Enhancing Cybersecurity in Healthcare: The KyberSoTe Project's Approach to Mitigating Cyber Threats

Ilkka Tikanmäki[1, 2], Tiina Blek[3], Johanna Niskakangas[3] and Katja Varamäki[4]
[1]Safety, Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland
[2]Department of Warfare, National Defence University, Helsinki, Finland
[3]Jamk University of Applied Sciences, Finland
[4]Tampere University of Applied Sciences, Finland

Ilkka.tikanmaki@laurea.fi
Tiina.blek@jamk.fi
Johanna.niskakangas@jamk.fi
Katja.varamaki@tamk.fi

Abstract In today's digital age, healthcare organisations are increasingly vulnerable to cyberattacks, making cybersecurity a crucial component of healthcare management. Protecting sensitive patient, medical, and personal data against hackers, cybercriminals, and other malicious entities cannot be understated. The CIA triad—confidentiality, integrity, and availability—is fundamental to cybersecurity in healthcare, safeguarding data privacy, accuracy, and access. The Cybersecurity in Everyday Work in the Social and Healthcare Sector (KyberSoTe) project is designed to identify prevalent cyber threats social and healthcare professionals encounter by utilising high-quality research, surveys, and firsthand data. Organisations in the social and healthcare sectors must implement practices to strengthen the cyber-safe behaviour of their personnel. The importance of cybersecurity lies in the presence of educated staff and a robust information security culture, as cybersecurity often relies on human vulnerability. Despite the increasing frequency of cyberattacks, awareness of cybersecurity threats and the impact of individual actions on organisational security remains low among social and healthcare professionals. The social and health sector faces a growing threat from cyberattacks, necessitating preparedness for present and future risks. Hospitals have adopted various strategies, such as enhanced staff training, endpoint management, stakeholder coordination, and anti-virus solutions, to bolster their cyber resilience. National and international organisations recommend measures, including software and application security, infrastructure protection, cloud and IoT security, and robust security management systems. Key components of cyber resilience include access control, information security, network security, and user security. Healthcare facilities can prevent cyberattacks through staff training, routine system updates, and advanced security tools. Prioritising cybersecurity and establishing detailed strategies and contingency plans are crucial for preventing intrusions. Insufficient security standards and a lack of comprehensive security strategies are reasons why hospitals are particularly vulnerable. Preventing data breaches that threaten patient data requires urgent attention to cybersecurity and cyber-hygiene practices. Healthcare institutions must develop clear policies and contingency plans to manage potential cyberattacks and their consequences. Emphasising the importance of cybersecurity, healthcare organisations must take proactive measures to safeguard sensitive patient data and prevent losses from system failures, reputational damage, and other cyberattack-related issues.

Keywords: Cybersecurity, Staff training, Cyber threats, Social and healthcare sector

1. Introduction

In the current era of digitalisation, the growing threats of cyberattacks target healthcare organisations and that's why cybersecurity is an important part of healthcare management (Barnett et al., 2024; Haukilehto, 2024; Rajamäki et al., 2024). Protecting electronic information and digital assets from unauthorised access, use, and disclosure is part of healthcare cybersecurity. Protecting sensitive patient information, medical information, and personal information from potential hackers, cybercriminals, and malicious actors is part of this. (Alanazi, 2023). The CIA triad, is the acronym for confidentiality, integrity, and availability, which are cybersecurity's primary goals in healthcare (Haukilehto, 2024). Confidentiality relates to the importance of personal information and safeguards it from unauthorised access. To maintain integrity, it is necessary to ensure that data is accurate and has not been manipulated or altered. Authorised users guarantee the availability of information to ensure it is accessible when required.

The main objective of the KyberSote project is to promote cyber preparedness, continuity of services and patient safety in social and healthcare organisations. The project will increase cybersecurity skills and the use of cybersecurity approaches among health professionals and strengthen cooperation between healthcare and IT professionals in cybersecurity. The project is structured around high-quality research data, existing surveys, and experience-based information from Finnish Wellbeing Service Counties. Due to their importance in disseminating information to personnel, the target audience is Wellbeing Service Counties management, decision-makers, and healthcare staff. The KyberSoTe project, financed by the Digital Security 2030 programme

of the National Emergency Supply Agency, produces training content that increases the cybersecurity expertise of social and healthcare professionals. (The National Emergency Supply Agency, 2023).

The topic is approached from two perspectives. The project's first perspective is to enhance the cybersecurity expertise of social and healthcare professionals. The second perspective in this project is to improve collaboration between the social and healthcare industry and information management professionals in cybersecurity. The social and healthcare sectors produce services that are central to the functioning of society, the continuity of which can be secured by improving the cybersecurity and information security skills of professionals in the sector. Cybersecurity content must be created in the social and healthcare education offerings, which supports the skills of future professionals in the field. The main implementer of the KyberSoTe project is Jyväskylä University of Applied Sciences, and the partial implementers are Laurea, Turku, and Tampere Universities of Applied Sciences. The project will be carried out during the years 2024-2026.

The research question of this study is:

- How can healthcare organisations enhance their cybersecurity practices to protect sensitive data and ensure service continuity in the face of increasing cyber threats?

The research question can help explore different cybersecurity dimensions in healthcare, from training and collaboration to technology and impact assessment. The research question addresses the core issues of improving cybersecurity awareness and practices among healthcare professionals, developing effective tools and models for evaluating and mitigating cyber threats and preparing for current and future cyber risks. The rest of the paper is structured into five chapters. Chapter 2 presents a literature review relevant to this study and defines the scope of the document. Results and practical background information are provided in Chapter 3. The findings are detailed in Chapter 4, and the study is concluded in Chapter 5.

2. Literature Review

The number of incidents and the impact on healthcare organisations are impacted by Ransomware, which is one of the most significant healthcare threats (54%). A data breach or data theft is the cause of 43% of ransomware cases. Another common consequence of an attack is disruption. The threats to health organisations' data (data breaches and leaks) account for almost half of all cases (99 cases, 46%). Data-related threats are still a major threat to society, not only in Europe but also worldwide. (ENISA, 2023a). One of the top five attacks in the healthcare sector is attacks on connected medical devices, which can impact patient safety (Sendelj & Ognjanovic, 2022). Novice and experienced nurses struggle with how technologies should be used and have little knowledge of how their use can impact patient safety (Kamerer & McDermott, 2020).

(Aljuraid & Justinia, 2022; Sunil & Mathew, 2024) articles, categorise cyber threats into subcategories. Those include insider threats, cybersquatting threats, and technological failures. Table 1 presents cyber security threats in the hospital environment by threat type and category.

Ransomware poses a significant threat to healthcare organisations, accounting for 54% of incidents, with data breaches or theft responsible for 43% of these cases. Disruption is another common consequence. Data-related threats, including breaches and leaks, represent nearly half of all cases (46%), highlighting their global impact (ENISA, 2023a). Attacks on connected medical devices, which can jeopardise patient safety, are among the top five threats in the healthcare sector (Sendelj & Ognjanovic, 2022). Both novice and experienced nurses often lack the knowledge to use technologies safely, impacting patient safety (Kamerer & McDermott, 2020).

Cyber threats in healthcare can be categorised into insider threats, cybersquatting threats, and technological failures (Aljuraid & Justinia, 2022; Sunil & Mathew, 2024). Table 1 classifies these threats by type and category.

Table 1*:* Classification of cyber security threats in hospital environments. Adapted from (Sunil & Mathew, 2024)

Threat type	Category	Potential motivation
Malware	Cybersquatting	The theft of sensitive information such as passwords. Ransom demands caused by a data breach.
Dos attack	Technological threats	System disturbances lead to system breaches and ransom demands.
Phishing	Cybersquatting	Theft of personal information, data breaches, and facilitation of other attacks

Threat type	Category	Potential motivation
Masquerade attacks	Technological threats	Acquiring sensitive information, changing/deleting patient health details.
Data injection attacks	Technological threats	Causing misdiagnosis, insurance fraud, and mission-critical interruptions.
Hardware/software malfunctions	Insider threats	Often by accident, can lead to inadequate service provision.
Hospital information system outdated technology	Insider threats	Unintentionally, can lead to unreliable systems.
Critical infrastructure failure	Insider threats	Unintentional, can result in serious consequences, such as data loss.
Human usability errors	Insider threats	Often due to carelessness, which causes significant data security risks.
Management weakness	Insider threats	Often unintentionally due to resource constraints or lack of expertise.

Insider threats can be caused by human errors like careless behaviour, lack of awareness, or unintentional security breaches (such as unauthorised password sharing) (Kamerer & McDermott, 2020). The malicious activities involved in cybersquatting include hacker infiltration, spyware, malware attacks, viruses, and data breaches. The impact of technical faults can be seen in hardware, software, infrastructure, and electrical systems. (Aljuraid & Justinia, 2022; Sunil & Mathew, 2024) Cyber threats can be avoided using technical protections like strong firewalls and anti-virus software. Staff safety is crucial in ensuring strong cyber security, but it has been largely ignored. Cybersecurity is not only a technical problem but also a complicated socio-technical one. The 'weakest link' in cybersecurity is frequently referred to as staff behaviour due to it being one of the primary causes of cybersecurity vulnerabilities. (Coventry et al., 2020).

According to the study of (Al-Qarni, 2023), healthcare institutions should take proactive measures to guarantee the security of sensitive patient information and decrease system errors, reputational damage, and other related issues. Hospitals are required to protect a wide range of assets that are crucial to their operations. While some smart hospital resources are important in traditional and smart hospitals, they are distinctive because they are intelligently connected and can make decisions independently. Mobile client devices, identification systems, and connected clinical information systems are just some of the things that fall under this category. (ENISA, 2016). European Union Agency for Cybersecurity (ENISA) summarise the specific assets of smart hospitals displayed in Table 2.

Insider threats often stem from human errors such as careless behaviour, lack of awareness, or unintentional security breaches like unauthorised password sharing (Kamerer & McDermott, 2020). Malicious activities in cybersquatting include hacker infiltration, spyware, malware attacks, viruses, and data breaches. Technical faults can impact hardware, software, infrastructure, and electrical systems. (Aljuraid & Justinia, 2022; Sunil & Mathew, 2024). While technical protections like strong firewalls and antivirus software can mitigate cyber threats, staff safety remains crucial but often overlooked. Cybersecurity is a complex socio-technical issue, with staff behaviour frequently cited as the 'weakest link'. (Coventry et al., 2020)

Healthcare institutions should proactively secure sensitive patient information to reduce system errors, reputational damage, and other issues (Al-Qarni, 2023). Hospitals must protect a wide range of assets crucial to their operations. Smart hospital resources, distinct due to their intelligent connectivity and autonomous decision-making, include mobile client devices, identification systems, and connected clinical information systems (ENISA, 2016). European Union Agency for Cybersecurity (ENISA) summarise the specific assets of smart hospitals displayed in Table 2.

Table 2: Overview of smart hospital assets. Modified from: (ENISA, 2016, pp. 13–15)

Asset	Description
Remote care system assets	Monitoring the patient's condition and measures related to treatment.
Networked medical devices	Portable terminals, wearable technology, assistive robots.
Identification systems	Smart bracelets, biometric scanners.

Asset	Description
Networking equipment	Connecting the above-mentioned remote devices to the hospitals' systems.
Mobile Client devices	Applications for mobile terminals, with which the necessary information travels with the nursing staff.
Interconnected clinical information systems	Information systems used for storing and processing patient information.
Data	Clinical patient information or research information, information related to personnel or information related to hospital operations.
Building and facilities	Building automation supports the operation of the smart hospital.

An ICT ecosystem is the foundation of a telehealth system, which enables a "smart hospital to extend its boundaries and provide healthcare services to patients at remote locations" (ENISA, 2016, p. 13). Patient monitoring and implantable device upgrades are made possible through networked medical devices. Clinical information systems are connected to fixed and mobile devices, resulting in increased automation and improved decision-making ability. Using identification systems involves tracking and identifying patients, staff, or hospital equipment. Devices and information systems are intelligently connected to biometric scanners. Hospitals depend on network devices to support their connections. Improved features such as routing protocols and bandwidth are characteristics of the necessary devices.

An ICT ecosystem forms the backbone of telehealth systems, enabling smart hospitals to extend their services to remote locations (ENISA, 2016). Networked medical devices facilitate patient monitoring and implantable device upgrades, while clinical information systems connected to fixed and mobile devices enhance automation and decision-making. Identification systems track and identify patients, staff, and equipment, integrating with biometric scanners. Hospitals rely on network devices for connectivity, requiring improved routing protocols and bandwidth. (Osama et al., 2023)

It is increasingly important for healthcare organisations to identify cybersecurity risks and prioritise effective measures to protect patient safety. One key approach is implementing cybersecurity training. Staff awareness of best practices in cybersecurity and data protection, and understanding the organisation's security guidelines are fundamental and crucial for each organisation's cybersecurity. (Cascella, 2022). Training should reach all healthcare professionals, including nurses, doctors, and other clinical staff (Jerry-Egemba, 2024).

Smooth and effective collaboration between IT professionals and healthcare professionals is essential to balance cybersecurity and the efficiency of daily operations. Communication and information channels designed for the organisation and work units facilitate mutual communication and enable flexible interaction. These channels can include regular email communication and newsletters. Involving healthcare professionals in security policies helps them understand the importance of cybersecurity and allows them to influence the implementation of security measures without disrupting patient care. Healthcare professionals should also have the opportunity to provide feedback on systems that hinder workflows. (Clarke & Martin, 2024)

3. Methodology

The methodology used in this study is qualitative research developed through desktop research. Creating social and cultural theory can be achieved through qualitative research (Alasuutari, 1996). The study entails a comprehensive analysis of documents, emphasising scientific, sectoral and political content pertinent to social and healthcare information security and cybersecurity (Alasuutari, 2003). The study uses high-quality research data and current surveys from Wellbeing Service Counties for its methodology (Patton, 2002). The development of KyberSoTe project's activities is assisted by providing detailed information through this approach. This is ideally suited for exploring contemporary phenomena and their underlying causes and consequences. The method's significance is due to the need to describe the particular social phenomena completely and strictly being investigated. Qualitative research is effective in enhancing understanding of individual, group, organisational, and socio-political dynamics, as demonstrated by (Benbasat et al., 1987; Dubé & Pare, 2003; Yin, 2009).

The project behind this study is focused on improving the cybersecurity proficiency of social and healthcare organisations and enhancing collaboration between social and healthcare professionals and information management professionals. Jyväskylä, Laurea, Turku, and Tampere Universities of Applied Sciences in Finland are conducting the project between 2024 and 2026. The methodology aims to address key issues relating to

enhancing awareness and cybersecurity practices of healthcare professionals. The development of effective tools and models to assess and mitigate cyber threats can help to prepare for current and future cybersecurity risks.

4. Results

This chapter is divided into three subchapters, which discuss cybersecurity threats to healthcare, threats and vulnerabilities to medical devices, and threats to the operational environment.

4.1 Cybersecurity Threats to Healthcare

Cybersecurity threats in the healthcare sector can significantly impact the economy and the medical care of patients. An attacker's attack on an entire system can, in the worst case, result in the death of several patients. Due to the inherent vulnerability of its systems, the healthcare sector faces more threats than other sectors. Healthcare systems are vulnerable to damage caused by weaknesses that can be exploited. Hardware, software, networks, operating systems, medical devices, processes, and even people are some of the weaknesses mentioned (Kamerer & McDermott, 2020). eHealth devices are a growing threat: they contain highly sensitive information, and patient safety can depend on their reliability. A cyberattack can result in patient safety issues, e.g., medical devices or IT services are unavailable in an emergency (ENISA, 2023a). Some threats to the healthcare sector are depicted in Table 3 below.

Table 3*:* Cyberthreats to the healthcare sector

Threat	Description
Malicious network traffic	A suspicious connection or file created or obtained by a network.
Man-in-the-middle Attack	An eavesdropping attack where an attacker blocks current correspondence or communication.
Phishing	A strategy to trick victims by sending emails with data collection links.
Ransomware	An attacker encrypts a victim's files and then requests money from the target to obtain the encrypted data.

A network creates or obtains suspicious connections or files considered malicious traffic. The initial step for this threat is obtaining network access to a hostile website through an application. Malicious implementation occurs when the network software is overridden, which could involve illegal software downloads and spying (Aljuraid & Justinia, 2022; Sunil & Mathew, 2024). An attacker blocking current correspondence or communication is known as a man-in-the-middle attack. The correspondence or data transfer process requires programmers to create a real person, and then they wake up to immerse themselves in it. The objective of this kind of attack is to listen to the conversation and gather important information. The high value of healthcare makes it a popular target for criminals (Alanazi, 2023). Phishing is a method used to trick people by sending emails that contain data collection links. Customised messages are created by attackers using information collected from websites, virtual entertainment accounts, and other sources. The beneficiary's curiosity, pressure, or vanity are expected from these messages. The attacker uses ransomware-type cyber threats to encrypt the victim's files. Cyber attackers use malware to prevent victims from accessing their computers until they pay a ransom. To recover the encrypted data, the cyber attacker demands money from the target (ENISA, 2016). When ransomware attacks hit the healthcare industry, critical operations are completely shut down. Following this, healthcare professionals revert to manual operating techniques. This effect delays medical processes and wastes money that could have been used to improve the hospital.

4.2 Threats and Vulnerabilities to Medical Devices

The next five scenarios are crucial for smart hospitals (Table 4). Each of the scenarios discussed could affect traditional hospitals. Smart hospitals may have trouble protecting themselves from these attacks, and if they become victims, they may face severe consequences (ENISA, 2016). Protection becomes difficult due to the many potential points of attack caused by the large number of devices connected to the network. The consequences can be worsened due to the close connection between information systems and devices in hospitals and across organisational boundaries.

Table 4*:* Threats to medical devices

Threat type	Description
Social Engineering Attack on Hospital Staff	Sensitive information gathering, computer-based social engineering.
Tampering with Medical Devices	Getting access to the device is a prerequisite for tampering with it.
Theft of Hospital Equipment	Device theft has become more important due to the popularity of mobile and wearable devices.
Ransomware Attack on Hospital Information Systems	A type of malware that restricts access to an infected computer system and requires the user to pay a ransom to remove the restriction.
Distributed Denial-of-Service (DDoS) Attack on Hospital Servers	An attempt to make a network resource or information system unavailable to its intended users.

The human element of hacking is social engineering (Kamerer & McDermott, 2020). Attacks can be categorised into two categories. Social engineering is based on humans and involves gathering sensitive information through person-to-person interactions and exploiting human traits like trust, fear, or helpfulness, while phishing and baiting are examples of computer-based social engineering. Patient safety, privacy, and hospital operations are all at risk when medical devices are interfered with, particularly if they function as a gateway to the hospital network. Tampering with the device requires access to it. Hacking is the term used to describe illegally accessing a device or computer system (ENISA, 2023a). Devices can be tampered with by legitimate accesses, but it's not always a hack. The act of stealing hospital equipment or hardware without the owner's consent is called hospital equipment or hardware theft. Equipment theft has become even more important in smart hospitals due to the proliferation of mobile and wearable devices.

Mobile and wearable devices are the primary assets affected, but other equipment, such as identification components, may also be affected (ENISA, 2023b). The theft of equipment can harm sensitive information. Ransomware attacks have become increasingly common in hospitals. Ransomware is a kind of malware that restricts access to the infected computer system and asks the user to pay a ransom to get rid of it (ENISA, 2023a). Infected email attachments and an existing botnet are commonly used by ransomware to spread malware. An attempt to prevent the use of an information system or other network resource by its intended users is known as a denial of service (DoS) attack. If there are multiple sources of attack, it is classified as a distributed attack. Denial-of-service attacks can be launched using many different programs. Botnets often flood a targeted network resource with traffic, leading to Distributed Denial of Service (DDoS) attacks. Not only are hospitals affected by DDoS attacks, but medical devices connected to the network are also susceptible to hijacking and misuse as part of botnets.

4.3 Threats to the Operational Environment

Malicious actions and human errors pose a significant risk. Malware, social manipulation, hacking, denial of service, and device tampering are the threats that malicious activities emphasise. Smart hospitals face significant risks due to human errors such as user error, non-compliance with policies and procedures, and the loss of hardware. Theft often leads to the loss of devices and other equipment. From a cybersecurity perspective, typical examples of insecure human behavior are related to poor computer and user account security, unsafe use of email, use of USBs, personal devices and connected medical devices, remote working, lack of updates, encryption and backups, and last but not least, poor physical security (Coventry et al., 2020). The underlying causes are often ignorance and inadequate skills (Aljuraid & Justinia, 2022; Kamerer & McDermott, 2020). Additionally, taking risks, carelessness and curiosity (Aljuraid & Justinia, 2022), as well as repetitive, routine tasks and fatigue, increase the risk of cybersecurity failure (Jerry-Egemba, 2024). Table 5 provides an overview of the threats that smart hospitals may face.

Table 5*:* Threats to smart hospitals. Modified from (ENISA, 2016, p. 21)

Threat	Example
Malicious actions	Malware Hijacking Medical device tampering Social engineering attack Device and data theft Skimming Denial-of-service (DoS) attack

Threat	Example
Human error	Medical system configuration error Absence of audit logs Unauthorised access control Non-compliance Physician and/or patient errors
System errors	Software failures Inadequate firmware Network components failure Overload Communication between IoT and non-IoT
Supply chain failure	Cloud service providers Medical device manufacturer Network providers Power suppliers
Natural phenomena	Earthquakes Flood Fires

The most important resources and multiple root causes are used to present potential attack points and threat types. Malicious activity, human error, system and third-party failures, and natural phenomena are the primary causes of threats facing smart hospitals. Smart hospitals are the focus of the taxonomy of threats, which also encompasses cybersecurity aspects for all IT systems.

5. Conclusions

Organisations in the social and healthcare fields need to have practices that strengthen the cyber-safe behaviour of personnel. In addition to technical means to protect organisations, educated personnel and a strong information security culture are needed. Cybersecurity is often based on people's vulnerability. Despite this, cybersecurity threats and risks are still not well-known among social and healthcare professionals. Furthermore, there is an insufficient comprehension of how their actions affect the organisation's cybersecurity. The project Cybersecurity in Everyday Work in the Social and Healthcare (KyberSoTe) develops tools and operating models to enhance the evaluation of cyber security levels within health organisations. The design of it and its development are intended to address both current and future cyber threats. Additionally, the project's training content helps future professionals develop cyber skills in social security training.

The social and healthcare sector is facing a growing threat from cyber-attacks. Preparing for both current and future cyber threats is necessary. To respond to increased data security and protection challenges, organisations in the social and health sectors must improve their ability to do so. The social and healthcare sector processes a lot of sensitive and confidential customer and patient data. The 'dark market' is enriched by this data, which makes the sector intriguing from the perspective of cybercriminals. The disclosure of the Vastaamo data breach in October 2020 marked a significant cyberattack on Finland's social and healthcare sectors.

Hospitals have implemented various strategies to enhance their resilience to meet cybersecurity needs. The control system is improved by enhancing personnel training, simplifying endpoint management, coordinating stakeholders' interests, and integrating anti-virus solutions. Numerous national and international organisations have played a significant role in developing defence strategies against cyber threats on a larger scale. A wide range of measures are recommended, including security for software and applications, infrastructure protection, cloud security, IoT security, and the construction of robust security management systems. The importance of access control, information security, network security and user security are highlighted as key components in strengthening cyber resilience.

Social and healthcare facilities can use staff training, routine system updates, and state-of-the-art security tools to prevent cyber-attacks. It is important for hospitals to prioritise cybersecurity and have detailed strategies and contingency plans in place to prevent intrusions. Scientific studies have found that hospitals are vulnerable to

attacks because of insufficient security standards. The lack of a comprehensive security strategy in most healthcare organisations shows a lack of attention to cybersecurity. Healthcare institutions must address cybersecurity breaches that could threaten patient data. Healthcare organisations need to create concrete policies and plans for dealing with the potential consequences of cyber-attacks on hospitals, which can result in serious consequences.

Innovative techniques and tools could be developed in future research to protect healthcare companies against cyber-attacks. For instance, research can examine how machine learning and artificial intelligence can be utilised to detect and prevent cyber-attacks in hospitals. Furthermore, studies could examine the impact of cyberattacks on patient safety and consider the ethical implications of data breaches in the healthcare industry. The importance of cybersecurity in the healthcare industry is emphasised, and healthcare companies need to take proactive measures to safeguard sensitive patient data and patient safety. Healthcare organisations should prioritise cybersecurity to prevent losses from system failures, reputational damage, and other related issues caused by cyberattacks against hospitals.

Acknowledgements

This study has received funding from the Cybersecurity in Everyday Work in the Social and Healthcare Sector (KyberSoTe) project funded by the National Emergency Supply Agency. The views expressed are those of the authors only and do not necessarily reflect those of the funder. The granting authority cannot 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

Alasuutari, P. (1996). Theorizing in qualitative research: A cultural studies perspective. *Qualitative Inquiry*, *2*(4), 371–384.

Alasuutari, P. (2003). The globalization of qualitative research. In C. Seale, D. Silverman, J. F. Gubrium, & G. Gobo (Eds.), *Qualitative research practice* (pp. 595–608). SAGE Publications Ltd. https://www.torrossa.com/gs/resourceProxy?an=5018485&publisher=FZ7200#page=526

Aljuraid, R., & Justinia, T. (2022). Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review. *Studies in Health Technology and Informatics*, *295*, 362–365. https://doi.org/10.3233/SHTI220739

Al-Qarni, E. (2023). Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. *International Journal of Advanced Computer Science and Applications*, *14*(5), 135–140. https://doi.org/10.14569/IJACSA.2023.0140513

Barnett, M., Womack, J., Brito, C., Miller, K., Potter, L., & Palmer, X.-L. (2024). Botnets in Healthcare: Threats, Vulnerabilities, and Mitigation Strategies. *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, *23*(1), 58–65. https://doi.org/10.34190/eccws.23.1.2345

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

Cascella, L. M. (2022). *Strengthening the Frontline: Cybersecurity Training for Healthcare Workers | MedPro Group* [Education]. Cybersecurity Training for Healthcare Workers. https://www.medpro.com/cybersecurity-training-for-healthcare-workers

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

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. (2023a). *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

ENISA. (2023b, March). *Identifying emerging Cyber Security threats and challenges for 2030.* European Union Agency for Cybersecurity.

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

Osama, M., Ateya, A. A., Sayed, M. S., Hammad, M., Pławiak, P., Abd El-Latif, A. A., & Elsayed, R. A. (2023). Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions. *Sensors (Basel, Switzerland)*, *23*(17), 7435. https://doi.org/10.3390/s23177435

Patton, M. Q. (2002). *Qualitative Research & Evaluation Methods* (3rd ed.). Sage Publications.

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

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

Sunil, V., & Mathew, S. P. (2024). A Systematic Review on Cybersecurity Threats and Challenges in Hospitals. *Acta Medica International*, *11*(1), 1. https://doi.org/10.4103/amit.amit_7_24

The National Emergency Supply Agency. (2023). *Cybersecurity in Everyday Life*.

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