Review of Contemporary Philosophy
ISSN: 1841-5261, e-ISSN: 2471-089X
Vol 22 (1), 2023
Pp 2143 - 2152

Cybersecurity Challenges in Health Information Management: Comprehensive Review

[1]-Khadijah Ahmad Abdallh Bin Zarah,[2]-Manief Dahwi Al Enezi,[3]-Thamer Ali Ibrahim Olwani,[4]-Mohammed Ali Mohammed Daghriri,[5]-Ibrahim Hassan Mohammad Alamri,[6]-Talal Ayedh Ghazi Almutairi,[7]- Ahmed Khulaif Munawir Alharbi,[8]- Sabhaa Oudah Alhawiti,[9]- Mona Humod Alaseeri,[10]- Abdullah Makki Ali Abualqasim,[11]-Fadah Hamad Magaad Albugami,[12]- Saleh Sulaman Ahrani,[13]-Abdullah Saad Alharbi,[14]- Mohammed Joud Allah M,[15]- Waleed Muhamaed Muslim Al Anzey

1. Ksa, Ministry Of Health, Bahra Healte Center
2. Ksa, Ministry Of Health, Alyamamah Hospital
3. Ksa, Ministry Of Health, Samta General Hospital
4. Ksa, Ministry Of Health, Samitah General Hospital
5. Ksa, Ministry Of Health, King Saud Medical City
6. Ksa, Ministry Of Health, Riyadh First Health Cluster
7. Ksa, Ministry Of Health, King Saud Medical City
8. Ksa, Ministry Of Health, King Abdulaziz Specialist Hospital Taif.
9. Ksa, Ministry Of Health, King Abdulaziz Specialist Hospital Taif
10. Ksa, Ministry Of Health, Prince Mohammed Bin Nasser Hospital In Jazan
11. Ksa, Ministry Of Health, King Abdulaziz Specialist Hospital - Taif
12. Ksa, Ministry Of Health, Al Khalidiya Health Center
13. Ksa, Ministry Of Health, King Saud Medical City
14. Ksa, Ministry Of Health, Alqabbari
15. Ksa, Ministry Of Health, Erada Mental Health Complex Hail

Abstract

Background: The healthcare sector has increasingly integrated digital technologies, enhancing service delivery but also exposing sensitive data to cyber threats. The COVID-19 pandemic has accelerated this digital transformation, making cybersecurity a critical concern, particularly in protecting patient information.

Methods: This systematic review analyzes existing literature on cybersecurity challenges in health information management, focusing on the human factors contributing to vulnerabilities. A comprehensive search was conducted across three databases: Web of Science, CINAHL, and PubMed, employing eight distinct search queries. A total of 70 relevant studies were selected for analysis.

Results: The findings highlight three primary types of cyber threats in healthcare: attacks that exploit IT infrastructure vulnerabilities, ransomware incidents, and threats arising from human error and social engineering. Notably, the majority of data breaches stem from employee negligence rather than external hacking. The review emphasizes the importance of training and awareness programs to bolster cybersecurity defenses among healthcare professionals.

Conclusion: Effective cybersecurity in healthcare requires a dual approach: implementing technological solutions alongside comprehensive training programs that address human behavior. Raising awareness of cyber threats and improving organizational practices are essential for enhancing the resilience of

healthcare systems against cyberattacks. Future research should focus on developing standard methodologies for cybersecurity training and awareness in the healthcare sector.

Keywords: Cybersecurity, Healthcare, Digital Transformation, Human Factors, Systematic Review.

Received: 07 october 2023 **Revised:** 22 November 2023 **Accepted:** 06 December 2023

1. Introduction

Digital transformation, as described by Faddis [1], refers to the comprehensive impact generated by a software program that profoundly alters a certain area. Historically, the healthcare sector embraced digital transformation via the integration of health information systems and the implementation of cybersecurity measures for networked medical equipment. Nevertheless, the persistent COVID-19 epidemic has accelerated the deployment rate of these technologies [2,3]. In [1], the authors said that healthcare technology management experts are tasked with providing expert counsel on the use of healthcare facilities by clinical personnel and supervising the maintenance and functioning of medical equipment throughout their life cycle. The technical specialists include health technology, enabling the use of medical innovations to enhance and provide safer patient care.

The World Health Organization (WHO) technical series on primary health care indicates that information and communication technology (ICT) is becoming ubiquitous due to the proliferation of smartphones, tablets, and laptops [4]. Digital technologies for health are transforming the delivery and operation of health services, including advancements in health management, improved illness diagnostics, and the assessment of policy impacts on population health. A significant obstacle to the implementation of digital transformation plans is cybercrime, which exploits both system vulnerabilities and human weaknesses. Cybercrime originated in the late 1970s with the development of the computer information technology (IT) sector. What started as spam ultimately evolved into computer viruses and malware (e.g., WannaCry). The healthcare sector is a lucrative target for cybercriminals due to the presence of sensitive personal and financial data inside health records [5-7].

The increase in cybersecurity events poses an escalating danger to the healthcare sector, especially to hospitals. Yet the influence of cybersecurity is not exclusive to the healthcare sector; yet efforts to safeguard stakeholder data have been insufficient and have fallen behind those in other businesses. A comprehensive enumeration of many types of cyber assaults is included in Table A1. The rapid digitization of patient health information results in significant economic and intangible harm to hospitals due to data breaches. Organizations have implemented governance methods to mitigate the effects of cybersecurity attacks and to promote best practices for safeguarding the electronic infrastructure of hospitals and other therapeutic settings [6,8]. Notwithstanding the economic problems sometimes faced by healthcare organizations in providing services, there is growing evidence of investment from hospital administration to enhance the ICT infrastructure [8]. Although this move may be voluntary, the data governance regulations implemented by national agencies have also impacted investment priorities.

The effective implementation of digital transformation plans in the healthcare business depends on the acceptance of healthcare professionals in tackling the risks associated with cyber threats. Consequently, it is essential to provide awareness and training programs for healthcare personnel. The influence of human behavior in managing cyberattacks and enhancing cyber defenses is included under the topic of "human factors" in cybersecurity.

In light of the growing volume of publications since 2016 concerning the human role in augmenting cybersecurity [8-28], it is essential to synthesize the study outcomes. The primary aim of this systematic review is to analyze the literature to collect evidence from organizational case studies, author observations, and scientific advancements in cybersecurity, in order to ascertain the significance of incorporating human involvement in enhancing cyber defense within the healthcare sector. This systematic review is a comprehensive compilation of studies spanning over a decade that examine the challenges of cybersecurity

including organizational threats and personal assaults on the private information of healthcare professionals.

2. Methods

Three bibliographic databases—Web of Science (WoS), Cumulative Index to Nursing and Allied Health Literature (CINAHL), and PubMed®/MEDLINE—were searched using a total of eight distinct search queries. The search results from several databases were exported from their individual platforms and then put into the "Rayyan" platform for collaborative article filtering. Rayyan is an online platform that facilitates a blind evaluation of papers authored by numerous individuals. The imported results from PubMed, CINAHL, and WoS are analyzed individually based on the inclusion and exclusion criteria specified in the preceding paragraph.

3. Prevalent Cyber Threats in Healthcare Organizations

The literature on cyber threats faced by healthcare organizations can be categorized into three primary types: attacks that exploit vulnerabilities in IT infrastructure due to misconfigurations of network components, such as firewalls, and overwhelm digital services through flooding requests (denial of service (DoS), DDoS) [29-34], software bugs (e.g., structured query language (SQL) injections, privilege escalation, man-in-the-middle (MITM) attacks or eavesdropping, and cryptographic attacks; (ii) ransomware [20,32,35-39] attacks targeting healthcare organizations to disrupt services and extort data for financial gain; the emerging threat of exploiting human vulnerabilities to gain access to healthcare infrastructure.

The history of cyber threats to IT systems dates back to 1982, when a high school student launched the first computer virus, known as “Elk Cloner,” which was a benign software that showed a poem on Apple II computers. Over the last two decades, several advanced advancements have occurred in the design and execution of cyberattacks [38]. The evolving characteristics of cyber assaults targeting healthcare and clinical settings are mirrored by the extent and magnitude of digital tactics used inside healthcare organizations.

A concise historical account of the many events that influenced the domain of cybersecurity is provided in [40]. Since the first documented instance of a virus in 1982, a total of 14 cases have been recorded, leading to the establishment of the U.S. The National Institute of Standards and Technology (NIST) published the first edition of the "Framework for Improving Critical Infrastructure Cybersecurity" in 2014. According to [30], around 94% of healthcare organizations worldwide have had data breaches involving patient records, experienced information loss, been hacked, or had their data compromised. The cumulative number of cyber incidents amounts to 150 million compromised patient health data in the U.S. from 2009 to 2014. During this period, a growing number of healthcare organizations transitioned their operations to incorporate digital technologies, resulting in the maintenance of patient records in digital format, thereby creating an optimal environment for cyber attackers to execute systematic assaults on healthcare entities [40]. Although prevailing sentiment attributes data breaches to foreign hackers, research in [41] indicates that the majority of breaches stem from employee negligence and/or noncompliance with information security rules and procedures. In light of the rising incidence of cyberattacks, there is heightened awareness of the need to safeguard patient data and electronic health records from both external and internal threats, as indicated in [42]. The authors advocate for the significance of international standards like ISO/IEC 80001-1, which offers a framework to unite stakeholders in cyber defense to facilitate improved clinical care delivery.

Unlike conventional cybersecurity assaults targeting the IT systems and services of healthcare organizations, a significant ransomware event occurred in 2016 when the Hollywood Presbyterian Medical Center in Los Angeles paid a ransom of USD 17,000 to hackers. The event established a precedent for initiating assaults driven by financial incentives, leading to the interruption of healthcare service delivery. To raise awareness of the ramifications of ransomware, [23] executed a tabletop exercise with C-Level healthcare executives in a simulated scenario to formulate tactics as countermeasures. The intensity of ransomware attacks was further analyzed in [15], which included best practice suggestions to improve

cyber hygiene for healthcare professionals. In [6], the authors contended that to improve cybersecurity in hospitals, the senior management team, including chief information officers and chief security officers, should prioritize stakeholder alignment in formulating cybersecurity plans. Conversely, a different kind of danger has arisen, aimed at healthcare personnel. These attacks, often classified as "social engineering," enable the attacker to use the extensive public information available on social media sites to get the personal details of healthcare professionals [15]. Social engineering attacks aim to bypass conventional cybersecurity protocols [18]. Phishing is a well-recognized social engineering technique. The function and effect of phishing assaults have been extensively examined in the literature [8,9,10,13,15-18,41,43].

In [44], the authors provide an assessment of the current status of cybersecurity in healthcare, including cybersecurity breaches that include information theft, ransomware assaults on hospitals, and attacks on medical equipment. The authors categorize insider assaults as the unintentional or intentional activities of healthcare personnel that jeopardize the cybersecurity integrity of healthcare organizations. Such behaviors include replying to phishing emails, via which attackers might get login credentials to compromise the IT infrastructure with malware. Additional human behaviors recognized by the authors include incorrect security configurations, password mismanagement, and the loss of property, such as laptops with sensitive information.

Despite a strong agreement among healthcare organizations to improve service quality, budgetary obstacles hinder the adoption of cyber defense technologies. This problem was addressed in [8]. The authors contended that cybersecurity measures represent not only a cost, but an opportunity for value generation. The authors coined the term "value-based healthcare (VBH)" to connect healthcare compensation from insurance organizations to the quality of healthcare services. The article references a commercial service interruption in the U.K. resulting from the WannaCry ransomware, which led the National Health Service (NHS) to cancel over 600 procedures and over 19,000 appointments [45]. The direct cost of such assaults is represented by the ransom paid to the perpetrators, while the indirect cost to the organization is assessed via reputational damage and adverse effects on service delivery. Qualitative criteria should be taken into account when evaluating the investment costs in developing cyber defense capabilities inside healthcare organizations [46].

In light of the rising incidence of phishing attempts targeting healthcare workers, a study in [13] identified the underlying reason for employees inside an organization continuing to click on phishing links. The study was framed within the theory of planned behavior (TPB) and included trust theories. The authors determined that an investigation of attitude, subjective standards, and perceived behavioral control reveals a discrepancy between the decision-making process and the actual compliance behavior. The authors note a lower intention for organizational compliance with cyber defense measures compared to the intention to click on phishing links [13]. Research in [9,10] reported on the efficacy of a training program used in the U.S. healthcare system to mitigate the phishing click rate, hence amplifying the effects of phishing assaults on a national scale. The authors noted that phishing is a prevalent threat vector, and in the simulated scenario, employee click rates decrease with successive simulations. The authors in [15] found that healthcare workers had a low understanding of the hazards presented by social engineering attacks, especially phishing attempts, highlighting the need to enhance cyber hygiene and information governance rules among these professionals.

To mitigate the cognitive burden experienced by healthcare workers while processing emails, reference [16] introduces a methodology for assessing the attention necessary to determine the authenticity of an email against a phishing attempt. The authors assert that a thorough comprehension of the psychological elements of these assaults is lacking, which contributes to their elevated success rate. In [43], the authors contend that cyber defense is a joint endeavor between personnel and the administrative members of the healthcare organization. The authors provide guidelines to assist healthcare workers in effectively identifying phishing email assaults. In [17], the authors assert that, with the technology aspect, it is essential to unite organizational scientists to study human behavior in response to phishing attempts.

4. Strategic Approaches to Enhance Cybersecurity Competencies

Healthcare data breaches are recognized as an escalating concern to the healthcare sector, resulting in data loss, financial theft, and assaults on medical equipment and infrastructure, therefore endangering human lives [6]. The rising prevalence and changing characteristics of cyber assaults targeting healthcare and clinical settings need a comprehensive organizational approach to implement risk prevention and mitigation strategies.

Nonetheless, it is observed that several healthcare organizations are struggling with cybersecurity measures, owing to the scale and intricacy of their operations, along with the existence of various legacy and standalone systems. This is identified as the primary challenge in executing effective cybersecurity measures [31]. The authors observed that healthcare organizations have embraced the philosophy of "if it isn't broken, don't fix it" among top management. The intricacy of healthcare organizations was delineated in [6], whereby the authors asserted that these organizations are environments saturated with technology, akin to other organizations. The hospital setting has challenges in managing a diverse range of devices, from outdated IT systems to contemporary networked medical equipment. Furthermore, the internal policies of hospital organizations need collaboration among finance, IT, and human resources for efficient administration, while providing support for specialized services, like radiology, cardiology, and pediatrics, among others.

The level of specialization needed in each healthcare service delivery is distinct and often necessitates entirely separate equipment to address the demands of various patients. These intricate systems include distinct processes and use a highly specialized workforce that requires years of training. Unlike other industrial sectors, healthcare organizations often face regulatory constraints from governmental agencies and regulatory bodies. The protection of personally identifiable information (PII) is very important in healthcare. Personally Identifiable Information (PII) is defined as any data that may be used to identify an individual. Examples of such information include a complete name, social security number, license number, bank account number, passport number, and email address, among others. The authors assert that healthcare organizations prioritize patient-centered care, placing patient services above money production. Numerous studies in the literature have indicated the financial constraints faced by healthcare organizations [6,17,30,31,42].

In [47], the authors contended that the cyber domain is a multidisciplinary area that integrates skills from computer science, mathematics, economics, law, psychology, and engineering. The finding broadens the research to include not just the interactions across networks of online devices but also to ascertain how people engage with and are impacted by these technologies. The regulation of these interactions must be standardized across healthcare organizations to enhance interoperability and ensure regulatory compliance [42]. Healthcare businesses are advised to establish a dedicated cybersecurity staff structure to mitigate intrusions.

The authors outlined seven key roles within the framework, which are: security provision, responsible for conceptualizing, designing, and building secure information and communication technologies (ICT) systems; operation and maintenance, tasked with supporting, administering, and maintaining ICT systems; overseeing and governance, which involves providing leadership, management, and direction for implementing strategies to defend against cybersecurity threats and enhance resilience; protection and defense, focused on identifying, analyzing, and mitigating threats to internal ICT systems and networks; analysis, dedicated to reviewing and evaluating incoming cybersecurity information to assess its potential value for intelligence purposes; collection and operation, which entails conducting specialized denial and deception operations, as well as gathering cybersecurity information that could aid in intelligence development; and investigation, responsible for examining cybersecurity incidents or crimes involving ICT systems, networks, and digital evidence.

Although the proposed organizational roles utilize a bottom-up approach for information dissemination from the operational level to management, the authors in [6] contended that cybersecurity strategies should implement a top-down approach, wherein chief information officers (CIOs) and chief information security officers (CSIOs) establish the vision for improving organizations' cyber resilience. In

addition to the discoveries in [48], the authors of [6] asserted that cybersecurity capabilities include a range of programs, behaviors, and technology that a hospital uses to enhance cyber resilience. Nonetheless, several techniques lack sustainability and deteriorate with time [6,47].

The literature study on organizational tactics may be categorized into two primary types: technological solutions used to improve cyber resilience, and human factor techniques aimed at bolstering cyber defense. The technological method documented in the literature indicates that the implementation of organizational tactics pertains to collaborative information-sharing platforms, whereby a cyber-attack occurrence is communicated to other healthcare organizations [38]. The authors contend that information gathered during cybersecurity events needs to be disseminated across healthcare organizations for the purpose of blacklisting the sources of these occurrences. The information shared between the organizations may include data such as IP addresses, communications associated with those addresses, and user activities and browsing trends. The receiver of this knowledge might promptly rearrange the IT systems and amend the firewall rules to avert a similar assault. The authors advocate for the use of standardized information sharing protocols, namely Threat Information Expression (STIX) [34] and Trusted Automated sharing of Intelligence Information (TAXII) [43], to convey cyber occurrences. In addition to disseminating information on cyber events, the authors in [18] advocated for the implementation of international standards ISO/IEC 27002:2013 and ISO 27799:2016 to bolster cyber resilience in healthcare organizations. The ISO/IEC 27002:2013 standard provides advice for management techniques based on the risk profile of the environment. The standard advocates for the use of industry-recognized information security procedures to safeguard the ICT infrastructure. The ISO 27799:2016 standard on "health informatics" provides instructions for protecting the organizational ICT infrastructure based on suggested management practices.

The identified range of technical mitigation measures encompasses: regular backups as per ENISA guidelines; the implementation of firewalls and network segmentation; disabling unused physical ports to restrict access to universal serial buses (USBs); whitelisting authorized applications; adopting the principle of least privilege for user authentication and access rights management to healthcare resources; conducting regular updates and patches; employing software for virus and malware protection; encrypting data both at rest and in transit; implementing audit trails and logging for incident reporting; utilizing applications for network monitoring and intrusion detection; ensuring secure system configurations; and safeguarding mobile devices for Bring-Your-Own-Device (BYOD) services. The significance of system configuration is emphasized in [43], alongside the need of establishing dependable system defenses via user-centric tactics. In addition to technological techniques for mitigating cyber threats, the organizational tactics informed by human aspects documented in the literature include [9,17,20,25,30,43].

5. Methodology for Cyber Risk Assessment in Healthcare Organizations

The influence of digital technology and the implementation of digitalisation plans has empowered healthcare institutions to provide teleconsultation and tele-expertise, maintain electronic patient records, and interact with health equipment. The ubiquitous presence of digital technology necessitates a comprehensive examination of the many risk assessment approaches used by healthcare organizations. The ISO/IEC 27000:2018 standard defines information security as the preservation of confidentiality, integrity, and availability of data handled by computer systems. In a complicated healthcare system, a more comprehensive language should be used [33].

Historically, hazards to healthcare organizations were categorized as physical threats, such as fire or power outages, unauthorized physical or electronic access, and authorized physical or electronic access. Since the release of this risk assessment categorization, the nature of threats has altered; nowadays, healthcare organizations confront issues associated with cyber assaults. In formulating a risk-assessment technique, the authors in [33] contended that it is essential to model various types of threats. They said that threat intelligence must be founded on evidence-based information, including context, mechanisms, indications, consequences, and actionable recommendations about the rising danger or risk to assets. Numerous endeavors have been documented in the literature to formalize threat modeling methodologies

and threat classification models, including Structured Threat Information eXpression (STIX), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE), the Trike conceptual framework for security auditing, and Visual, Agile, and Simple Threat Modelling (VAST) [33]. A comprehensive review of the threat modeling approach for developing cyber risk assessment is offered in [64].

In [65], the authors delineated the supplementary risks associated with the integration of connected medical devices and proposed suggestions for organizational policies to implement in risk assessment procedures. The authors advocated for the implementation of international standards for documentation, change management, risk management, and responsibility allocation from a managerial viewpoint, such as the ISO/IEC 80001 standard, "Application of risk management for IT networks incorporating medical devices - Part 1: Roles, responsibilities and activities," issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). A comparable case study was reported in [7], whereby the authors advocated for the development of strategies to safeguard information resources against sophisticated and persistent cyberattacks from both scientific and practical viewpoints. The allocation of resources by an organization towards formal controls (e.g., risk management, policies, and procedures), informal controls (e.g., training), technological controls (e.g., firewalls, intrusion detection systems, anti-virus software, and encryption layers), physical controls, and administrative controls (e.g., Control Objectives for Information Technologies (COBIT), ISO/IEC 27001, NIST 800-53). Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 of the United States. The government and the Sarbanes–Oxley Act (SOX), a federal legislation in the United States, safeguard investors from deceptive financial reporting by firms, alongside the Payment Card Industry Data Security Standard (PCI-DSS).

In [54], the authors asserted that most data breaches result from employee negligence and carelessness toward information security, an issue that cannot be entirely resolved by legislation or technical measures. The author contended that the cybersecurity risk approach need to concentrate on modeling employee behavior related to information security. The authors presented the Information Security Climate Index (ISCI), a concise instrument including nine components, created via two pilot studies that reflect a comprehensive validation process grounded in best practices for scale development. Furthermore, in [31], the authors asserted that managing cybersecurity risk involves a delicate equilibrium between security and resilience. The authors developed a three-stage cybersecurity risk management framework comprising: (i) comprehending cybersecurity hazards; (ii) assessing the value of cybersecurity risks and mitigation strategies; and (iii) conveying cybersecurity activities and solutions. The risk assessment technique entails identifying essential, mission-critical activities and processes to create an inventory of susceptible assets linked to these core functions and processes. The technique facilitates the allocation of a risk impact score to each at-risk asset. In [52], the authors detailed the case study of the WannaCry assault in the United Kingdom. NHS services adversely affected the delivery of healthcare. The paper attributes the causes to an inability to adapt to increasing technical problems [41].

6. Conclusions

This article is a systematic review aimed at examining the existing research on the role of people in enhancing cyber security defenses. Seventy papers were chosen for inclusion in the study from a total of 695. Best practices and advice from healthcare organizational specialists should be disseminated to healthcare stakeholders, including physicians, nurses, patients, administrators, and IT professionals. Although academics have examined the influence of human variables, there is an urgent need to establish a systematic technique to integrate the study results, which can be objectively assessed by cybersecurity professionals in relation to safeguarding the IT infrastructure of the healthcare sector. Future research on assessing the efficacy of training and awareness initiatives in healthcare would benefit from exploring various threat methodologies and scenarios. There is a need to establish objective benchmarks for consolidating national research to enhance cyber hygiene inside healthcare. Our systematic review concludes that a collaborative and standardized methodology for developing training programs, awareness

campaigns, and information dissemination regarding the nature and types of cybersecurity attacks is essential to collectively fortify healthcare organizations against escalating cyber threats.

References

1. Faddis, A. The digital transformation of healthcare technology management. Biomed. Instrum. Technol. 2018, 52, 34–38.
2. Kim, D.W.; Choi, J.Y.; Han, K.H. Risk management-based security evaluation model for telemedicine systems. BMC Med Inform. Decis. Mak. 2020, 20, 106.
3. Venkatesha, S.; Reddy, K.R.; Chandavarkar, B.R. Social Engineering Attacks During the COVID-19 Pandemic. SN Comput. Sci. 2021, 2, 78.
4. World Health Organisation (WHO) on Primary Health Care. Available online: https://www.who.int/docs/default-source/primary-health-care-conference/digital-technologies.pdf?sfvrsn=3efc47e0_2.
5. Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol. Health Care 2017, 25, 1–10.
6. Jalali, M.S.; Kaiser, J.P. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J. Med. Internet Res. 2018, 20, e10059.
7. Ahmad, A.; Maynard, S.B.; Desouza, K.C.; Kotsias, J.; Whitty, M.T.; Baskerville, R.L. How can organizations develop situation awareness for incident response: A case study of management practice. Comput. Secur. 2021, 101, 102122.
8. Alami, H.; Gagnon, M.P.; Ahmed, M.A.A.; Fortin, J.P.; Alami, H.; Gagnon, M.P.; Ahmed, M.A.A.; Fortin, J.P. Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. Health Policy Technol. 2019, 8, 319–321.
9. Gordon, W.J.; Wright, A.; Aiyagari, R.; Corbo, L.; Glynn, R.J.; Kadakia, J.; Kufahl, J.; Mazzone, C.; Noga, J.; Parkulo, M.; et al. Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. JAMA Netw. Open 2019, 2, e190393.
10. Gordon, W.J.; Wright, A.; Glynn, R.J.; Kadakia, J.; Mazzone, C.; Leinbach, E.; Landman, A. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. J. Am. Med. Inform. Assoc. 2019, 26, 547–552.
11. Zafar, H. Cybersecurity: Role of Behavioral Training in Healthcare. In Proceedings of the AMCIS 2016 Proceedings, San Diego, CA, USA, 11–14 August 2016.
12. Hadlington, L.; Parsons, K. Can Cyberloafing and Internet Addiction Affect Organizational Information Security? Cyberpsychol. Behav. Soc. Netw. 2017, 20, 567–571.
13. Jalali, M.S.; Bruckes, M.; Westmattelmann, D.; Schewe, G. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. J. Med. Internet Res. 2020, 22, e16775.
14. Baillon, A.; de Bruin, J.; Emirmahmutoglu, A.; van de Veer, E.; van Dijk, B. Informing, simulating experience, or both: A field experiment on phishing risks. PLoS ONE 2019, 14, e0224216.
15. Priestman, W.; Anstis, T.; Sebire, I.G.; Sridharan, S.; Sebire, N.J. Phishing in healthcare organisations: Threats, mitigation and approaches. BMJ Health Care Inf. 2019, 26, e100031.
16. Montañez, R.; Golob, E.; Xu, S. Human Cognition Through the Lens of Social Engineering Cyberattacks. Front. Psychol. 2020, 11, 1755.
17. Dalal, R.S.; Howard, D.J.; Bennett, R.J.; Posey, C.; Zaccaro, S.J.; Brummel, B.J. Organizational science and cybersecurity: Abundant opportunities for research at the interface. J. Bus. Psychol. 2021, 1–29.
18. Eichelberg, M.; Kleber, K.; Kämmerer, M. Cybersecurity Challenges for PACS and Medical Imaging. Acad. Radiol. 2020, 27, 1126–1139.
19. Johansson, D.; Jonsson, P.; Ivarsson, B.; Christiansson, M.; Johansson, D.; Jonsson, P.; Ivarsson, B.; Christiansson, M. Information Technology and Medical Technology Personnel's Perception Regarding Segmentation of Medical Devices: A Focus Group Study. Healthcare 2020, 8, 23.
20. Budke, C.A.; Enko, P.J. Physician Practice Cybersecurity Threats: Ransomware. Mo. Med. 2020, 117, 102–104.

21. Hewitt, B.; Dolezel, D.; McLeod, A.J. Mobile Device Security: Perspectives of Future Healthcare Workers. Perspect. Health Inf. Manag. 2017, 14, 1c.
22. Schmidt, T.; Nøhr, C.; Koppel, R. A Simple Assessment of Information Security Awareness in Hospital Staff Across Five Danish Regions. Stud. Health Technol. Inform. 2021, 281, 635–639.
23. Maggio, L.A.; Dameff, C.; Kanter, S.L.; Woods, B.; Tully, J. Cybersecurity Challenges and the Academic Health Center: An Interactive Tabletop Simulation for Executives. Acad. Med. 2021, 96, 850–853.
24. Švábenský, V.; Čeleda, P.; Vykopal, J.; Brišáková, S. Cybersecurity knowledge and skills taught in capture the flag challenges. Comput. Secur. 2021, 102, 102154.
25. Li, L.; He, W.; Xu, L.; Ash, I.; Anwar, M.; Yuan, X. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. Int. J. Inf. Manag. 2019, 45, 13–24.
26. Kweon, E.; Lee, H.; Chai, S.; Yoo, K. The Utility of Information Security Training and Education on Cybersecurity Incidents: Empirical evidence. Inf. Syst. Front. 2021, 23, 361–373.
27. Tan, Z.; Beuran, R.; Hasegawa, S.; Jiang, W.; Zhao, M.; Tan, Y. Adaptive security awareness training using linked open data datasets. Educ. Inf. Technol. 2020, 25, 5235–5259.
28. He, W.; Zhang, Z.J. Enterprise cybersecurity training and awareness programs: Recommendations for success. J. Organ. Comput. Electron. Commer. 2019, 29, 249–257.
29. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ 2021, 372, n71.
30. Bhuyan, S.S.; Kabir, U.Y.; Escareno, J.M.; Ector, K.; Palakodeti, S.; Wyant, D.; Kumar, S.; Levy, M.; Kedia, S.; Dasgupta, D.; et al. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J. Med Syst. 2020.
31. Abraham, C.; Chatterjee, D.; Sims, R.R.; Abraham, C.; Chatterjee, D.; Sims, R.R. Muddling through cybersecurity: Insights from the US healthcare industry. Bus. Horizons 2019, 62, 539–548.
32. Rehman, H.U.; Yafi, E.; Nazir, M.; Mustafa, K.; Rehman, H.U.; Yafi, E.; Nazir, M.; Mustafa, K. Security Assurance Against Cybercrime Ransomware. Intell. Comput. Optim. 2019, 866, 21–34.
33. Spanakis, E.G.; Bonomi, S.; Sfakianakis, S.; Santucci, G.; Lenti, S.; Sorella, M.; Tanasache, F.D.; Palleschi, A.; Ciccotelli, C.; Sakkalis, V.; et al. Cyber-attacks and threats for healthcare—A multi-layer thread analysis. In Proceedings of the 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Montreal, QC, Canada, 20–24 July 2020; Volume 2020, pp. 5705–5708.
34. Rajamaki, J.; Nevmerzhitskaya, J.; Virag, C.; Rajamaki, J.; Nevmerzhitskaya, J.; Virag, C.G.P.I. Cybersecurity Education and Training in Hospitals Proactive Resilience Educational Framework (Prosilience EF). In Proceedings of the 2018 IEEE Global Engineering Education Conference (Educon)-Emerging Trends and Challenges of Engineering Education, Santa Cruz de Tenerife, Spain, 17–20 April 2018; pp. 2042–2046.
35. Dameff, C.J.; Selzer, J.A.; Fisher, J.; Killeen, J.P.; Tully, J.L. Clinical Cybersecurity Training Through Novel High-Fidelity Simulations. J. Emerg. Med. 2019, 56, 233–238.
36. Rayyan.ai. Available online: https://rayyan.ai/.
37. Ouzzani, M.; Hammady, H.; Fedorowicz, Z.; Elmagarmid, A. Rayyan—A web and mobile app for systematic reviews. Syst. Rev. 2016, 5, 210.
38. Azad, M.A.; Bag, S.; Ahmad, F.; Hao, F.; Azad, M.A.; Bag, S.; Ahmad, F.; Hao, F. Sharing is Caring: A collaborative framework for sharing security alerts. Comput. Commun. 2021, 165, 75–84.
39. Pears, M.; Henderson, J.; Konstantinidis, S.T. Repurposing Case-Based Learning to a Conversational Agent for Healthcare Cybersecurity. Stud. Health Technol. Inform. 2021, 281, 1066–1070.
40. Grimes, S.; Wirth, A. Holding the Line: Events that Shaped Healthcare Cybersecurity. Biomed. Instrum. Technol. 2017, 51, 30–32.
41. Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E.; Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E. Information security climate and the assessment of information security risk among healthcare employees. Health Inform. J. 2020, 26, 461–473.
42. Alwi, R.; Prowse, P.; Gaamangwe, T. Proactive Role of Clinical Engineering in the Adoption of ISO/IEC 80001-1 within Healthcare Delivery Organization. In Proceedings of the 2020 42nd Annual International

Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Montreal, QC, Canada, 20–24 July 2020; Volume 2020, pp. 5623–5626.
43. DF, S.; Singh, H. A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Appl. Clin. Inform. 2016, 7, 624–632.
44. Coventry, L.; Branley, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 2018, 113, 48–52.
45. Farringer, D.R. Maybe If We Turn It Off and Then Turn It Back On Again? Exploring Health Care Reform as a Means to Curb Cyber Attacks. J. Law Med. Ethics J. Am. Soc. Law Med. Ethics 2019, 47, 91–102.
46. Panda, S.; Panaousis, E.; Loukas, G.; Laoudias, C. Optimizing Investments in Cyber Hygiene for Protecting Healthcare Users. In From Lambda Calculus to Cybersecurity Through Program Analysis; Springer: Berlin/Heidelberg, Germany, 2020; pp. 268–291.
47. Dawson, J.; Thomson, R. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Front. Psychol. 2018, 9, 744.

تحديات الأمن السيبراني في إدارة المعلومات الصحية: مراجعة شاملة

الملخص

الخلفية :أدى تكامل التقنيات الرقمية في قطاع الرعاية الصحية إلى تحسين تقديم الخدمات، ولكنه كشف أيضًا البيانات الحساسة لتهديدات سيبرانية. وقد سرعت جائحة كوفيد-19 من هذا التحول الرقمي، مما جعل الأمن السيبراني قضية حيوية، خاصة في حماية معلومات المرضى.

الطرق :تحلل هذه المراجعة المنهجية الأدبيات الحالية حول تحديات الأمن السيبراني في إدارة المعلومات الصحية، مع التركيز على العوامل البشرية التي تسهم في الثغرات. تم إجراء بحث شامل في ثلاث قواعد بيانات Web of Science :و CINAHLوPubMed، باستخدام ثماني استفسارات بحثية متميزة. وتم اختيار 70 دراسة ذات صلة للتحليل.

النتائج :تسلط النتائج الضوء على ثلاثة أنواع رئيسية من التهديدات السيبرانية في مجال الرعاية الصحية: الهجمات التي تستغل ثغرات البنية التحتية لتقنية المعلومات، وحوادث برامج الفدية، والتهديدات الناجمة عن الأخطاء البشرية والهندسة الاجتماعية. ومن الجدير بالذكر أن غالبية انتهاكات البيانات تنبع من إهمال الموظفين أكثر من الاختراقات الخارجية. تؤكد المراجعة على أهمية برامج التدريب والتوعية لتعزيز الدفاعات السيبرانية بين العاملين في مجال الرعاية الصحية.

الاستنتاج :يتطلب تحقيق الأمن السيبراني الفعال في الرعاية الصحية نهجًا مزدوجًا: تنفيذ حلول تقنية إلى جانب برامج تدريب شاملة تتناول السلوك البشري. يُعد رفع مستوى الوعي بالتهديدات السيبرانية وتحسين الممارسات التنظيمية أمرًا ضروريًا لتعزيز قدرة أنظمة الرعاية الصحية على مقاومة الهجمات السيبرانية. يجب أن تركز الأبحاث المستقبلية على تطوير منهجيات معيارية للتدريب والتوعية بالأمن السيبراني في قطاع الرعاية الصحية.

الكلمات المفتاحية :الأمن السيبراني، الرعاية الصحية، التحول الرقمي، العوامل البشرية، مراجعة منهجية.