprehensive overview of the importance of cybersecurity in safeguarding healthcare systems against cyber threats. The section highlights the growing risks of cyberattacks and emphasizes the need to adopt the latest security protocols to counter such threats effectively. Section 2 conducts a review of existing literature on the uses of cybersecurity in the healthcare sector.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

2. REVIEW WORK

The healthcare sector has adopted digital technologies that pose numerous cybersecurity challenges. This literature review examines new approaches and directions for improving cybersecurity in healthcare. Factors that are considered in the evaluation include legal environment, insurance impact, human factors, technology innovations, trends, and threats. The evaluation considers several factors, such as the legal environment, insurance implications, human factors, technological advancements, trends, and threats.

Healthcare cybersecurity is constantly being updated because of several relevant contemporary threats. [9] provided a thorough assessment of the state cybersecurity healthcare industry. Their objectives included finding actionable resolutions and understanding the transforming forms of cyber threats. The difficulties healthcare organizations have safeguarding private data are clarified by this study. Likewise, [10] offers significant perspectives on contemporary developments and methodologies in healthcare cybersecurity. Their research explores the problems, strategies, and innovations in technology that are reshaping cybersecurity. Through the emphasis on these components, the study offers a complex viewpoint on strategies and assets that healthcare organizations can utilize to strengthen their cybersecurity. In their paper, propose a novel approach to automated cybersecurity measures. Using cutting-edge methods, they present an automated cybersecurity attack detection approach for healthcare systems. This emphasizes how crucial advanced detection algorithms are to enhancing healthcare systems' cybersecurity. Healthcare organizations can effectively mitigate risks and address vulnerabilities proactively by implementing automated threat identification. A thorough summary of current trends, security threats, and possible solutions in the healthcare sector can be found in [11] narrative review. Issues including ransomware attacks, data breaches, and malfunctions in medical equipment are all discussed in the article.

Further, it provides proactive steps to reduce cybersecurity risks by ensuring that healthcare providers and their organizations are aware of new threats and have the potential to implement strong security measures.[13] highlight the challenges posed by human behavior in cybersecurity, suggesting a paradigm shift towards security measures that are more people focused. [14] argues that cybersecurity issues stem from unrealistic requirements imposed by system design and promote a strategy sensitive to human behavior. [15] emphasizes the importance of customized training and education to reduce cyber risks by identifying high-risk users and providing them with the necessary tools. These viewpoints underscore the necessity of a human-centric strategy when tackling cybersecurity issues, creating a safer digital environment.

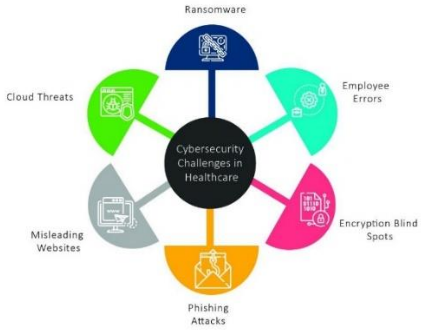


Fig 2.1. Risks associated with the healthcare industry [16]

The author emphasizes how crucial it is to consider elements like an organization's online presence, the kind of information it manages, and the scope of its patients. These elements are crucial in deciding the cost, conditions, and scope of cyber insurance plans. The dynamic and quickly changing nature of cyber threats makes customization even more difficult, so insurance providers must keep up with the most recent risks and vulnerabilities. The interdependence of risks and concerns about moral hazard are two important aspects of cyber risk and insurance that [17] address to add to the conversation. The authors identify potential obstacles to the wider adoption of cyber insurance as the dependency and the correlation of cyber risks. Because many systems have similar designs and share common components, they are vulnerable to similar kinds of losses, which leads to their interdependence.

Intentional cyberattacks are subject to a complicated legal environment in the quickly developing world of cyberspace. The complexity of this environment is clarified by [3], who highlight the lack of an international body responsible for regulating cyberspace. When it comes to handling cyber threats that cut across national boundaries, this gap in global governance presents serious difficulties. Payne draws attention to the idea of state authorization, pointing out that states can freely bind themselves to duties by express or implicit consent. In the lack of a formal international legal body, legal obligations arise from both explicit consent—signing a treaty, for example—and implicit consent—living up to general legal and customary principles. In this framework, intentional cyberattacks are compared to established legal principles, like the rule against using force and the non-intervention principle. It is complicated and far from straightforward to analyze these cyberattacks considering the laws currently in place. Payne's research raises important questions regarding matters such as sovereignty over territory in digital spaces and highlights the difficulties in translating standard legal principles to the ambiguous world of the internet. In conclusion, the legal landscape surrounding cyber risks is still complex, with issues stemming from the lack of a centralized regulatory authority, the difficulty of applying conventional legal standards to cyberattacks, and the challenge of controlling the global impact of the digital world. International organizations' efforts to bridge this regulatory gap highlight the continuing search for a strong legal framework that can handle the complex aspects of cybersecurity in healthcare globally [3].

As with the growing adoption of IoT-based systems in healthcare systems, there is a need for research and investigation into security risks and privacy concerns. Medical equipment can be more secure and reliable through more focused research and briefly overlooked challenges and risks. Recent studies have conducted the healthcare technology and data privacy, which form an environment full of challenges ranging from both public policy to industry relations. [18] delve into the realm of intelligent healthcare systems and investigate the potential of deep learning methods to bolster their security. Deep learning, a subset of artificial intelligence, has proven to be an effective tool in identifying complex patterns and anomalies within vast datasets. By leveraging this technology, healthcare systems can more accurately detect and prevent security breaches, ultimately safeguarding sensitive patient information [18]. The goal of Thilagam et al.'s [18] integration of algorithms based on deep learning into healthcare frameworks is to improve the system's capacity to identify and stop possible security breaches. Ali et al. [19] concentrate on the incorporation of blockchain-based technologies into intelligent healthcare systems in an additional way.

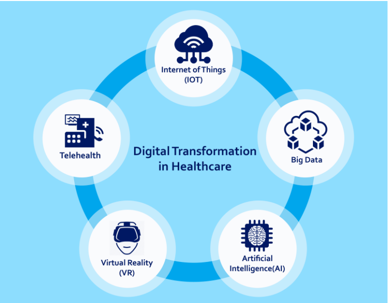

Internet of Things (IOT)
Telehealth
Digital Transformation in Healthcare
Big Data
Virtual Reality (VR)
Artificial Intelligence(AI)

Fig 2.2. Digital Healthcare Transformation [26].

The rapid implementation of digital health services has been catalyzed by the pandemic, underscoring the benefits for both healthcare providers and patients. However, this swift adoption has also increased the vulnerability of the healthcare industry to cyberattacks. With the proliferation of digital health data on the dark web, cybersecurity threats have escalated, with ransomware attacks expected to quadruple by 2021 [23]. Hospital administrators are realizing more and more how important it is to safeguard patient data, but in comparison to other industries, the healthcare sector invests very little money in cybersecurity. As cyberattacks pose serious operational risks, matching cybersecurity measures with healthcare system vulnerabilities is crucial for maintaining the integrity and resilience of global healthcare systems [24] [25].

The final section discusses new cybersecurity risks in the healthcare sector, emphasizing ransomware and malware's ability to infect the sector. Considering potential disruptions to patient care, disaster response, and public health protection, the review highlights the critical gap in preparedness for ransomware attacks. Realizing the seriousness of these new threats, it exhorts healthcare organizations to strengthen defenses against low-probability, high-impact events. The literature review highlights the necessity for continued research and preventative measures to secure sensitive healthcare data by offering an extensive overview of the complex issues and modern solutions in healthcare cybersecurity. However, there is a significant lack of research on how healthcare organizations can effectively tackle cybersecurity challenges. As a result, this study aims to fill this gap by exploring the role of cybersecurity in healthcare and suggesting practical strategies to mitigate cyber threats. By exploring key cybersecurity features, technologies, and responsibilities within the healthcare industry, the study seeks to provide insights into enhancing cybersecurity practices tailored to the unique needs of healthcare organizations. Furthermore, this research will focus on developing effective measures to address the interdependence of cyber risks, the challenges in underwriting cyber insurance policies, and the changing legal environment related to ethical risks and cyber threats in healthcare. The main goal of this study is to improve cybersecurity practices in the healthcare industry by addressing the existing gaps. The study aims to safeguard sensitive healthcare data and provide recommendations for best security practices that can be implemented. The ultimate objective of this project is to contribute to the ongoing efforts to strengthen cybersecurity in the healthcare sector.

3. RESEARCH METHODOLOGY

In this section, we outline the various sources of secondary data utilized for the systematic literature review on cybersecurity within the healthcare sector. The data analysis involves sample articles and research papers obtained from both general and specialized databases renowned for their extensive coverage of scholarly literature in cybersecurity and healthcare.

3.1 General Databases:

- ✓ **Google Scholar:** Google Scholar is a well-known academic search engine. It also catalogs books, conference papers, and other scholarly works including articles. The Internet resource covers many disciplines like cyber security and medical care.
- ✓ **SCOPUS:** SCOPUS is a multidisciplinary database covering patents, trade publications, conference proceedings, and scholarly journals. In this way, it offers extensive literature coverage in healthcare and cybersecurity facilitating comprehensive analysis of research in these areas.

3.2 Specialized Databases:

- ✓ **JSTOR:** JSTOR is an online resource that preserves academic publications, books, and original materials from various fields. It provides access to a huge library of peer-reviewed literature, which includes publications about healthcare and cybersecurity.
- ✓ **ERIC (Education Resources Information Centre):** A popular database called ERIC indexes materials from journals, research reports, conference papers, and other sources that are relevant to education. ERIC covers research pertinent to cybersecurity awareness and training in healthcare education programs, despite its primary focus being on education.

3.3 Bibliographic Databases

The search strategy involved querying three bibliographic databases known for their extensive coverage of healthcare-related literature:

- ✓ **PubMed/MEDLINE:** The National Library of Medicine maintains PubMed, a free search engine that provides access to the MEDLINE database of biomedical literature. It offers thorough coverage of research on healthcare, including sections on cybersecurity problems that have an impact on the industry.
- ✓ **The CINAHL, or Cumulative Index to Nursing and Allied Health Literature:** Indexing publications on nursing and allied health, the CINAHL is one of the unique or specialized databases. It consists of articles from medical journals, nursing journals, and related fields that provide insightful data on cybersecurity problems faced by healthcare professionals.
- ✓ **Web of Science (WoS):** The recognized literature in various disciplines is indexed by cross-disciplinary citation database Web of Science. It provides scholarly resources, conference proceedings, and research papers of the best quality, thus allowing us to examine

in detail cyber security trends in the healthcare industry.

Eight different search strings were used throughout the chosen databases during the search process. For collaborative filtering, the search results have been exported from each of the platforms and imported into the "Rayyan" platform. Rayyan provides features like blind review, which reduces the possibility of bias by guaranteeing that the results are hidden from other researchers while they are being analyzed. Every imported result from WoS, CINAHL, and PubMed was examined separately using the preset inclusion and exclusion standards listed in the methodology section.

The techniques of search applied in the current study were specifically designed to ensure that national and international cybersecurity healthcare states are fully comprehended. This study aimed to recognize the main tendencies and research directions by a systemic search through several bibliographic databases using appropriate keywords and queries. The purpose of this method is to obtain an abundance of articles on cybersecurity in the current healthcare industry and to help readers get the overall picture of it. Eight different individual search queries were constructed for the search performed that were all distinct to select out the different sub-topics of the cybersecurity problem in the healthcare industry. They mentioned a wide range of subjects related that needed to be covered, including organizational policies, social engineering, cybersecurity awareness, and its risks.

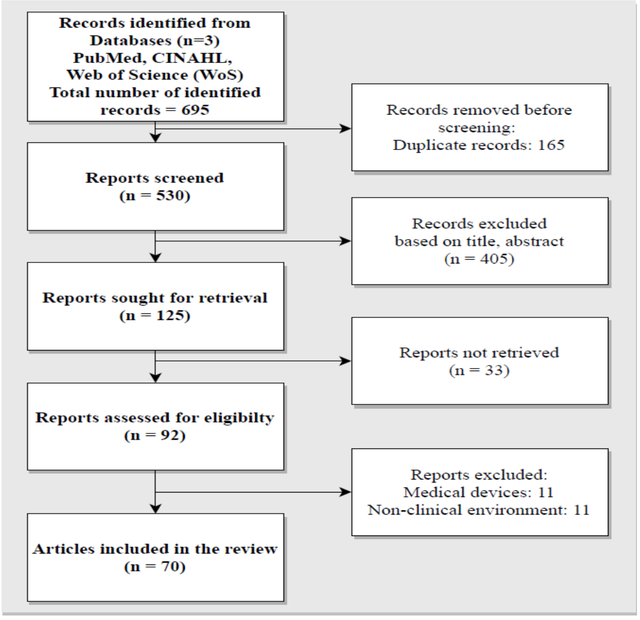

Records identified from Databases (n=3) PubMed, CINAHL, Web of Science (WoS) Total number of identified records = 695
Records removed before screening: Duplicate records: 165
Reports screened (n = 530)
Records excluded based on title, abstract (n = 405)
Reports sought for retrieval (n = 125)
Reports not retrieved (n = 33)
Reports assessed for eligibilty (n = 92)
Reports excluded: Medical devices: 11 Non-clinical environment: 11
Articles included in the review (n = 70)

Fig 3.1: A Brief Overview of the Process of Finding Literature

Figure 3.1 shows a graphic depiction of the literature search procedure. This example shows how a methodical approach was used to find, evaluate, and choose pertinent articles to include in the systematic review.

Three well-known bibliographic databases were searched throughout: the Web of Science (WoS), CINAHL (Cumulative Index to Nursing and Allied Health Literature), and PubMed®/MEDLINE. A wider range of multidisciplinary research was accessible through the Web of Science, while PubMed and CINAHL were chosen due to their extensive coverage of the literature on health topics.

The eight queries used in the search were as follows:

Query 1: Human-related Cybersecurity Training
MeSH Terms: Human
Keywords: Cybersecurity, training, Information security awareness
Filters: Articles published from 2010 to 2021, English language
Search Strategy: MeSH term for "Human" combined with TIAB searches for specified keywords.

Query 2: Human-related Cybersecurity Awareness
MeSH Terms: Humans
Keywords: Cybersecurity, security awareness, Information security awareness
Filters: Articles published from 2010 to 2021, English language
Search Strategy: MeSH term for "Humans" combined with TIAB searches for specified keywords.

Query 3: Cybersecurity Awareness in Healthcare
Keywords: Cybersecurity, human-related awareness, healthcare
Filters: Articles published from 2010 to 2021, English language
Search Strategy: Combination of keywords related to "Cybersecurity," "human," "awareness," and "healthcare."

Query 4: Social Engineering and Organizational Policy in Healthcare Cybersecurity
Keywords: Healthcare, social engineering, Organizational policy, cybersecurity
Filters: Articles published from 2010 to 2021, English language
Search Strategy: Combination of keywords related to "Healthcare," "social engineering," "Organizational policy," and "cybersecurity."

Query 5: Cybersecurity and Social Engineering in Healthcare
Keywords: Cybersecurity, social engineering, healthcare professionals
Filters: Articles published from 2010 to 2021, English language
Search Strategy: Combination of keywords related to "Cybersecurity," "social engineering," and "healthcare professionals."

Query 6: Cybersecurity Training and Awareness in Healthcare
Keywords: Cybersecurity, Healthcare, social engineering, training, awareness
Filters: Articles published from 2010 to 2021, English language
Search Strategy: Combination of keywords related to "Cybersecurity," "Healthcare," "social engineering," "training," and "awareness."

Query 7: Healthcare Training and Awareness in Cybersecurity
Keywords: Healthcare, Cybersecurity, training, awareness
Filters: Articles published from 2010 to 2021, English language
Search Strategy: Combination of keywords related to "Healthcare," "Cybersecurity," "training," and "awareness."

Query 8: Comprehensive Search String
Keywords: Cybersecurity*, Awareness, Healthcare
Filters: Articles published from 2010 to 2021, English language
Search Strategy: Predefined search string combined with language and document type filters, conducted across multiple indexes.

These research questions were thoughtfully designed to ensure relevance to the study's goals while focusing on cybersecurity and healthcare concepts. The search sought to retrieve articles that met the predetermined criteria by utilizing TIAB (Title/Abstract) searches, MeSH (Medical Subject Headings) terms, and language and document type filters.

The number of articles returned for each search query determined the variation in the search query results. For instance, query 2 yielded 217 articles while query 1 only produced 17. The most comprehensive search, query 8, yielded 221 articles from the Web of Science repository. A total of 695 articles were returned for all queries.

To conduct a systematic review, it is crucial to establish specific inclusion and exclusion criteria for selecting relevant literature. These criteria act as a filter, ensuring that the studies included in the review meet the objectives and significantly contribute to the evidence synthesis. The study's inclusion and exclusion criteria were applied systematically and comprehensively to facilitate an organized and thorough filtering process.

1) Inclusion Criteria:

1. **Articles on Cyber Threats/Attacks:** Studies that detail cyber threats or attacks directed towards hospitals and other clinical settings fall under this criterion. The nature and consequences of cybersecurity breaches in the healthcare industry are discussed in these articles, which add to our understanding of the difficulties that healthcare organizations confront.
2. **Identification of Vulnerabilities:** This criterion includes studies pinpointing weaknesses cybercriminals exploit. Comprehending these vulnerabilities is imperative to formulate efficacious cybersecurity tactics and alleviate hazards to patient information and healthcare infrastructure.
3. **Organizational Cybersecurity Risk Assessment:** Research on organizational cybersecurity risk assessment in healthcare settings is included in this criterion. These studies provide insightful information about the procedures and approaches used to evaluate and control cybersecurity risks, helping healthcare organizations develop best practices.
4. **National Case Studies:** This criterion includes articles that discuss national case studies focusing on cyber defense tactics. National case studies facilitate comparative analyses and the identification of broad trends by offering context-specific insights into cybersecurity challenges and responses at the national level.

2) Exclusion Criteria:

1. **Irrelevance to Research Questions:** Excluded studies do not directly address the research questions that formed the framework for the systematic review. This criterion makes sure that the literature chosen for analysis closely matches the goals of the research, which improves the review's relevance and coherence.
2. **Language Limitation:** Articles composed in languages other than English are not considered. This criterion guarantees accessibility for the research team while facilitating effective data extraction and analysis.
3. **Duplicate Studies:** Excluded studies are those that have been published before to avoid duplication and expedite the review process. The analysis and apparent volume of evidence may be distorted by duplicate studies, jeopardizing the review's objectivity.
4. **Lack of Relevance to Clinical Environments:** Excluded from consideration are studies that have no direct connection to hospitals or other clinical settings. This criterion guarantees that the literature chosen for examination concentrates exclusively on cybersecurity issues and their resolutions in healthcare environments.
5. **Focus on Medical Devices:** Articles that only address medical device cybersecurity are not accepted. Although crucial, this review's focus is on more general organizational cybersecurity issues in the healthcare industry; it does not address the cybersecurity of medical devices.
6. **A Focus on Medical Device Patient Safety:** Research that primarily addresses patient safety concerns with medical devices and relevant cybersecurity technologies is not considered. While patient safety is a critical component of healthcare cybersecurity,

articles that solely address this topic are not included in this review.

7. **Technical Development without Healthcare Professional Involvement:** Research that only discusses technological advancements (software, algorithms, etc.) without consulting medical experts is not included. By using this criterion, it is ensured that the literature chosen for analysis addresses cybersecurity challenges from the practitioner's perspective and is directly relevant to the healthcare context.

Cooperation among healthcare stakeholders is paramount in solving cybersecurity issues and exchanging best practices. Healthcare companies should collaborate with government departments, business associates, cybersecurity suppliers, and universities to share lessons learned, exchange threat intelligence, and create cooperative projects aimed at enhancing cybersecurity resilience. Establishing industry-wide cybersecurity standards and certification programs ensures uniformity and interoperability among healthcare organizations.

3.3.1 Technical Recommendations:

- ✓ **Implement Robust Access Controls:** Healthcare organizations need to implement a least-privilege access model. This model restricts user access to only the resources and data necessary to perform their job duties. Role-based access controls (RBAC) can be used to assign permissions based on defined roles and responsibilities. This ensures that users only have the necessary privileges to perform their duties. Additionally, advanced authentication mechanisms such as biometrics, smart cards, or token-based authentication can be used to enhance access controls and prevent unauthorized access to sensitive systems and data. Continuous monitoring and auditing of access logs can help in identifying and preventing unauthorized access attempts. This allows organizations to respond promptly to potential security incidents and minimize the risk of data breaches.
- ✓ **Encryption of Data:** Healthcare organizations have a responsibility to protect sensitive data from unauthorized access or disclosure. One way to do this is by encrypting such data using strong encryption algorithms like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman), both at rest and in transit. This ensures that even if data is intercepted or compromised, unauthorized parties cannot read or use it. Additionally, organizations should implement key management practices to securely store and manage encryption keys, thereby ensuring that only authorized personnel can access and decrypt such data as needed. It is also important for organizations to conduct regular encryption audits and compliance checks to ensure that encryption policies and procedures are being followed and that encryption mechanisms remain effective.

The distribution of publications categorized by year of publication is as follows:

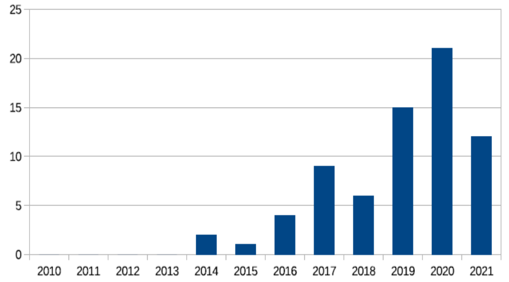
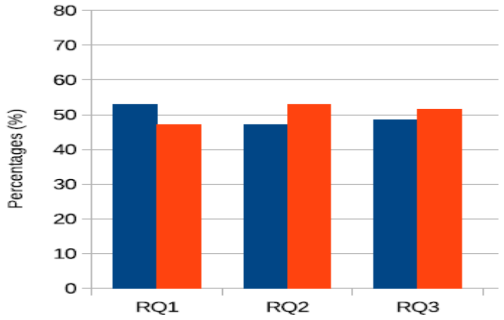


Fig 4.1: The selected 70 articles grouped by year of publication.

- ➢ Percentage of published articles related to the Research



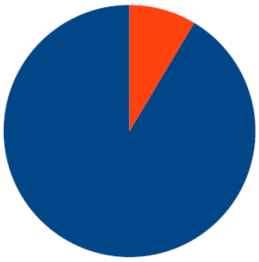
> 60% 🟦 relevance
< 50% 🟧 relevance

Fig 4.2: Illustrates the relevance of articles in addressing the research questions.

After discussing the distribution of publications by year, it is essential to examine the relevance of the articles in addressing the research questions posed in the study. Fig 4.2 provides a graphical representation of the percentage of published articles categorized based on their relevance to the research questions.

Upon analysis of Fig 4.2, it is evident that a significant proportion of the published articles, over 60%, demonstrate high relevance to the research questions. This indicates that a substantial portion of the existing literature effectively addresses the key objectives and inquiries outlined in the study. These articles offer valuable insights, analyses, and findings that contribute to advancing knowledge and understanding in the field of patient privacy and data security in healthcare. Conversely, there is a smaller percentage of articles, less than 50%, that exhibit lower relevance to the research questions. Overall, Figure 4.2 emphasizes the importance of determining the relevance of published articles in answering research questions. By identifying and prioritizing sources that are closely related to the study's objectives, researchers can ensure the quality and rigor of their research findings, ultimately contributing to the advancement of knowledge and understanding in the field of healthcare cybersecurity.

➢ Percentage of publication in journal/ conference included in Research review.



🟦 Journal (91.43%) 🟧Conferences (8.57%)

Fig 4.3: The distribution of article types among the 70 publications included in the systematic review consists of 6 conference papers and 64 journal papers.

In addition to determining the relevance of articles to research questions, it is critical to examine the distribution of publication types among the articles included in the systematic review. Figure 4.3 depicts the percentage of journal and conference papers included in the review. According to Fig 4.3, the majority of publications included in the systematic review are journal papers, accounting for approximately 91.43% of the total. This indicates that a substantial portion of the literature relevant to the research questions is published in peer-reviewed journals. Journal papers are often considered to undergo rigorous peer review processes, which enhance the credibility and reliability of the research findings presented in these publications.

Using ranking metrics makes it possible to assess articles' relevance and correlation to the main goals of the research in a more sophisticated way. Using this method, the systematic literature review becomes more robust and reliable, and only highly relevant and influential research is incorporated into the analysis. Additionally, the application of ranking metrics makes the evaluation process transparent and methodical, allowing researchers to recognize and rank the articles that have the greatest impact on the body of knowledge regarding cybersecurity in healthcare.

4. CONCLUSIONS

The healthcare sector is going through a major digital revolution, utilizing technology to increase operational effectiveness, improve patient care, and facilitate professional communication. However, this change has also made healthcare organizations more vulnerable to various cybersecurity risks, compromising patient confidentiality and organizational integrity. Our study has thoroughly examined the cybersecurity issues facing the healthcare industry, emphasizing how important it is to have strong cybersecurity defenses. Our thorough examination of published literature from reliable databases, including PubMed/MEDLINE, CINAHL, and Web of Science, has allowed us to recognize important patterns and weaknesses that healthcare organizations must deal with. The growing industry recognition of cybersecurity's importance is demonstrated by the increasing frequency of research publications about cybersecurity. Attacks using ransomware and phishing have become major concerns, highlighting the vulnerabilities present in healthcare systems.

To protect patient data and organizational integrity, our research concludes that it is vitally important to advance cybersecurity measures in the healthcare industry. To create and execute successful cybersecurity strategies, stakeholders—including technology vendors, legislators, and healthcare providers—must work together. By addressing current problems and leveraging technological advancements, healthcare organizations can lower the risk of cyberattacks and continue to provide safe and effective patient care in the digital age.

REFERENCES

[1]. Cartwright, A.J., 2023. The elephant in the room: cybersecurity in healthcare. Journal of Clinical Monitoring and Computing, pp.1-10.

[2]. Kiser, S. and Maniam, B., 2021. Ransomware: Healthcare industry at risk. Journal of Business and Accounting, 14(1), pp.64-81.

[3]. Payne, B.K., He, W., Wang, C., Wittkower, D.E. and Wu, H., 2021. Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course. Journal of Information Systems Education, 32(2), pp.134-149

[4]. Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. and Bonacina, S., 2021. Influence of human factors on cyber security within healthcare organizations: A systematic review. Sensors, 21(15), p.5119.

[5]. Martin, G., Martin, P., Hankin, C., Darzi, A. and Kinross, J., 2017. Cybersecurity and healthcare: how safe are we? *Bmj*, *358*.

[6]. Garcia-Perez, A., Cegarra-Navarro, J.G., Sallos, M.P., Martinez-Caro, E. and Chinnaswamy, A., 2023. Resilience in healthcare systems: Cyber security and digital transformation. Technovation, 121, p.102583.

[7]. Dameff, C., Tully, J., Chan, T.C., Castillo, E.M., Savage, S., Maysent, P., Hemmen, T.M., Clay, B.J. and Longhurst, C.A., 2023. Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Network Open*, *6*(5), pp.e2312270-e2312270.

[8]. MacColl, J., Hüsch, P., Mott, G., Sullivan, J., Nurse, J.R., Turner, S. and Pattnaik, N., 2024. Ransomware: Victim Insights on Harms to Individuals, Organisations and Society.

[9]. 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. https://doi.org/10.3233/THC-161263

[10]. Javaid, M., Haleem, A., Singh, R.P., & Suman, R. (2023). Cyber Security and Applications.

[11]. Coventry, L. and Branley, D., 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturates, 113, pp.48-52.

[12]. Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. and Dameff, C., 2020. Healthcare challenges in the era of cybersecurity. Health security, 18(3), pp.228-231.

[13]. Pfleeger, S.L. and Caputo, D.D., 2012. Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), pp.597-611.

[14]. Schneier, B., CORPORATE SECURITY THREATS WITHIN THE COMMUNICATION ASPECT. Nauka i tehnologija, p.69.

[15]. Korpela, K., 2015. Improving cyber security awareness and training programs with data analytics. Information Security Journal: A Global Perspective, 24(1-3), pp.72-77.

[16]. Biener, C., Eling, M. and Wirfs, J.H., 2015. Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance-Issues and Practice, 40, pp.131-158.

[17]. Baer, W.S. and Parkinson, A., 2007. Cyberinsurance in its security management. IEEE Security & Privacy, 5(3), pp.50-56.

[18]. Geetha, R. and Thilagam, T., 2021. A review on the effectiveness of machine learning and deep learning algorithms for cyber security. Archives of Computational Methods in Engineering, 28, pp.2861-2879.

[19]. Ali, A., Rahim, H.A., Pasha, M.F., Dowsley, R., Masud, M., Ali, J. and Baz, M., 2021. Security, privacy, and reliability in digital healthcare systems using blockchain. Electronics, 10(16), p.2034.

[20]. Kumar, S., Biswas, B., Bhatia, M.S. and Dora, M., 2021. Antecedents for enhanced level of cyber-security in organisations. Journal of Enterprise Information Management, 34(6), pp.1597-1629.

[21]. Kute, S.S., Tyagi, A.K. and Aswathy, S.U., 2022. Security, privacy and trust issues in internet of things and machine learning based e-healthcare. Intelligent Interactive Multimedia Systems for e-Healthcare Applications, pp.291-317.

[22]. Drew, J., 2012. Managing cybersecurity risks. Journal of Accountancy, 214(2), p.44.

[23]. Williams, C.M., Chaturvedi, R. and Chakravarthy, K., 2020. Cybersecurity risks in a pandemic. Journal of medical Internet research, 22(9), p.e23692.

[24]. Morgan, G. and Gordijn, B., 2020. A care-based stakeholder approach to ethics of cybersecurity in business. The ethics of cybersecurity, 21, pp.119-138.

[25]. Weber, K. and Kleine, N., 2020. Cybersecurity in health care. The Ethics of Cybersecurity, 21, pp.139-156.

[26]. Pranggono, B. and Arabo, A., 2021. COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 4(2), p.e247.

[27]. Thamer, N. and Alubady, R., 2021, April. A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In 2021 1st Babylon International Conference on Information Technology and Science (BICITS) (pp. 210-216). IEEE.

[28]. Montasari, R., 2023. Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom. Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity, pp.7-25.

[29]. Thomasian, N.M. and Adashi, E.Y., 2021. Cybersecurity in the internet of medical things. Health Policy and Technology, 10(3), p.100549.

Appendix:

LIST OF ABBREVIATION

PubMed	Public Medline
MEDLINE	Medical Literature Analysis and Retrieval System Online
CINAHL	Cumulative Index to Nursing and Allied Health Literature
IT	Information Technology
DevOps	Development Operations
DevSecOps	Development Security Operations
ICT	Information and Communication Technology
AI	Artificial Intelligence
ML	Machine Learning
NLP	Natural Language Processing
IoT	Internet of Things
EDR	Endpoint Detection and Response
COVID	Coronavirus Disease
EHRs	Electronic Health Records
U. S	United States
HCA	Healthcare Assistant
NHS	National Health Service
HIPAA	Health Insurance Portability and Accountability Act
GDPR	General Data Protection Regulation
PHI	Protected Health Information
SCOPUS	Scientific Citation Index Expanded
JSTOR	Journal Storage
ERIC	Education Resources Information Centre
WoS	Web of Science

BIOGRAPHIES

Sapna Kumari, an IT enthusiast with a strong background in Computer Systems and a specialization in IT Security Management. She completed my bachelor's in computer systems, where she honed technical skills in software development, system architecture, and networking. Recently, she has taken her passion for technology a step further by earning my Master's in IT Security Management, focusing on cybersecurity, risk assessment, and safeguarding digital assets.

Dr. Priyadarshini Pattanaik is currently a Lecturer at the Berlin School of Business and Innovation, specializing in quantitative analysis and artificial intelligence. She is expert in deep neural networks for visual computing, with a focus on medical image analysis and disease detection. Conducted advanced research in France at IMT Atlantique and Telecom Sudparis on microscopy reconstruction and musculoskeletal joint analysis, collaborating with academic and industrial partners.Completed a Ph.D. in 2019, specializing in machine learning for early malaria detection using blood smear image classification. Authored numerous publications in high-impact SCI and Scopus-indexed journals and conferences.