Cybersecurity Training in the Healthcare Domain

Ilkka Tikanmäki[1,2]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]National Defence University, Helsinki, Finland

Ilkka.tikanmaki@laurea.fi

Abstract: Integrating digital technologies in healthcare, such as electronic health records (EHR), telemedicine, and smart devices, has significantly enhanced patient care and operational efficiency. However, this digital transformation also introduces substantial cybersecurity challenges, threatening patient safety and data integrity. This study examines the current state of cybersecurity training within the healthcare sector, highlighting the critical need for continuous and comprehensive training programs tailored to healthcare professionals' diverse needs and technical skill levels. The study identifies key vulnerabilities, including software weaknesses, human errors, and information security shortcomings, emphasising the importance of staff motivation and adherence to cybersecurity measures. Through a qualitative case study methodology, the study explores effective training practices that promote cybersecurity awareness and compliance among healthcare staff. Findings indicate that despite existing training efforts, many healthcare workers feel undertrained and uninformed about secure technology use, leading to frustration and potential data breaches. The study underscores the importance of customised training programs that address strong password practices, phishing detection, secure data management, and device protection. Additionally, it emphasises the role of healthcare workers in safeguarding Protected Health Information (PHI) and the necessity for a collaborative approach to cybersecurity risk management. The research concludes with recommendations for enhancing cybersecurity training and fostering a culture of vigilance and responsibility within healthcare organisations. This study uses a qualitative research methodology through desk research. The data collection process was based on existing cybersecurity policy documents, training materials, incident reports, and compliance information. The results were validated using multiple data sources to ensure data triangulation. The study's approach ensured an understanding of the current state of cybersecurity training in healthcare and provided practical recommendations for improving the effectiveness of training programs. This research may help further enhance the understanding and implementation of effective cybersecurity training programs in healthcare, ultimately improving the protection of sensitive health information and patient safety. This study's research question addresses the modification of training and learning practices to improve healthcare professionals' awareness of and compliance with cybersecurity.

Keywords: Cybersecurity training, Healthcare, Cyber threats, Digital transformation

1. Introduction

The integration of information and communication technology in healthcare is rising, encompassing automated systems for diagnosing and gathering patient information (Rajamäki & Ruoslahti, 2021). In an era where digital technologies are increasingly integral to healthcare, enhancing both patient care and operational efficiency, the need to address cybersecurity has become paramount. This study seeks to examine and refine training and learning practices to promote a more cooperative approach within the healthcare sector, guaranteeing the reliability and accuracy of healthcare data in the face of escalating cyber threats. Digital advancements such as electronic health records (EHR), telemedicine, and smart devices have revolutionised the healthcare industry, improving communication and patient access to treatments. However, this digital shift brings substantial cybersecurity challenges. Cyberattacks represent a worldwide menace to patient safety and care, impacting all healthcare domains (Kamerer & McDermott, 2020). There has been a notable increase in cybercrime within the healthcare industry, emphasising the urgent necessity for stringent cybersecurity protocols (Clarke & Martin, 2024).

Healthcare organisations face vulnerabilities arising from software weaknesses, human mistakes, and information security shortcomings (Bulai et al., 2019; Sendelj & Ognjanovic, 2022). To counter these threats, continuous cybersecurity training programs are crucial. These should address strong password practices, phishing detection, secure data management, and device protection. Training must be customised to accommodate the varied needs and technical skill levels of distinct user groups (Clarke & Martin, 2024; Coventry et al., 2020; Sendelj & Ognjanovic, 2022). Despite sufficient training, keeping staff motivated to comply with cybersecurity protocols is challenging. Negligence or incorrect application of cybersecurity tools can result in data breaches (Alanazi, 2023). Research indicates that many healthcare staff feel undertrained and uninformed about secure technology use, leading to widespread frustration, and highlighting the need for comprehensive training programs (Coventry et al., 2020).

Healthcare workers on the front lines are pivotal in safeguarding Protected Health Information (PHI) and securing data for patients, colleagues, and other stakeholders (Kamerer & McDermott, 2020). Yet, the prevalence of cybersecurity attacks indicates that numerous healthcare institutions remain underprepared to

confront these challenges (Sendelj & Ognjanovic, 2022). Bridging this divide with improved training and cooperative learning methods is vital for advancing healthcare cybersecurity.

This study focuses on modifying training and learning practices to foster a more collaborative approach in the healthcare domain. The research question of this study is:

- How can training and learning practices be modified to improve healthcare professionals' cybersecurity awareness and compliance?

The rest of the paper is organised into five chapters. Chapter 2 presents a literature review pertinent to this study and outlines the document's scope. Chapter 3 offers both theoretical and practical backgrounds. Chapter 4 outlines the findings, and Chapter 5 provides conclusions of the study.

2. Literature

The evidence of cybersecurity attacks has shown that numerous sectors and industries, such as healthcare organisations and the industry as a whole, are still insufficiently ready to deal with these threats (Sendelj & Ognjanovic, 2022). Healthcare organisations must create ongoing training programs to teach their employees about cybersecurity best practices. The subjects that need to be included in these programs cover robust password management, identification of phishing attempts, secure data handling, and device security. Tailoring these training programs to meet the diverse demands and technical proficiency levels of distinct user groups is imperative. (Clarke & Martin, 2024; Coventry et al., 2020; Sendelj & Ognjanovic, 2022). Table 1 presents some key cybersecurity threats and prevention measures in the healthcare domain.

Table 1*:* Cybersecurity threats and prevention measures. Adapted from (Kamerer & McDermott, 2020)

Threat	Example	Preventive measure
Physical	Unintentional employee actions	Hard-copy documents are shredded or disposed
Portable devices	Lost or stolen device	Portable devices should be kept in secure storage areas
Insider use	Intentional breaches of cybersecurity protocols	Immediate reporting of any suspicious actions
Technical	Social engineering threats exploit human trust	Frequent password changes, updated systems
Administrative	A breakdown of day-to-day operations and policies	Training on data access and usage

Even with adequate training, staff members might lack the necessary motivation to adhere to cybersecurity measures, potentially leading to data breaches due to negligence or improper use of cybersecurity tools (Alanazi, 2023). According to (Coventry et al., 2020, p. 105) “a range of seven insecure behaviours were reported: poor computer and user account security; unsafe email use; use of USBs and personal devices; remote access and home working; lack of encryption, backups, and updates; use of connected medical devices; and poor physical security”. (Sendelj & Ognjanovic, 2022, p. 195) lists five of the most important healthcare organisations’ cybersecurity challenges as 1) e-mail phishing, 2) ransomware attack, 3) equipment or data lost and theft, 4) insider (accidental or intentional) data loss, and 5) attack on medical devices affecting patient safety. The five newest and most common cybersecurity threats to the healthcare sector according to (Department of Health & Human Services, 2023) are:

- Social engineering attack
- Ransomware attack
- Loss or theft of device or data
- Insider, accidental or intentional data loss, and
- Attacks on networked medical devices that may affect patient safety.

The lack of awareness is a concern and needs to be addressed through staff training (ENISA, 2023; Pollini et al., 2022). Coventry et al.'s research indicates that several staff highlighted the absence of cybersecurity training as an issue, with many believing undertrained and uninformed about the secure use of technology. The lack of adequate training has led to widespread frustration among Administrators, who often find themselves at the end of the line for training opportunities if they are provided with any. (Coventry et al., 2020). The widespread use of electronic health records (EHR), healthcare information systems, wireless communication and cloud services, and technology devices cause challenges to healthcare personnel in their daily work. They operate on

the front line and play a key role in protecting protected health information (PHI) and various stakeholders such as patients, colleagues, healthcare organisations and other caregivers, in ensuring data protection (Kamerer & McDermott, 2020).

Organising staff awareness and cybersecurity training is crucial to mitigate risks associated with human factors (ENISA, 2016). Developing and maintaining employee awareness requires personnel training in cybersecurity (Bulai et al., 2019) and regularly renewing the training of users is necessary (Haukilehto, 2024; Kioskli et al., 2023). The challenge of cybersecurity is not restricted to Information Technology (IT), it is a company-wide issue that requires commitment from all levels of the organisation, healthcare professionals, and managers. Organisations can overcome this challenge by engaging employees, enhancing education and awareness, and promoting transparency and coordination across the domain. (Department of Health & Human Services, 2023). The findings of (Jerry-Egemba, 2024) indicate the necessity to enhance the awareness and training of healthcare personnel to enhance cybersecurity through training programs. A comprehensive understanding of cybersecurity practices can be achieved through effective training programs including versatile delivery methods like computer-assisted modules, classroom instruction, and group discussions. (Jerry-Egemba, 2024; Nifakos et al., 2021).

(Rajamäki & Ruoslahti, 2021) suggest streamlining healthcare systems, increasing awareness, and identifying cybersecurity competencies while creating training programs for healthcare staff at all levels. Predefined security requirements simplify the creation of basic service levels and the attainment of desired security standards (Rajamäki & Ruoslahti, 2021). Healthcare organisations should allocate resources for ongoing training and awareness initiatives for all staff members. The importance of such programs lies in informing employees about cybersecurity best practices, data protection regulations, and the consequences of their actions. Employees must understand their pivotal role in upholding cybersecurity and thwarting insider threats. (Burrell, 2024). Cybersecurity training conducted by organisation's ICT professionals can significantly enhance employees' cybersecurity competencies and information security awareness (Ruoslahti et al., 2021). This empowers them to adequately defend themselves and safeguard the organisation's assets from cyber-attacks.

Beltempo (2024) interviewed cybersecurity experts and healthcare professionals and identified significant shortcomings in cybersecurity knowledge among healthcare workers based on document analysis and interview data. The interviews resulted in identifying emergency response, data protection, and risk management as critical competencies for healthcare workers. The interviewees relied on their general IT skills but admitted that they were not enough for the ever-changing threat landscape due to their lack of professional cybersecurity training. The findings indicate the need for a specific training program focusing on healthcare cybersecurity to address cybersecurity issues. (Beltempo, 2024)

3. Method

This study employs a qualitative study methodology developed using desktop research. The purpose of this study is to provide specific information that supports development activities in the healthcare sector. The study approach becomes particularly significant when research questions aim to explain a current phenomenon, including its causes and effects. The significance of the method lies in the necessity for a comprehensive and detailed description of specific social phenomena addressed in the questions. Employing case studies in various contexts can enhance comprehension of individuals, groups, organisations, and socio-political dynamics. (Benbasat et al., 1987; Dubé & Pare, 2003; Yin, 2009). Case studies are an excellent choice when looking for solutions to particular issues or when suggesting methods to advance research (Yin, 2009).

Existing cybersecurity policy documents, training materials, incident reports, and compliance records served as a basis for the data collection process. The results were validated by using multiple data sources to ensure data triangulation. The study's methodological approach ensured an accurate and detailed understanding of the current state of healthcare cybersecurity training and provided practical recommendations to enhance the effectiveness of training programs.

4. Results

While employees may be aware of external threats, they may not know how their actions contribute to threats. Awareness training ensures that employees are informed of the potential consequences of their actions at work. Safe behaviour among healthcare staff is not always promoted in a fast-paced and stressful environment. Personnel must be aware of dangerous practices and their potential consequences to engage in safe behaviour. Employers must convey to their employees the expectations set for them, the reasons for those expectations,

and where they can go for additional information or guidance. (Coventry et al., 2020). Internal and external cyber threats pose a risk to anyone with access to Electronic Health Records (EHR), particularly nurses who frequently access this information throughout their workday and might not realise the impact of their actions on the safety of patient information (Kamerer & McDermott, 2020).

The following table highlights existing challenges and solutions for the healthcare domain. The table explains the challenges, their descriptions, proposed solutions, and references, allowing for easier comprehension of the key points and the sources supporting them.

Table 2*:* Comparison of existing challenges and solutions

Challenge	Description	Proposed Solutions
Email Phishing	Phishing attacks target healthcare staff via email.	Ongoing training on identifying phishing attempts, robust email security protocols. (Department of Health & Human Services, 2023; Sendelj & Ognjanovic, 2022)
Ransomware Attack	Malicious software that encrypts data, demands ransom for decryption.	Regular backups, updated antivirus software, staff training on avoiding suspicious links. (Department of Health & Human Services, 2023; Sendelj & Ognjanovic, 2022)
Loss or Theft of Device/Data	Physical loss or theft of devices contains sensitive data.	Secure data handling practices, encryption, physical security measures. (Department of Health & Human Services, 2023; Sendelj & Ognjanovic, 2022)
Insider Threats	Accidental or intentional data breaches by employees.	Comprehensive training programs, strict access controls, monitoring systems. (Alanazi, 2023)
Attacks on Medical Devices	Cyber-attacks target networked medical devices and risk patient safety.	Regular updates and patches, secure network configurations, staff training. (Department of Health & Human Services, 2023; Sendelj & Ognjanovic, 2022)
Lack of Cybersecurity Training	Insufficient training leads to insecure behaviours.	Tailored training programs, regular updates, diverse delivery methods. (Coventry et al., 2020; Jerry-Egemba, 2024)
Poor Password Management	Weak or reused passwords compromise security.	Training on robust password practices, use of password managers. (Clarke & Martin, 2024; Coventry et al., 2020)
Unsafe Email Use	Insecure practices in handling emails.	Training on secure email practices, use of secure email systems. (Coventry et al., 2020)
Use of USBs and Personal Devices	Risks from the use of personal devices and USBs.	Policies restricting use, secure device management practices. (Coventry et al., 2020)
Remote Access and Home Working	Security risks from remote work setups.	Secure remote access protocols, VPN usage, training on secure remote work practices. (Coventry et al., 2020)
Lack of Encryption, Backups, and Updates	Failure to encrypt data, backup systems, and update software.	Regular encryption, scheduled backups, timely software updates. (Coventry et al., 2020)
Poor Physical Security	Inadequate physical security measures.	Implementing physical security protocols, training on physical security. (Coventry et al., 2020)

Significant issues can arise from employee actions that are not intentional, such as improper document disposal. All hard-copy documents must either be shredded or disposed of properly. Notify IT security immediately of any lost or stolen devices and keep portable devices in secure storage areas or designated charging stations. Breaking cybersecurity protocols intentionally, such as unauthorised access or data deletion, is a serious offence. Identity theft, ransomware, phishing, and spoofing are social engineering threats that exploit human trust. A detailed analysis of the regular management and maintenance tasks within an organisation is necessary to break down

day-to-day operations and policies. These encompass staff management, project oversight, budget monitoring, and ensuring the achievement of organisational objectives.

Healthcare professionals need to be informed about cybersecurity threats that can impact their practices and patients, given the recent proliferation of healthcare technology and the uncertainty of future technological disruptions. Given the rapid expansion of healthcare technology and the potential for future technological disruptions, healthcare actors must be educated about cybersecurity threats that could impact their practice and their patients (Rajamäki et al., 2024). Every individual working in the healthcare sector should be trained in preventing and managing cybersecurity threats (Bulai et al., 2019; Kamerer & McDermott, 2020).

The fight against cyber-attacks requires policies and procedures established at the organisational level. Technical procedures and recommended protection mechanisms can be used to develop cyber hygiene and ensure personnel's appropriate response. The organisation's cybersecurity cannot be improved by simply implementing technical practices; it requires continuous risk assessment and management within the framework of technical practices for effective and rapid improvement (Sendelj & Ognjanovic, 2022).

Regular training programs for their staff are necessary for healthcare organisations to strengthen their cyber security measures (Burrell, 2024; Kioskli et al., 2023; Rajamäki et al., 2024). Employees are kept up to date with the latest threats through this, and a culture of vigilance is developed. Adding cybersecurity modules to disciplines' curricula is essential for professionals to effectively contribute to improving cybersecurity in healthcare (Jerry-Egemba, 2024). Healthcare professionals are advised to receive comprehensive and ongoing cybersecurity training (Nifakos et al., 2021). It must be tailored to their specific tasks and encompass technical skills, risk identification, and the security of protected health information. The overall cybersecurity posture is strengthened by promoting information sharing among organisations. The protection of patient data and the reliability of the healthcare system requires increasing cybersecurity awareness and strengthening the culture of responsibility. Safe patient care in the digital age requires a comprehensive understanding of cybersecurity. (Jerry-Egemba, 2024).

5. Discussion and Conclusions

Acknowledging the safety hazards associated with their responsibilities, healthcare professionals ought to undergo training. This training should concentrate on secure data exchange, mobile device data protection, the utilisation of secure communication channels, and protocols for responding to incidents. Moreover, training sessions are vital in helping staff understand the potential repercussions of data breaches and their responsibility to avert them. Addressing interoperability issues among healthcare end users necessitates a proactive, collaborative stance on cybersecurity risk management. It is imperative for all parties involved to exercise diligence in upholding the security strategy. By educating end users, we foster a secure operational environment in healthcare, thereby preserving the integrity of patient safety.

Healthcare organisations face challenges when implementing cybersecurity measures, including a shortage of time and resources. Rapid changes can be challenging, leading to inefficient processes and stakeholders' frustration. Healthcare organisations also face challenges when promoting cybersecurity awareness and culture. Personnel participation in training and workshops is necessary to establish a secure operating environment. The strength of an organisation is determined by its weakest link. The staff must be kept up to date on the importance and basics of cybersecurity measures. Continuous training ensures that employees have the necessary cybersecurity knowledge and skills.

Healthcare organisations can face operational delays due to cyber-attacks. To swiftly address any disruptions, it is important to have well-defined procedures for employees to follow. Cybersecurity encompasses the protection of data and the detection and response to cyber-attacks. Human error can lead to security breaches, even with advanced technical safeguards. Healthcare personnel's lack of knowledge and training in cybersecurity can lead to errors that can be mitigated with education and appropriate training. Many technical security features are available to protect against cyber-attacks and threats, but the human factor remains one of the most common concerns, according to the literature.

The importance of cybersecurity threats, which are a part of everyday life, should not be overlooked by healthcare organisations. The wide range of opportunities for attention and potential value that healthcare organisations provide, from public exposure to financial gain, makes them attractive targets for attackers. The healthcare organisation's size is not the primary factor. Medical information systems that manage patient data and integrate medical devices and other subsystems can be the targets of cyber-attacks. Cyber-attacks are constantly evolving and becoming more sophisticated. Healthcare institutions should prioritise investing in

cybersecurity. Patient protection can be improved by investing in cybersecurity. Healthcare organisations must summarise the lessons learned from recorded cyber-attacks to strengthen cybersecurity.

Healthcare organisations should ensure that all employees (e.g. doctors, nurses, paramedics, laboratory technicians, administrative personnel and IT experts) receive ongoing training and awareness programs. Staff members are educated on cybersecurity best practices, data protection policies, and the possible consequences of their actions through these programs. Employees should be aware of the steps needed to maintain cybersecurity and prevent insider threats. Healthcare cybersecurity best practices can be implemented through training to protect sensitive patient data and ensure the smooth operation of healthcare. The example cases in Table 3 can be used as cybersecurity training topics for healthcare personnel.

Table 3*:* Examples of training cases

Case	Training	Practices
Email: Phishing (Ransomware)	Training employees to recognise phishing messages and be cautious with email attachments.	Clear instructions on how to handle suspicious emails and who to report potential threats to.
IoT/IoMT Device on Network	Training staff on cybersecurity and identifying vulnerabilities.	Regular software updates and vulnerability patches are essential.
Risks Related to Cloud Services, Use of Generative AI, and Communication Applications	Training staff on security practices and handling sensitive information.	Clear instructions on handling sensitive information and which tools to use for processing. Use reliable anti-malware software
Remote Work	Training staff on security practices and handling sensitive information.	Sensitive discussions should be held in private spaces where outsiders cannot hear.
Locking Computers from Unauthorized Access/Access Permissions	Training staff on security practices and handling sensitive information.	Computers should be locked whenever not in use, and passwords should be stored securely.
Misused User Credentials	Training staff and students on security practices and handling sensitive information.	Each user should have their credentials and not share them with others. Implement two-factor authentication (2FA) in all possible systems.
Shoulder Surfing	Training staff on security practices and handling sensitive information.	Use screen protectors to prevent side viewing, especially in public spaces. Computers should be locked whenever not in use. Passwords are stored securely.
Connecting USB to Computer	Training staff on security practices and not connecting unknown USB devices to computers.	Encrypt sensitive data to prevent it from being easily accessible even if spyware enters the system. Clear instructions and practices should be followed when handling unknown objects.
Password Recycling	Training staff on security practices and handling sensitive information.	Use strong and unique passwords for different services. Use a password manager. Implement two-factor authentication (2FA).
Software updates not being applied	Train staff on information security practices and identify the need for updates.	Establish a routine schedule for checking and applying software updates. Use automated tools to manage and deploy updates across all systems.

The training goals of cybersecurity are to enhance employees' awareness of cybersecurity, ensure the safe handling of personal data, and ensure business continuity and recovery after disruptions. The most effective way to protect against cyber threats is to provide comprehensive training programs to all healthcare professionals. Annual training should be given to all employees that cover the safe handling of customer data and its appropriate sharing on social media platforms. Through this method, employees can learn to identify and avoid the most common cyber threats, such as email phishing attacks. Improving cybersecurity awareness among healthcare professionals can be achieved by developing training and learning practices. This can be implemented, for example, by including modules related to cybersecurity in healthcare continuing education,

by organising regular workshops and simulation exercises, and by ensuring that cybersecurity is part of everyday activities and decision-making in healthcare. Training enables healthcare personnel to acquire and maintain a staff skilled in cybersecurity, bolsters preparedness for incident response and enhances overall productivity.

Future research topics should examine how different training methods, like online modules, in-person workshops, and simulations, can improve cybersecurity awareness and compliance among healthcare professionals. Another future research topic could investigate the impact of training programs tailored to specific roles in healthcare organisations (such as nurses, physicians, and administrators) on cybersecurity practices and vulnerability reduction.

Acknowledgements

This study has received funding from the European Union project DYNAMO, the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 101069601 and The Cybersecurity in Everyday Work in the Social and Healthcare Sector (KyberSoTe) project. The views expressed are those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

References

Alanazi, A. T. (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. *Cureus*, *15*(10), e47026. https://doi.org/10.7759/cureus.47026

Beltempo, E. (2024). *Implementation of the ECHO Cyber-Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities* [Thesis, Laurea University of Applied Sciences]. https://www.theseus.fi/bitstream/handle/10024/869217/Beltempo_Eleonora.pdf?sequence=2&isAllowed=y

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. https://doi.org/10.2307/248684

Bulai, R., Țurcanu, D., & Ciorbă, D. (2019). Education in Cybersecurity. *Central and Eastern European eDem and eGov Days*, *335*, 33–44. https://doi.org/10.24989/ocg.v335.2

Burrell, D. N. (2024). Understanding Healthcare Cybersecurity Risk Management Complexity. *Land Forces Academy Review*, *29*(1), 38–49. https://doi.org/10.2478/raft-2024-0004

Clarke, M., & Martin, K. (2024). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum*, *37*(1), 17–20. https://doi.org/10.1177/08404704231195804

Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Cyber-Risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour. In *HCI for Cybersecurity, Privacy and Trust* (pp. 105–122). Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-50309-3_8

Department of Health & Human Services. (2023). *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*. Healthcare & Public Health Sector Coordinating Council. https://405d.hhs.gov/Documents/HICP-Main-508.pdf

Dubé, L., & Pare, G. (2003). Rigor In Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. *MIS Quarterly*, *27*(4), 597–635. https://doi.org/10.2307/30036550

ENISA. (2016). *Cyber security and resilience for Smart Hospitals*. European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

ENISA. (2023). *ENISA Threat Landscape: Health Sector* (Threat Landscape Report No. TP-04-23-546-EN-N; p. 36). European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/health-threat-landscape

Haukilehto, T. (2024). *Cybersecurity management in healthcare: Policies, awareness and incident reporting* [Academic Dissertation, University of Vaasa]. https://osuva.uwasa.fi/bitstream/handle/10024/17420/978-952-395-140-2.pdf?sequence=2&isAllowed=y

Jerry-Egemba, N. (2024). Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs. *Healthcare Management Forum*, *37*(1), 21–25. https://doi.org/10.1177/08404704231194577

Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the Front Line of Prevention and Education. *Journal of Nursing Regulation*, *10*(4), 48–53. https://doi.org/10.1016/S2155-8256(20)30014-4

Kioskli, K., Fotis, D. T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. *Applied Sciences*, *13*(6), 3410. https://doi.org/10.3390/app13063410

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors*, *21*(15), Article 15. https://doi.org/10.3390/s21155119

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Rajamäki, J., & Ruoslahti, H. (2021). ECHO Federated Cyber Range as a Tool for Validating SHAPES Services. *Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021*, *53*, 623–627. https://doi.org/10.34190/EWS.21.076

Rajamäki, J., Wood, K., & Espada, B. (2024). LOCKing Patient Safety: A Dynamic Cybersecurity Checklist for Healthcare Workers. *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, *23*(1), 807–811. https://papers.academic-conferences.org/index.php/eccws/article/view/2072

Ruoslahti, H., Coburn, J., Trent, A., & Tikanmäki, I. (2021). Cyber Skills Gaps – A Systematic Review of the Academic Literature. *Connections: The Quarterly Journal*, *20*(2), 33–45.

Sendelj, R., & Ognjanovic, I. (2022). Cybersecurity Challenges in Healthcare. *Studies in Health Technology and Informatics*, *300*, 190–202. https://doi.org/10.3233/SHTI220951

Yin, R. K. (2009). *Case study research: Design and methods* (No. 1; 4th ed., Vol. 14). Thousand Oaks, CA: Sage Publications. https://journals.nipissingu.ca/index.php/cjar/article/view/73