Systematic Review

A Systematic Review on Cybersecurity Threats and Challenges in Hospitals

Vishnu Sunil[1], Sherry P. Mathew[2]

[1]Assistant Professor, Department of Hospital Administration, All India Institute of Medical Sciences Kalyani, West Bengal, [2]Associate Professor, Department of Hospital Administration, Vydehi Institute of Medical Sciences and Research Centre, Bengaluru, Karnataka, India

Abstract

The inception of cybercrime can be traced back to the late 1970s, a period that coincided with the early development of the computer information technology (IT) sector. Due to its system vulnerabilities, healthcare has become particularly vulnerable to digital assaults. Hardware, software, networks, operating systems, medical devices, processes, and users make this sector vulnerable. This report identifies healthcare cybersecurity issues and solutions and opportunities for improvement in response to rising threats. This review's methodology was organised so that it complies to PRISMA criteria. A thorough search was undertaken in Web of Science, Scopus, Google Scholar, Saudi Digital Library, ACM Digital Library, PMC, and NCBI/PubMed. The search strategy included threats, ransomware, cybercrime, healthcare, and hospitals. The above overview of "cybersecurity" includes technological and organisational measures. Healthcare organisations cybersecurity defence concerns were the focus of the research questions. The search technique targeted relevant literature from bibliographic databases to answer these research concerns. A total of 352 potential entries were obtained from the search in the chosen databases. Of these, 13 were manually picked following preliminary assessment. The study examined these studies, which fit its focus on "cybersecurity, dangers, and challenges," in detail. Data confidentiality, integrity, and availability are the foundation of information security. The study examined cyberthreats and their cascade effects. The growing usage of varied technologies for sensitive patient data transfer makes it difficult for healthcare organisations to stay up with the newest cybersecurity breaches and threats. A cohesive and integrated strategy involving training programmes, awareness campaigns, and cyberattack information sharing is advocated to protect healthcare organisations from cyberattacks. To protect our infrastructure and provide excellent patient care, all healthcare workers must recognise and accept their role in cybersecurity risk management.

Keywords: Challenges, cybercrime, cybersecurity, health care, hospitals, threats

Introduction

The genesis of cybercrime can be traced back to the late 1970s, marking the dawn of the computer information technology (IT) industry. The initial wave of spam served as a precursor to more sophisticated forms of malicious software. As technology has advanced, so too has the complexity of cyber threats. The health-care sector, with its vast repositories of personal and financial data, has become a prime target for cybercriminals.

The significance of health care in society

Healthcare is based on social justice, equity, solidarity, and participation, It is built on the idea that everyone has the right to the best health.[1] The recent global pandemic and population growth have dramatically amplified the demand for health-care services.[2] Hospitals are tasked with the dual responsibilities of safeguarding sensitive personal data and ensuring its accessibility to authorized entities. The digitalization of health records marks a pivotal shift in health-care delivery toward more decentralized, patient-centric models.[3,4] However, this shift also exposes the sector to increased cybersecurity risks due to the inherent vulnerabilities in its systems, encompassing hardware, software, networks, operating systems, medical devices, and human users.[5]

Submitted: 19-Jan-2024 **Revised:** 16-Feb-2024
Accepted: 04-Mar-2024 **Published:** 29-Apr-2024

Access this article online

Quick Response Code:

Website: www.actamedicainternational.com

DOI: 10.4103/amit.amit_7_24

Address for correspondence: Dr. Vishnu Sunil, Assistant Professor, Department of Hospital Administration, All India Institute of Medical Sciences Kalyani, West Bengal, India.
E-mail: Vishnu.ha@aiimskalyani.edu.in

How to cite this article: Sunil V, Mathew SP. A systematic review on cybersecurity threats and challenges in hospitals. Acta Med Int 2024;11:1-6.

Increasing threats in health-care cybersecurity

Since 2010, there has been a notable rise in data breaches within the health-care sector, making it one of the most targeted industries for cyberattacks globally, as highlighted in a 2016 IBM and Ponemon Institute study.[6,7] The immutable nature of health data makes it particularly attractive to criminals.[8] The WannaCry ransomware attacks in May 2017, which disrupted the UK's National Health Service, underscore the severe operational and financial implications of such breaches.[9]

Challenges in health-care information technology security

Despite the critical need, cybersecurity often receives minimal funding within the financially constrained health-care sector.[10] The integration of numerous interconnected medical devices and inconsistent business processes further complicates the cybersecurity landscape. This is exacerbated by the use of vulnerable medical equipment within hospital premises and beyond.[10]

The emergence of smart hospitals

Recent technological advancements in health care aimed at enhancing efficiency and reducing costs have led to the concept of smart hospitals.[2] This development necessitates robust data protection measures, given the plethora of connected devices. The health-care industry is often characterized by its "low-security maturity" and limited data security capabilities, attributed to budgetary limitations, lack of cybersecurity awareness among health management, fragmented IT infrastructure, and an overreliance on wireless devices.[11] Typically, health-care organizations implement cyber defenses reactively, postincident.[11]

Lagging cybersecurity in health care

Despite the global surge in cyberattacks, the health-care industry remains significantly behind other sectors in protecting patient information.[12] The growing concern for cybersecurity in health care is often underestimated and under-prioritized.[13]

Objective of the analysis

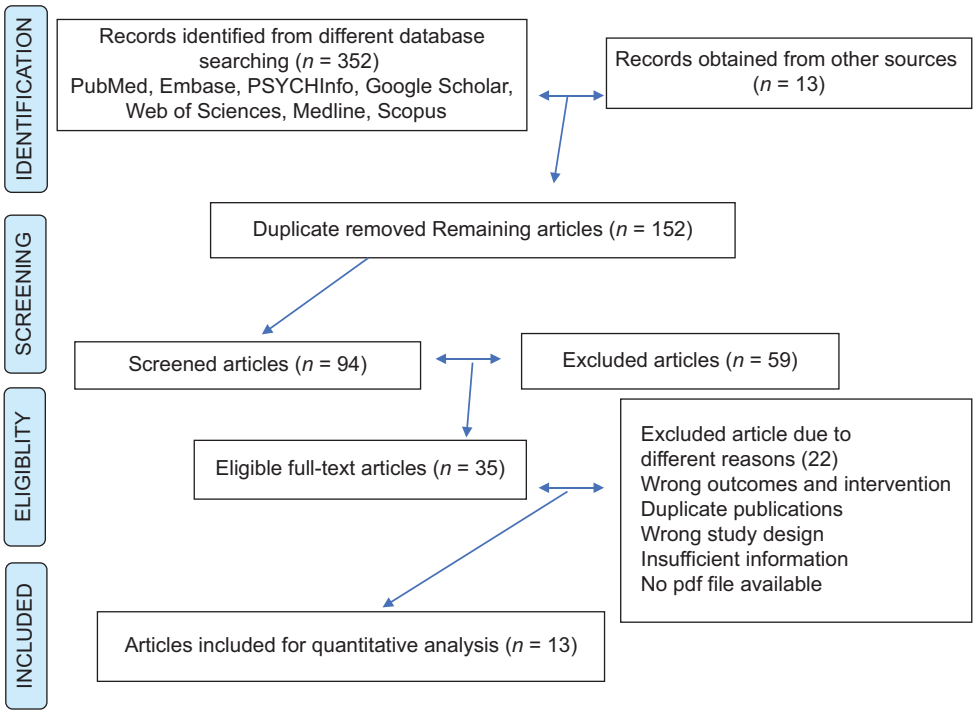
The primary objective of this analysis is to identify and assess the critical cybersecurity threats, challenges, and existing solutions within the health-care sector, as well as to propose areas for improvement in response to the increasing frequency of cyberattacks.

Materials and Methods

This systematic review was meticulously structured in alignment with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines. A comprehensive literature search was conducted using several databases, including Web of Science, Scopus, Google Scholar, the Saudi Digital Library, ACM Digital Library, PMC, and NCBI/PubMed [Flow Chart 1]. The selection of search terms was strategically focused on areas central to cybersecurity, encompassing "threats," "ransomware," "cybercrime," "healthcare," and "hospitals."

Research questions

The term "cybersecurity" encompasses a wide array of activities, extending from technological advancements to the implementation of organizational security measures. The study's research questions were formulated to delve into



Flow Chart 1: The Preferred Reporting Items for Systematic Reviews and Meta-Analyses technique was used for the selection mechanism schedule of articles in this study

a prevalent challenge faced by health-care organizations: enhancing their cyber defense mechanisms. Tailored search phrases were utilized for extracting relevant literature from bibliographic databases.

RQ1: What are the prevalent cybersecurity threats encountered by hospitals? RQ2: Can the return on investment for internal training and awareness campaigns be quantified, and how do these initiatives contribute to health-care workers' understanding of cyber threats? RQ3: What is the recommended approach for hospitals to conduct a comprehensive cybersecurity risk assessment, considering the human element? RQ4: What strategies and protocols have hospitals adopted to bolster their cybersecurity resilience? RQ5: What recommendations have international and national bodies proposed for cyber defense strategies to enhance cyber resilience?

Inclusion criteria

This review was limited to articles published in English. A thorough approach was adopted, including articles that featured the specified keywords in their titles or abstracts, regardless of the availability of full texts. To be considered for this review, articles needed to specifically address cybersecurity in health care and associated security risks. Duplicate articles identified during the literature search were excluded.

Search results and selection process

Using the search terms "ransomware OR cybersecurity," a total of 365 articles were identified [Flow Chart 1]. The majority of ransomware-related content appeared in news outlets, while cybersecurity-related articles were predominantly found in academic journals.

Two independent evaluators were involved in the selection of studies for inclusion. The selection process also involved a detailed examination of gray literature and reference lists to identify additional relevant studies, aiming to expand the sample size and mitigate publication bias. Both authors independently reviewed the titles and abstracts of each article for potential conflicts of interest, utilizing co-evidence. Discrepancies were collaboratively resolved through discussion. A similar approach was adopted during the full-text screening phase, ensuring thorough evaluation and adherence to the study's objectives. This meticulous screening process, although time-consuming, was essential for validating the inclusion of each selected study.

Results

In our comprehensive search across designated digital databases, we identified 352 potential records. Following a meticulous review process, 13 studies were ultimately selected. These papers were chosen for their direct relevance and insightful contribution to our primary focus areas: "cybersecurity, threats, and challenges" within the health-care sector.

To gain a more nuanced understanding of the cyber threat landscape in health care, we categorized these threats into several distinct subthemes. These include insider threats, which encompass human errors such as careless behavior, lack of awareness, or inadvertent security breaches (like sharing passwords unauthorizedly); cybersquatting threats, involving more malicious actions such as hacker intrusions, spyware, malware attacks, viruses, and data breaches; and technological failures that span hardware, software, infrastructure, and power systems. Our analysis further differentiated these threats into intentional and unintentional risks, evaluating the potential impact and likelihood of each. For instance, cybercrimes such as hacking (intentional threats) and power outages (unintentional risks) were identified as high risks due to their significant potential for damaging health data. Conversely, internal factors like user errors were classified as low-risk, given their unintentional nature. The diverse categories of cyberattacks are systematically outlined in Table 1.

The core foundation of information security hinges on three critical principles: ensuring data confidentiality, maintaining data integrity, and guaranteeing data availability. To address these aspects, our research delved into a broad spectrum of academic literature pertaining to cyber threats and their cascading effects. Table 2 provides a detailed examination of the various cyber threats and vulnerabilities

Table 1: Classification of cybersecurity threats in hospital settings

Threat type	Category	Risk level	Potential motivations
Malware (including ransomware)	Cybersquatting	Medium	Disrupting systems to facilitate system breach; theft of passwords/private data
		High	Data breach for ransom; financial extortion
DoS attacks	Technological threats	High	System disruption; prelude to system breach; ransom demands
Phishing	Cybersquatting	Medium	Data breaches; personal information theft for sale; facilitation of other attacks
Masquerade attacks	Technological threats	High	Acquisition of confidential data; alteration/deletion of patient health records
Data injection attacks	Technological threats	High	Causes misdiagnosis, insurance fraud; mission-critical disruptions
Hardware/software malfunctions	Insider threats	Medium	Often accidental; can lead to suboptimal service provision
Outdated technology/HIS	Insider threats	Medium	Generally unintentional; results in unreliable systems
Critical infrastructure failure	Insider threats	High	Severe consequences like data loss; typically unintentional
Human usability errors	Insider threats	Low	Often due to carelessness, posing significant information security risks
Management weaknesses	Insider threats	Medium	Often inadvertent due to resource limitations or lack of expertise

DoS: Denial of service, HIS: Hospital information system

that challenge the three foundational pillars of health information security. Table 3 synthesises PRISMA-compliant research publications on healthcare cybersecurity threats. It evaluates studies from various countries and years based on predefined research questions (RQ1-RQ5) about cybersecurity challenges, finding high to moderate relevance across healthcare cybersecurity topics like social engineering attacks, cybersecurity education, and proactive risk management.

Discussion

The rapid digitization across various sectors, including health care, has significantly amplified the frequency and intricacy of cybercrimes. Health-care organizations, in particular, are increasingly targeted by diverse cyber threats such as phishing, identity theft, email fraud, banking fraud, masquerade attacks, data injection attacks, and technological malfunctions. Venkatesha *et al*. (2021) recommends multidisciplinary approaches to healthcare cybersecurity's complex cyber threats. Phishing, identity theft, and data breaches have grown with COVID-19's digitization.[14] PACS and medical imaging system vulnerabilities by Eichelberg et al. demonstrate the need for complete cybersecurity.[15] Bhuyan *et al*. proactive cybersecurity measures meet the need for healthcare staff training to preserve patient privacy and organisational integrity.[16] Spanakis *et al*. analysis of healthcare infrastructures' multi-layered cybersecurity threats highlights the need for a holistic security paradigm that incorporates technology and human factors.[17] The "Prosilience EF" and conversational agents' unique training approaches teach healthcare workers how to manage and reduce cyber risks.[18,19] Research demonstrates that Information Security Awareness is essential for cyberattack preparedness.[20] In digital healthcare, the studies advocate a comprehensive and integrated cybersecurity approach that tackles technology vulnerabilities and human factors to safeguard sensitive patient data and healthcare systems.[21-26] A prominent example illustrating the severity of these threats is the WannaCry

Table 2: Barriers and vulnerabilities in cybersecurity impacting health information security goals

Health information security goal	Vulnerabilities	Threats	Cascading consequences
Confidentiality	Password sharing	Unauthorized access, phishing, eavesdropping	Malicious exploitation leading to patient harm or illicit data sales
Integrity	Typographical errors, data modification	False data injection attacks	Potential patient harm due to incorrect treatments or medication resulting from inaccurate data
Availability	Data access and maintenance issues	Technological challenges (e.g., obsolescence and DDoS attacks)	Delays in critical processes, data loss, wastage of time and resources

DDoS: Distributed denial of service

Table 3: Synthesized review of research articles in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses protocols

Author	Year	Country	Topic	RQ1–RQ5
Venkatesha *et al*.[14]	2021	India	"Social Engineering Attacks During the COVID-19 Pandemic"	RQ2: High relevance
Eichelberg *et al*.[15]	2020	Germany	"Cybersecurity Challenges for PACS and Medical Imaging"	RQ1, RQ3, RQ4: High relevance
Bhuyan *et al*.[16]	2020	India	"Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations"	RQ1, RQ2, RQ3, RQ4: High relevance
Spanakis *et al*.[17]	2020	Canada	"Cyber-attacks and threats for healthcare-a multi-layer thread analysis"	RQ1, RQ3, RQ4: Moderate relevance
Rajamaki *et al*.[18]	2018	Finland	"Cybersecurity Education and Training in Hospitals Proactive Resilience Educational Framework (Prosilience EF)"	RQ1, RQ2, RQ3, RQ4, RQ5: Moderate to high relevance
Pears *et al*.[19]	2021	England	"Repurposing Case-Based Learning to a Conversational Agent for Healthcare Cybersecurity"	RQ1, RQ2: Moderate relevance
Schmidt *et al*.[20]	2021	Denmark	"A Simple Assessment of Information Security Awareness in Hospital Staff Across Five Danish Regions"	RQ1, RQ2, RQ5: High relevance
Tully *et al*.[21]	2020	USA	"Healthcare Challenges in the Era of Cybersecurity"	RQ5: High relevance
Williams C.M. *et al*.[22]	2020	USA	"Cybersecurity Risks in a Pandemic"	RQ1, RQ3, RQ4, RQ5: High relevance
Coventry and Branley[23]	2018	England	"Cybersecurity in healthcare: A narrative review of trends, threats and ways forward"	RQ1, RQ2, RQ3, RQ4, RQ5: High relevance
Gordon *et. al*.[24]	2019	USA	"Assessment of Employee Susceptibility to Phishing Attacks at U.S. Health Care Institutions"	RQ1, RQ2, RQ4, RQ5: High relevance
Kessler *et al*.[25]	2020	USA	"Information security climate and the assessment of information security risk among healthcare employees."	RQ1, RQ3, RQ4: High relevance
Coronado and Wong[26]	2014	USA	"Healthcare Cybersecurity Risk Management: Keys to an Effective Plan"	RQ1, RQ2, RQ3, RQ4, RQ5: Moderate to high relevance

PACS: Picture archiving and communications systems

ransomware attack in May 2017, which had a profound impact on healthcare facilities worldwide, underscoring the critical need for enhanced cybersecurity measures.[27] The escalation in cybercrime and data breaches within the healthcare sector, as discussed in numerous studies, mirrors the advancing complexity of hacking techniques.[28-30]

Further highlighting this trend is the ransomware attack on the All India Institute of Medical Sciences in November 2022, resulting in the compromise of sensitive patient records, including those of notable figures.[31] This systematic review aims to explore the changing landscape of cyber threats in health-care settings, particularly those handling extensive patient records and sensitive personal information. Identified contributing factors to these security vulnerabilities include the high stress levels commonly experienced by health-care staff, leading to an increased risk of falling prey to phishing attacks, and the lack of adequate cybersecurity training and awareness.

The COVID-19 pandemic significantly intensified the use of e-health-care services, thereby amplifying the cybersecurity challenges in health-care institutions already contending with resource and staffing constraints.[32] To mitigate these challenges, it is imperative for hospitals to develop and implement comprehensive cybersecurity training and awareness programs. Key strategies include establishing clear objectives for online training, identifying potential security risks, forming de-escalation teams, and rigorously assessing the effectiveness of training through course completion rates. Such initiatives are vital in providing health-care personnel with the necessary skills and knowledge to effectively combat cyber threats.

In response to these evolving cybersecurity needs, hospitals have adopted a range of strategies to bolster their resilience. These include enhancing staff training, simplifying endpoint management, aligning stakeholder interests, and integrating continuous monitoring systems with antivirus solutions. At a broader level, numerous national and international organizations have played a pivotal role in formulating defense strategies against cyber threats. Recommendations from these bodies encompass a diverse range of measures, including software and application security, infrastructure protection, cloud security, IoT security, and the establishment of robust security management systems. Notably, the United Nations Conference on Trade and Development has highlighted the significance of access control, data security, network security, and operational security as key components in reinforcing cyber resilience.[33]

Blockchain technology has emerged as a promising solution in the realm of cybersecurity. Its decentralized nature ensures the integrity and immutability of data, thereby offering substantial protection against hacking attempts.[34] The adoption of blockchain technology in health-care cybersecurity holds the potential to significantly reduce the risk of future cyberattacks, safeguarding sensitive patient information and health-care systems.

The literature offers several techniques for improving cybersecurity in health care, despite the limited availability of sensitive information in the public domain. One important aspect is the focus on regularly updating software and hardware, implementing robust security measures for information and communication technology systems, and effectively managing vulnerabilities that occur from the interchange of information by health-care staff. Moreover, the intricate system of networked medical devices presents substantial cybersecurity obstacles.

There is an increasing consensus within the health-care business regarding the necessity of incorporating integrated and secure digital technologies. Recent studies have emphasized the increased acknowledgment of the important nature of teaching health-care personnel about cybersecurity concerns.[35] Our analysis highlights the importance of implementing specific educational and training requirements that specifically target human elements in cybersecurity. These guidelines are essential for efficiently reducing cyber dangers. The subject of human element research in health-care cybersecurity is still in its nascent stage. However, the various case studies and research findings covered in this review indicate the increasing significance and potential influence of this topic.

Conclusion

A key limitation of this systematic review was the inability to conduct a meta-analysis due to the varied technological approaches to transmitting sensitive patient data in health care. This complexity hinders effective tracking and response to cyber threats. We advocate for a unified approach in enhancing cybersecurity, involving comprehensive training, awareness campaigns, and information exchange on cyber threats. Collective efforts are vital to strengthen health care against increasing cyber risks. It is essential for all in health care to engage in managing cybersecurity risks, protecting sensitive data, and ensuring patient care quality. Our findings highlight the need for a cohesive cybersecurity strategy, emphasizing each individual's role in this crucial task.

Financial support and sponsorship

Nil.

Conflicts of interest

There are no conflicts of interest.

References

1. Primary health care. Who.int n.d. Available form: https://www.who.int/news-room/fact-sheets/detail/primary-health-care. [Last accessed on 2024 Feb 14].
2. Ranganayaki RS, Sreeja B, Gandhari S, Ranganath PT, Kumar S. Cyber Security in Smart Hospitals: A Investigational Case Study. 2021 10th International Conference on System Modeling and Advancement in Research Trends (SMART). Moradabad, India; 2021. p. 92-8.
3. Abd-Alrazaq AA, Bewick BM, Farragher T, Gardner P. Factors that affect the use of electronic personal health records among patients: A systematic review. Int J Med Inform 2019;126:164-75.

4. Zeb K, Saleem K, Al-Muhtadi J, Thuemmler C. U-Prove Based Security Framework for Mobile Device Authentication in eHealth Networks; 2016.
5. Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Med Devices (Auckl) 2015;8:305-16.
6. Sponsored by ID Experts. Sixth annual benchmark study on privacy & security of healthcare data. Ponemon.org n.d. Available form: https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf. [Last accessed on 2024 Feb 1].
7. Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity and healthcare: How safe are we? BMJ 2017;358:j3179.
8. Alvarez M. Security Trends in the Healthcare Industry. Somers: IBM; 2017. p. 2-18.
9. Millard WB. Where Bits and Bytes Meet Flesh and Blood. Annals of Emergency Medicine. 2017;70:A17-21. [doi: 10.1016/j.annemergmed.2017.07.008].
10. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin MV, Calcavecchia F, Anderson D, *et al.* Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak 2020;20:146.
11. Offner KL, Sitnikova E, Joiner K, MacIntyre CR. Towards understanding cybersecurity capability in Australian Healthcare Organisations: A systematic review of recent trends, threats and mitigation. Intelligence and National Security. 2020;35:556-85. doi:10.1080/02684527.2020.1752459.
12. West DM, Skahill E. Why hospitals and healthcare organizations need to take cybersecurity more seriously. Brookings 2021. Available form: https://www.brookings.edu/articles/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/. [Last accessed on 2024 Feb 14].
13. Gordon WJ, Fairhall A, Landman A. Threats to information security – Public health implications. N Engl J Med 2017;377:707-9.
14. Venkatesha S, Reddy KR, Chandavarkar BR. Social engineering attacks during the COVID-19 pandemic. SN Comput Sci 2021;2:78.
15. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity challenges for PACS and medical imaging. Acad Radiol 2020;27:1126-39.
16. Bhuyan SS, Kabir UY, Escareno JM, Ector K, Palakodeti S, Wyant D, *et al.* Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. J Med Syst 2020;44:98.
17. Spanakis EG, Bonomi S, Sfakianakis S, Santucci G, Lenti S, Sorella M, *et al.* Cyber-attacks and threats for healthcare – A multi-layer thread analysis. Annu Int Conf IEEE Eng Med Biol Soc 2020;2020:5705-8.
18. Rajamaki J, Nevmerzhitskaya J, Virag C, Rajamaki J, Nevmerzhitskaya J, Virag CG. 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; 2018. p. 2042-6.
19. Pears M, Henderson J, Konstantinidis ST. Repurposing case-based learning to a conversational agent for healthcare cybersecurity. Stud Health Technol Inform 2021;281:1066-70.
20. 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;281:635-9.
21. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health Secur 2020;18:228-31.
22. Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity risks in a pandemic. J Med Internet Res 2020;22:e23692.
23. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 2018;113:48-52.
24. Gordon WJ, Wright A, Aiyagari R, Corbo L, Glynn RJ, Kadakia J, *et al.* Assessment of employee susceptibility to phishing attacks at US health care institutions. JAMA Netw Open 2019;2:e190393.
25. Kessler SR, Pindek S, Kleinman G, Andel SA, Spector PE. Information security climate and the assessment of information security risk among healthcare employees. Health Informatics J 2020;26:461-73.
26. Coronado AJ, Wong TL. Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. Biomedical Instrumentation & Technology. 2014;48:26-30.
27. Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. BMC Med Inform Decis Mak 2019;19:10.
28. News From The Nation's Health. American Journal of Public Health. 2017;107:1195-5.https://doi.org/10.2105/AJPH.2017.303913.
29. Frumento E. Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution. EAI/Springer Innovations in Communication and Computing. 2019;35-69.
30. Langer SG. Cyber-security issues in healthcare information technology. J Digit Imaging 2017;30:117-25.
31. Ciso ET. AIIMS ransomware attack: what it means for health data privacy. ETCISO 2022. Available form: https://ciso.economictimes.indiatimes.com/news/aiims-ransomware-attack-what-it-means-for-health-data-privacy/96538957 [Last accessed 2024 Feb 13].
32. Khan NA, Brohi SN. Zaman N. Ten Deadly Cybersecurity Threats amid COVID-19 Pandemic. Berlin: IEEE, Researchgate Publications; 2020.
33. Perwej A, Haq K, Perwej Y. Blockchain and its influence on market. Int J Comput Sci Trends Technol 2019;7:82-91. [doi: 10.33144/23478578/IJCST-V7I5P10].
34. Grpoup D. Cyber Crime: New Challenge to Mankind Society Introduction to the Nature of Cyber Crime and Its Investigation Process; 2011.
35. Alami H, Gagnon MP, Ahmed MA, Fortin JP, Alami H, Gagnon MP, *et al*. Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. Health Policy Technol 2019;8:319-21.