Pius Ewoh

Cybersecurity of Healthcare

Socio-technical Analysis and Solutions

ACTA WASAENSIA 576

University of Vaasa
VAASAN YLIOPISTO

ISBN 978-952-395-241-6 (print)
978-952-395-242-3 (online)

ISSN 0355-2667 (Acta Wasaensia 576, print)
2323-9123 (Acta Wasaensia 576, online)

URN https://urn.fi/URN:ISBN:978-952-395-242-3

PunaMusta Oy, Joensuu, 2025.

ACADEMIC DISSERTATION

To be presented, with the permission of the Board of the School of Technology and Innovations of the University of Vaasa, for public examination on the 15th of December, 2025, at noon.

Article based dissertation, School of Technology and Innovations, Subject

Author	Pius Ewoh https://orcid.org/0000-0002-4006-619X
Supervisors	Professor Tero Vartiainen University of Vaasa. School of Technology and Innovations, Information Systems Science.
	Associate Professor Timo Mantere University of Vaasa, School of Technology and Innovations, Automation Technology.
Custos	Professor Tero Vartiainen University of Vaasa. School of Technology and Innovations, Information Systems Science.
Reviewers	Associate Professor Ella Kolkowska Orebro University. School of Business, Informatics.
	Adjunct Professor Jyri Rajamäki Laurea University of Applied Sciences. Department of Information Technology.
Opponent	Professor Reima Suomi University of Turku. Turku School of Economics, Information Systems Science.

Tiivistelmä

Sosiaali- ja terveydenhuollon järjestelmien nopea digitaalinen murros sekä sähköisten potilastietojärjestelmien (EHR) laajamittainen käyttöönotto ovat merkittävästi parantaneet palvelujen tuottamista ja tiedonhallintaa. Samalla nämä edistysaskeleet ovat kuitenkin lisänneet terveydenhuoltojärjestelmien haavoittuvuutta kyberhyökkäyksille, tietomurroille ja muille turvallisuusuhille.

Tämä väitöskirja tarkastelee terveydenhuollon kyberturvallisuuden haavoittuvuuksiin johtavia keskeisiä tekijöitä sosioteknisestä näkökulmasta, korostaen teknologian, ihmisten ja organisatoristen prosessien välistä vuorovaikutusta. Tutkimus perustuu systemaattisten ja kartoittavien kirjallisuuskatsausten sekä käsitteellisten ja empiiristen analyysien synteesiin. Se tunnistaa keskeiset riskitekijät, kuten inhimilliset virheet, vanhentuneen infrastruktuurin, monimutkaiset digitaaliset verkostot, riittämättömän koulutuksen, sääntelyn noudattamatta jättämisen ja uhkien havaitsemisen viiveet.

Väitöskirjassa esitellään ja sovelletaan sosioteknistä kyberturvallisuuden viitekehystä sekä yksityisyyden ja turvallisuuden tarkistuslistamallia, jotka on suunniteltu erityisesti EHR-ympäristöihin. Nämä mallit tarjoavat strategista ohjausta terveydenhuollon kyberturvallisuuden vahvistamiseen ennakoivan uhkien hallinnan, sääntelyn noudattamisen, informoidun suostumuksen käytäntöjen, henkilöstön koulutuksen ja automatisoitujen uhkien havaitsemisjärjestelmien integroinnin kautta.

Väitöskirja korostaa sosioteknisen vuorovaikutuksen merkitystä ja puoltaa siirtymistä reaktiivisista turvallisuusstrategioista kohti ennakoivaa, integroitua ja ihmiskeskeistä lähestymistapaa terveydenhuollon kyberturvallisuudessa.

Asiasanat: kyberturvallisuus terveydenhuollossa, sähköiset potilastiedot, tietosuoja ja tietoturva, terveydenhuollon tiedonvaihto, sosiotekniset järjestelmät

Abstract

The rapid digital transformation of health care systems and the widespread adoption of Electronic Health Records (EHRs) have significantly improved service delivery and information management. At the same time, these advancements have increased the vulnerability of health care systems to cyberattacks, data breaches and other security threats.

This dissertation examines the key factors that contribute to cybersecurity vulnerabilities in health care from a sociotechnical perspective, emphasising the interaction between technology, humans and processes. Drawing on a synthesis of systematic and scoping reviews as well as conceptual and empirical analyses, the thesis identifies critical risk factors, including human error, outdated infrastructure, complex digital networks, insufficient training, non-compliance with regulatory requirements and delays in threat detection.

The dissertation introduces and applies a sociotechnical cybersecurity framework and a privacy–security checklist model specifically designed for EHR environments. These models offer strategic guidance for strengthening cybersecurity in health care through proactive incident management, regulatory compliance, informed consent practices, staff training and the integration of automated threat detection systems.

The dissertation highlights the importance of sociotechnical interaction and advocates a shift from reactive security measures to a proactive, integrated and human-centred cybersecurity approach in health care.

Keywords: cybersecurity in healthcare; electronic health records; data privacy and security; health information exchange; sociotechnical systems.

ACKNOWLEDGEMENT

I sincerely want to thank the almighty God for His mercies and blessings in my life because my strength cometh from Him. My doctoral studies journey has been inspiring and turbulent, but with a possibility mindset and leaning on the shoulders of my benefactors, I knew there was a light at the end of the tunnel.

First and foremost, I would like to express my utmost gratitude to my supervisors, Prof. Tero Vartiainen, for your invaluable academic supervision, guidance, funding, and unwavering support throughout this academic journey. These immense contributions have really improved my academic prowess in doing research and have been instrumental to the completion of this great dissertation work and achievement in this research direction.

I also want to express my heartfelt gratitude to my second supervisor, Associate Professor Timo Mantere, for your constant support in academic matters, funding recommendations, and the invaluable insight you have shared with me in this doctoral study. Your contribution and advisory role have been a great learning curve for me in this journey, and I do appreciate it. Also, I want to thank Dr Beatrice Obule-Abila for your support during my article reviews.

I want to sincerely thank the Dean School of Technology and Innovations, Dr. Raine Hermans, for your funding support, encouragement, and leadership quality for ensuring a conducive environment for learning and doing research. I am also grateful to Tomi Pasanen, the deputy Dean, for the good work supervision, advisory role, and for providing an enabling environment for work. Many thanks to the administrators Juuli Honko, Susanna Laurila, and Anna-Riikka Ringvall for their guidance, and to the entire faculty and staff.

I want to acknowledge the University of Vaasa for this enabling environment, community for learning, innovations, funding, and advancing scientific and arts research for a better world. The world-class facility for learning, experience, teachers, professors, and other administrative staff put together to deliver quality education and research has helped me to shape my academic prowess. I am proud to be part of this community.

I extend my sincere appreciation to the members of the thesis committee for your time and critical review, and constructive feedback that have helped in shaping the quality of this dissertation.

I would like to extend a big thank you to Prof. Heidi Kuusniemi, Prof. Amit Shukla, Prof. Duong Dang, Prof. Mike Mekkanen, Prof. Rebekka Rousi, Dr. Ulla Laakkonen, Ms. Heidi Järviniemi, Dr. Teemu Mäenpää, Dr. Tero Haukilehto and Zhu Zhe for your support and encouragement.

To my family, I want to sincerely thank my parents, Pharm. Reuben Ewoh, Hannah Ewoh, and Samantha Ewoh, for your encouragement and support. Also, I appreciate you, Ethel Ewoh-Odoyi, Engr. Emmanuel Odoyi, Love Ewoh, Ogelenye Patience Ewoh-Igbo, and other friends and family for your support.

I would also like to thank the Finnish Cultural Foundation for supporting my doctoral research thesis with funding, and I extend my gratitude to the Suomen Vakuutusyhdistys for their support of my conference travel.

Finally, I dedicate this work to my family, friends, and colleagues, who have been part of this journey, either directly or indirectly. Completing this Doctoral study would not have been possible without your immense support.

Contents

Figures

Tables

Abbreviations

AI	Artificial Intelligence
APT	Advanced Persistent Threats
CKMIR	Cybersecurity Knowledge Management and Intelligence Response Model
DICOM	Digital Imaging and Communications in Medicine
DOS	Denial of Service

EHR	Electronic Health Record
EMR	Electronic Medical Record
GDPR	General Data Protection Regulations
GUH	Geneva University Hospital
HHS	Health and Human Services
HIMSS	Health care Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HIS	Health Information Systems
HITECH	Health Information Technology for Economic and Clinical Health Act
IEC	International Electrotechnical Commission
IOMT	Internet of Medical Things
IoT	Internet of Things
ISO	International Standard Organization
NHS	National Health Scheme
NIST- CSF	National Institute of Standards and Technology Cybersecurity Framework
NIST	National Institute of Standards and Technology
OCR	Office of Civil Rights
PACS	Picture Archiving and Communication Systems
PHI	Patient Health Information
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-analyses
RBAC	Role-based Access Control
SCR	Scoping Review
SLR	Systematic Literature Review
STAMP	Systems Theoretic Accident Model and Processes
STPA-SEC	System-Theoretic Process Analysis for Security
STS	Socio-Technical Systems
TOE	Technology, Organization, and Environment Framework

Publications

This dissertation incorporates the following four research articles

[1] Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for health care systems. Systematic review. *Journal of Medical Internet Research, 26*, https://doi.org/10.2196/46904. CC BY.

[2] Ewoh P, Vartiainen T, Mantere T. Sociotechnical Cybersecurity Framework for Securing Health care from Vulnerabilities and Cyberattacks: Scoping Review. *Journal of Medical Internet Research, 27*, https://doi.org/10.2196/75584. CC BY.

[3] Ewoh, P. (2025). Cybersecurity in health care: a checklist for security and privacy [Manuscripts submitted under review) [Manuscript submitted for Journal publication].

[4] Ewoh, P., Vartiainen, T, Haukilehto T. (2025). Sociotechnical Cybersecurity Response Framework for Managing Cyber Incidents in Health care [Manuscript submitted for Journal publication].

1 INTRODUCTION

1.1 Background of the study and research gaps

Cybersecurity in health care is critical and of great importance in this era of digitalization, where the health care system is increasingly interconnected with medical device technologies and applications integrated with other care systems to advance health care delivery and services, leading to better precision, diagnosis, and outcomes. While the digitalization of health care has brought about significant advancements, it has also introduced substantial cybersecurity vulnerabilities and challenges in health care delivery systems (Argaw et al., 2019; Coventry & Branley, 2018). Despite the challenges, significant progress has been made in employing cybersecurity strategies and solutions to protect critical health care infrastructure (C. J. Dameff et al., 2019) and enhancing secure health outcomes across various developed countries such as Finland, the United Kingdom, Israel, and the United States of America. The intersection of cybersecurity in health care systems helps safeguard electronic information and assets against unauthorized access, use, and disclosure (Health Information and Management Systems Society (HIMSS, 2019). The "CIA trinity" describes the three aims of cybersecurity: confidentiality ensures that health information is accessible exclusively to authorized users, integrity guarantees that the information remains accurate and unaltered without permission, and availability ensures that sensitive health information and systems are accessible whenever required by authorized users (Giansanti, 2021).

The question remains: as individuals, governments, organizations, or stakeholders in the health care sector, have we ensured that health care systems are better protected against cyberattacks, threats, and breaches? The answer to this question could be yes, with a statement that we are completely secure, but with a caveat that we may underreport threats to maintain public confidence and avoid loss of trust, as well as to protect our public image, prevent loss of profits, and hypothetically comply with regulatory requirements to stay in the business of care. Alternatively, a firm believes that there is a need for a better conceptualization of cybersecurity in health care service delivery.

Health and Human Services (HHS) reported that at least two healthcare data leaks occur daily (Hippa J., 2023; Hippa Journal, 2022). It can be said that health care organizations are facing increasing challenges and crises, which include data breaches of personal health information (PHI) and vulnerabilities in their critical infrastructure (Offner et al., 2020). The office of the civil right (OCR) reported

between 2012 and 2022 that over 128,244,290 million US dollars has been paid as a result of health information breaches, fined on health care organization for unable to protect health information to surface in the public domain (HIPAA Journal, 2025), which violates HHS and the European General Data Protection Regulations (GDPR) compliance standard. In 2015, an estimated 113.27 million patient health records were stolen and exposed in the United States of America, resulting from hacking, computer-related attacks, email phishing, and other forms of social engineering attacks (Hippa Journal, 2022). However, 185 countries worldwide have not been factored into this breach report or cybersecurity-related challenges. Cybersecurity in health care can now be considered a global pandemic, given these factors and many others. Research has also highlighted the neglect of cybersecurity infrastructure, including the continued use of legacy systems, ineffective training, and insufficient investment in health care systems (Karambelas, 2020). Health care systems management seeks to enhance connected care operations and diagnostic service outcomes. However, when security is not integrated into the planning and design of technology, human processes, and organizational workflows, it creates vulnerabilities that expose health care systems to an increasing number of cybersecurity threats, breaches, and attacks (Casola et al., 2018; Coventry & Branley, 2018; Kioskli et al., 2021; Lechner, 2018; Rajamäki & Pirinen, 2017). Preventing health information breaches and cyberattacks requires understanding the multidimensional complexities of health care systems and identifying human, technology, and process vulnerabilities that pose cybersecurity risks.

The NIST cybersecurity framework (NIST-CSF) recognizes that these vulnerabilities may stem from human, technology, and organizational processes (Kaberuka & Johnson, 2023). Advancements in technology, changes in human behavior towards health care systems, and organizational process factors have led to vulnerabilities that are exploited by cybercriminals or state-sponsored attackers, enabling them to gain access to and control of critical health care infrastructure or sensitive data, thereby disrupting health care services. This can be regarded as a sociotechnical challenge within a complex health care system (Haukilehto, 2024; Kaberuka & Johnson, 2023; Sittig & Singh, 2016).

Emery and Trist (1960) defined sociotechnical systems (STS) as comprising two interrelated subsystems: the social and the technical. STS can be defined as the integration of new technology (referred to as technical systems) into the workplace, with equal emphasis on social systems, including organizational structure, processes, and personnel (Davis et al., 2014; Woodward, 1965). Mumford (2000) and Trist & Baumforth 1951) stated that the optimization of social and technical systems is crucial for health care organizations to enhance the efficacy of digital health transformation. Cybersecurity in health care is a sociotechnical system that

recognizes that vulnerabilities are not purely technical, but arise from the complex interplay between people, technology, and organizational processes. (Lehto et al. 2022). McEvoy and Kowalski (2019) view cybersecurity in health care through the lens of sociotechnical systems theory, arguing that protecting critical infrastructure, such as health care, is not just about implementing the right technology but also about how people interact with systems, how processes govern their behaviour, and how technology supports these interactions. By mapping health care system vulnerabilities to cyberattacks, a protection approach to technology, humans, and processes can create a comprehensive defense framework that proactively addresses the challenges they pose (Ewoh & Vartiainen, 2024; Zimmermann & Renaud, 2019).

Cybersecurity in health care presents a significant challenge for health care organizations, particularly with the advent of the Internet of Medical Things (IoMT), in which technology-enabled diagnoses and services, such as telehealth, are delivered remotely from home via a computer. However, the complexity and heterogeneity of the internet, health information, or patient data can easily be compromised through hacking. Despite these challenges, the digitalization of health care and the integration of technology have offered substantial benefits. Health information or patient data can be accessed remotely by physicians or patients using a unique identification number or tag name across multiple data points, thereby facilitating seamless health care service delivery through IoMT. However, this advancement complicates the protective landscape of health care organizations. Solutions have been proposed to protect the health care sector from cyberattacks and other threats. However, health care is among the sectors that lag in protection, which positions them as the most affected sector with cyber threats and breaches due to a lack of investment budget for health care cybersecurity, which exacerbates the frequency of breaches in the sector (Dias et al., 2021; Fernando & Dawson, 2014; Filipec & Plášilb, 2021; He et al., 2021). As digital transformation continues to accelerate the delivery of health care services, the importance of robust cybersecurity to combat emerging threats and build a resilient health care system cannot be overstated.

Existing literature on cybersecurity in health care has provided solutions with a focus on cybersecurity threats and trends, (Argaw et al., 2019; Coventry & Branley, 2018; Kruse et al., 2017; Luna et al., 2016; Offner et al., 2020) policies, awareness, and incident reporting (Haukilehto, 2024). Other authors have focused on the vulnerability of health care systems and areas of future improvement to tackle health information breaches and attacks (Jalali, Razak, et al., 2019; Jalali, Siegel, et al., 2019; Jalali & Kaiser, 2018; Mohammed, 2022). Some research has focused on the intersection of cybersecurity and health care to improve security posture (Jalali & Kaiser, 2018; Zarour et al., 2021). However, to the best of my knowledge, there have been very few studies that have approached cybersecurity on why health care

systems are vulnerable to cyberattacks from a sociotechnical lens, even when some studies acknowledge that cybersecurity in health care is a complex sociotechnical problem (Kaberuka & Johnson, 2023; McEvoy & Kowalski, 2019; Offner et al., 2020). Tackling the cybersecurity of health care systems in response to cyber threats and attacks, solutions must be factored into the three core constructs of the sociotechnical systems theory: technology, humans, and processes, to be integrated as a holistic solution for solving health care system vulnerability and responding to cyber threats and attacks as a further area of call for empirical and review research (Coventry & Branley, 2018; Malatji et al., 2020). Based on the call and limited studies in the health care aspect, this dissertation seeks to address this significant gap by researching the cybersecurity of health care systems and why they are vulnerable to cyberattacks from a sociotechnical perspective, factoring in humans, technology, and processes.

To complete this dissertation, a qualitative study including systematic, scoping, integrative reviews, and a qualitative survey was conducted. A sociotechnical cybersecurity framework and solutions were developed for health care organizations. The main contribution of this dissertation is the development of a conceptual framework for preventing and responding to cyberattacks and threats in health care systems.

1.2 Problem statement

Globally, health care organizations are facing a rising number of cyberattacks, threats, and breaches (Budzak, 2016; Federal Bureau of Investigation, 2023; Gourisetti et al., 2020; Malatji et al., 2020; Zimmermann & Renaud, 2019). The conceptualization of cybersecurity in health care is a critical issue that requires fundamental organizational changes within health care to protect sensitive patient data, ensure the integrity of health care systems, and safeguard cyber-critical infrastructure from cyberattacks and threats. Cybersecurity in health care will continue to become more complex due to the heterogeneity and connectivity of health care systems. Thus, cybersecurity is more important than ever in this era of digitalization (Haukilehto, 2024). Despite the availability of technological and social solutions intended to address the vulnerabilities of health care systems to cyberattacks and other threats, these systems continue to lag. Consequently, applying a sociotechnical approach to address these challenges is essential, requiring the integration of technology, humans, and processes. Furthermore, there is a lack of robust cybersecurity measures in the health care sector, limiting its resilience in the event of cyberattacks and threats. (Svandova & Smutny, 2024).

1.3 Research objectives

The objective of the dissertation is to investigate the vulnerabilities of health care systems to cyberattacks and threats from a sociotechnical perspective.

To achieve the objective, the first article Explored from a sociotechnical approach why digital health care systems are vulnerable to cyberattacks, provide sociotechnical solutions, and identify the areas of health care systems that need further improvement. This approach enables a detailed examination by providing a sociotechnical cybersecurity solution for health care organizations, facilitating the management of cyber threats and attacks.

The second article examined the dynamics of the factors of vulnerabilities to cyberattacks from a sociotechnical perspective and developed a conceptual sociotechnical cybersecurity framework to prevent vulnerabilities and respond to cyberattacks and threats in health care systems.

The third article identified security and privacy concerns within electronic health records systems. And developed a security and privacy checklist model for healthcare organizations to ensure the proper protection of patient records.

Finally, the fourth article examined the management of cyberattack incidents within Finnish health care organizations by analyzing the sociotechnical factors that influence effective incident response and management. This article adopted the Technological, Organizational, and Environmental (TOE) framework and the sociotechnical lens to analyse and develop a conceptual sociotechnical cybersecurity incident response framework to manage pre- and post-incident cyberattacks in Finnish hospitals.

1.4 Research question

To address the complex sociotechnical problem of vulnerabilities to cyberattacks in health care systems and to achieve the research objective, the following research questions were posed to provide answers.

RQ1: Why are health care systems vulnerable to cyberattacks? How can health care systems be protected?

RQ2: What are the sociotechnical factors of vulnerabilities to cyberattacks that affect health care systems? What kind of framework is best suited for preventing vulnerabilities and responding to cyberattacks and threats?

RQ3: What operational practices in health care data exchange contribute to the breach of security and privacy in EHRs? How can we ensure proper data security and privacy?

RQ4: How can we manage cyberattack incidents in health care organization?

Table 1 below outlines the dissertation's framework, including its areas of focus and research questions.

Table 1. Dissertation areas of focus and research questions

Article 1: Area of focus and RQ 1	Article 2 area of focus and RQ 2	Article 3 area of focus and RQ 3	Article 4: Area of focus and RQ 4
Health care systems' vulnerabilities to cyberattacks and threats	sociotechnical factors and dynamics of vulnerabilities to cyberattacks and threats	EHRs' data security and privacy breaches	Cyberattack incidents management
RQ 1: Why are health care systems vulnerable to cyberattacks? how can health care systems be protected?	RQ 2: What are the sociotechnical factors of vulnerabilities to cyberattacks that affect health care systems? What kind of framework is best suited for preventing vulnerabilities and responding to cyberattacks and threats?	RQ 3: What operational practices in healthcare data exchange contribute to the breach of security and privacy in EHRs? how can we ensure proper data security and privacy?	RQs 4: How can we manage cyberattack incidents in hospitals?

The cybersecurity of health care is important in this era of digitalization, as innovative technologies are being integrated into health care. As a result, there is a high level of complexities with these endpoints and medical technology, which expand the landscape of protection, making it difficult to cover due to the IoTs (Cartwright, 2023).

1.5 Research approach

The research approach adopted in this dissertation is a qualitative method, which takes the instance of the philosophical onion method (Saunders et al., 2009) on how

researchers view the world through the lens of research. In this dissertation, the philosophical worldview of this research was developed based on interpretivism and abductive (deductive-inductive) approach to seek an in-depth interpretation and understanding of the subject. This focuses primarily on people's insights, ideas, and experiences to provide a comprehensive view and understanding of the research subjects.

The approach for this research focuses on abductive reasoning, which primarily involves a combination of deductive and inductive reasoning, as researchers move back and forth between theory analysis and new themes or unexpected patterns emerging from the data. However, the dissertation aims to formulate a new theory using the qualitative grounded theory approach, grounded in new themes emerging from the literature and in qualitative themes and patterns. Based on Interpretivism and the abductive research approach, the dissertation will not focus on testing the framework or model generated from this research.

Furthermore, it follows a mono-method qualitative approach, based on a multi-strategy qualitative approach comprising narrative inquiry, archival research, and grounded theory to gain an in-depth understanding of a real-life experience on the subject. While the time horizon adopted is cross-sectional, the data were collected within a specific timeframe in this study. The primary data in Article 4 were collected through an online questionnaire administered to IT professionals and health care managers, which included open-ended questions.

Furthermore, the dissertation research utilizes significant secondary data from online databases and industrial white papers, as well as reports from the intersection of health care and cybersecurity. The data were analyzed using qualitative thematic analysis and literature synthesis (systematic and scoping), Expert Opinion, and an online questionnaire.

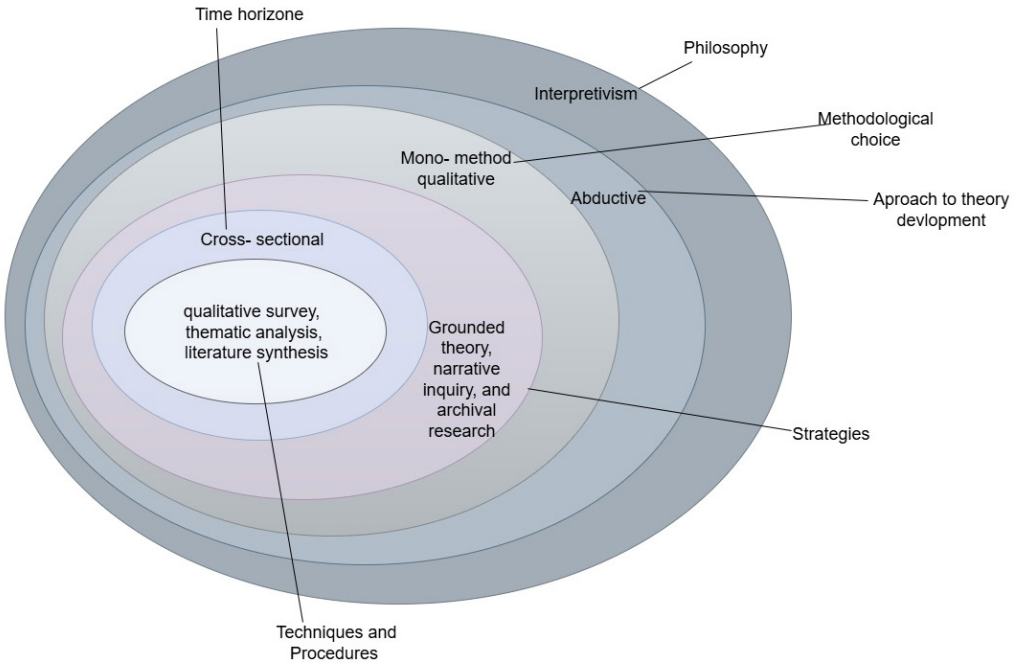


Figure 1. Dissertation's research onion

1.6 Dissertation structure

This dissertation comprises two main sections. The first sections are structured as follows: introductions, literature review, methods, article summaries, discussion, and conclusions. This section aims to provide the research context, explain the key foundational themes and ideas behind this dissertation, and place the articles in an orderly format. See figure 2 for details.

The second part of the section comprises four articles. In this section, article 1 was co-authored by Ewoh and Vartiainen. Ewoh, Vartiainen, and Mantere co-authored article 2. While Ewoh authored Article 3, Ewoh, Vartiainen, and Haukilehto co-authored Article 4. Ewoh was the primary author of the four articles, responsible for creating, writing, structuring, gathering, and analysing the data, and organising the review process. Vartiainen also contributed to the close structuring of articles, reviewing, and providing advisory guidance for articles 1, 2, and 4, while Mantere contributed to providing advisory guidance in article 2. Haukilehto contributed to refining the questionnaire and the data collection process.

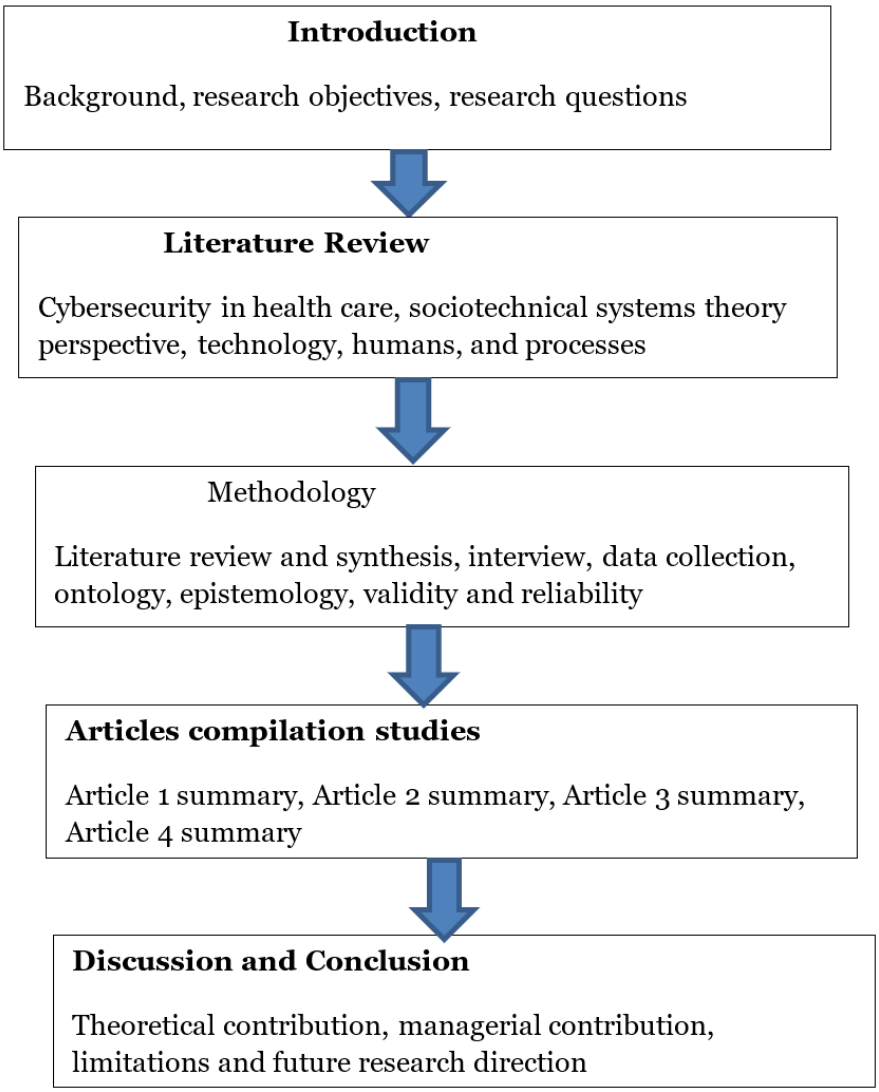


Figure 2. Dissertation structure

Table 2. Overview of the articles

Research objectives	Literature/ theory	Article ordering number	Title	Research designs	Tools	Data source	Unit of analysis
Explored from a sociotechnical approach why digital health care systems are vulnerable to cyberattacks, provide sociotechnical solutions, and identify the areas of health care systems that need further improvement.	STS Lens	One	Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review	Qualitative (systematic review)	Literature review and synthesis	Literature review (secondary)	Global
Examined the dynamics of the factors of vulnerabilities to cyberattacks from a sociotechnical perspective and developed a conceptual sociotechnical cybersecurity framework to prevent vulnerabilities and respond to cyberattacks and threats in health care systems.	STS Lens	Two	Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: scoping review	Qualitative (scoping review)	Literature review and synthesis	Literature review (secondary)	Global
Identified security and privacy concerns within electronic health records systems.	TOE Framework lens	Three	Cybersecurity in health care: a checklist for security and privacy	Qualitative Integrative Review	Literature review	Literature review (secondary)	Global
Examined the management of cyberattack incidents within Finnish healthcare organizations by analyzing the sociotechnical factors that influence effective incident response and management.	STS Lens	Four	Sociotechnical cybersecurity response framework for managing cyber incidents in healthcare	Qualitative survey	Literature and Manual, and memo, sticky note data analysis	Qualitative survey, online Questionnaire, (Primary data)	National

2 LITERATURE REVIEW AND THEORETICAL BACKGROUND

2.1 Cybersecurity in health care

Cybersecurity in health care, or health care cybersecurity can be defined as a system of health care safeguards, designed to protect, prevent, respond, and recover from attacks and threats to achieve relative security for all the users interacting within the health care systems (Athinaiou, 2022).

Cybersecurity is a crucial component of health care information technology infrastructure. However, the rapid advancement and technology digitization in health care service delivery from paper-based records to electronic health records, telemedicine, and mobile health, integrated with the networked connected endpoint and medical devices, introduces cyber-related risk of vulnerability to cyberattacks in health care systems (Haukilehto, 2024; Jalali, Razak, et al., 2019). The technology integrations and transitions left many healthcare organizations susceptible to health information breaches and cybercrime issues, such as identity theft, insurance fraud, and cyber espionage (Luna et al., 2016). (Pranggono & Arabo, 2021) highlighted that cybersecurity should be viewed from the process perspective with a comprehensive integration of the social and technical dimensions of the health care organization. The United State Health and human services defined cybersecurity as a process in healthcare organisations that required the mobilisation or convergences of technical and social mechanisms which includes IT vendors and systems, medical devices and developers, experts such as humans from organizations, community and regulatory body such as government, collaborating to mitigate cyberattacks risks and minimized the impacts of vulnerabilities or occurrence, which alludes to the instances of (Dawson, 2018; Nobles, 2018; Zoto et al., 2019).

According to NIST, a vulnerability can be defined as a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (Kissel, 2013; NIST, 2013).

2.2 Emerging cyber threats and vulnerabilities in health care systems

Modern health care technology integration is essential in this digital era for enhanced precision and accurate diagnosis. Health care systems become vulnerable to

cyberattacks due to the interconnectedness of health care and the complex, diverse nature of the Internet of Things, which widens the protection landscape by making them more susceptible to cyber threats and attacks.

Some of the key reasons for the increasing breaches and vulnerabilities of health care systems to cyberattacks are a result of a lack of investment in cybersecurity, critical infrastructure (Argaw et al., 2019; Cartwright, 2023), insider threats (Arafa et al., 2023); outdated systems (Zarour et al., 2021) human error, and (Nifakos et al., 2021). Studies show that health care is the most affected among all industries in breaches that occur (Seh et al., 2020; Verizon Enterprise, 2018). For example, at least one or two health care organizations experience cyber breaches daily globally (Hippa Journal, 2022). One of the emerging types of cyberattacks in health care systems is the ransomware attacks, which are a complex sociotechnical problem (Sittig & Singh, 2016). A survey conducted by HIMSS information security professionals in 2018 revealed that about 75% of health care organizations experienced a security incident (Health care Information and Management Systems Society, 2018). Furthermore, the report acknowledged that the causes of the cyber incident involve technology, people, human-related error, and cultural factors, which play an increasingly critical role in health care cybersecurity (Jalali, Razak, et al., 2019). Also, the study conducted by (Offner et al., 2020) It was described as a complex sociotechnical problem involving cyberattacks in health care systems. See Table 3 for the types of cyberattack incidents in health care organizations, and Table 4 for various studies conducted to address vulnerabilities and challenges related to cyberattacks in health care.

Table 3. Cyberattacks in health care organizations

Health care Organization	Cyberattack Type	Year	Target	Description	References
National Health Service (NHS). Hospitals in the United Kingdom and the Globe	WannaCry	2017	Cyber physical systems of health care organization and individual computers	A malware attack against hospitals in 2017 was launched via a phishing email link that was clicked, spreading across 155 countries.	(Coventry & Branley, 2018; He et al., 2021; Slayton, 2021)
Hollywood Presbyterian Medical Centre	Malware: Phishing email	2017	Cyber-physical systems of the hospital	The Hollywood Medical Centre was hit by a malware infection originating from a phishing email. The attackers encrypted all files.	(Chinthapalli, 2017; Choudhary & Jagre, 2024; C. Dameff et al., 2023; Winton R., 2016)
Vastaamo OY Mental Health Psychotherapy Centre, Finland	Hacking of the database management system	2020	Cyber virtual system database of the mental health hospital	Hacking of the database for Vastaamo mental health centre and exposure of protected health information. The attacker demanded a ransom of 40 bitcoins, equivalent to approximately 450,000 euros.	(Ghanbari & Koskinen, 2024; Lehto et al., 2022; Looi et al., 2024, 2025)
Oloran-Sainte-Marie Hospital France	Ransomware	2021	Cyber-physical systems of the hospital	A ransomware cyber-attack hit the hospital. The hospital's health information systems were paralyzed to the point that internal and external applications were not functioning.	(Chiaradonna et al., 2023; Djenna et al., 2021)

Table 4. Key studies on cybersecurity in health care

Authors	Methods	Domain	Study Contributions
(Coventry & Branley, 2018)	Narrative review	Health care	The study provides an understanding of why health care is vulnerable to cyberattacks and a way forward to protect health care.
(Kandasamy et al., 2022)	Qualitative	Health care	The study focuses on the examination of vulnerabilities and risk management in Asian health care systems from NIST's maturity perspectives.
(Javaid et al., 2023)	Literature review	Health care	The authors contribute by highlighting the tools, traits, and roles of cybersecurity through explorations of potential applications to secure health care
(Cartwright, 2023)	Literature review	Health care	The study highlights cybersecurity threats, vulnerabilities, and the risks associated with the adoption of IoMT devices in health care and recommends increased funding.
(Kruse et al., 2017)	Systematic Literature Review	Health care	The authors emphasize that health care is vulnerable to modern technological trends due to a lack of investment in cybersecurity technology, human resources, and procedures, and therefore requires a step-up in security standards.
(Jalali, Razak, et al., 2019)	Literature review/ Bibliometric	Health care	The study provides an overview of the literature at the intersection of cybersecurity and health care, conducted through a bibliometric analysis, to understand the various aspects of health care cybersecurity and inform future research.
(Offner et al., 2020)	Literature review	Health care	The authors examine health care cybersecurity breaches worldwide, with a focus on protecting Australians' health records, and propose a proactive maturity culture to enhance resilience against attacks.

Authors	Methods	Domain	Study Contributions
(He et al., 2021)	Literature scoping review	Health care	The study contributes by identifying cybersecurity challenges, areas for improvement, and solutions adopted to prevent a rise in cyberattacks amid COVID-19.
(Garcia-Perez et al., 2023)	Quantitative survey	Health care digital transformation and digital resilience.	The paper provides an understanding from cybersecurity perspectives and resilience as a phenomenon that will enable the digital transformation of health care systems to meet society's changing, increasingly demanding needs.
(K. A. Ali & Alyounis, 2021)	Literature review	Health care	The authors provide insight into the need to enhance health care security, identify the most common and severe cybersecurity threats, and offer recommendations to mitigate vulnerabilities in critical infrastructure.
(Loi et al., 2019)	Literature review	Health care ETHICS	The study provides an overview of the core values associated with the four principles of biomedical ethics, examining their support or conflict regarding cybersecurity in health care.
(Kioskli et al., 2021)	Conceptual review	Health care	The paper explores the vulnerabilities in the health care critical information infrastructures that are used in cyberattacks and proposes a living lab as a measure to mitigate cyberattacks.
(Haukilehto, 2024)	Mix method (Dissertation thesis)	Health care	The dissertation works enhanced understanding of cybersecurity in health care by introducing the PAR model and providing new insights into cybersecurity management, including policies, user awareness, and incident reporting and handling.

2.3 Definitions of terms and their interrelationship

The International Telecommunication Union (ITU) defines cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies used to protect the cyber environment, organizations, and users' assets. The health care organisation and users' assets comprise connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and or stored information in the health care cyber environment. (ITU, 2008; Von Solms & Van Niekerk, 2013)

Information security can be defined as the preservation of the confidentiality, integrity, and availability of information. ((ISO/IEC 27002, 2005, p. 1). In this context, health care information can take many forms, such as paper-based records or electronic health records, and can be transmitted by post, email, or other means. Whitman and Mattord (2009) view Information security as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information." This study also acknowledged that information security is not a product or technology but a process (Mitnick & Simon, 2003, p. 4), as illustrated by the process construct in the conceptualization of this thesis as a sociotechnical system, required for a comprehensive approach to tackling the vulnerability of health care systems.

Data security is the protection of data from accidental or malicious modification, destruction, or disclosure. It is strategy for protecting data in computer or medical devices and communication systems against unauthorized disclosure, transfer, delay, or alteration, whether accidental or intentional. (Aslan et al., 2023; Shukla et al. 2022).

Data privacy concerns the management of personal or patient-sensitive information stored in computers or information systems designed for personal communication. This domain includes considerations of dignity, medical data, and digital devices, enabling individuals to assert their right to privacy or to authorize others to utilize and process their personal information. In the context of health care, privacy concerns are centered on the collection, processing, sharing, and access of patient health information, situating it at the confluence of security and information governance. (Determann 2019).

The definitions of cybersecurity and information security are similar (Von Solms & Van Niekerk, 2013), However, some authors see cybersecurity as a subset of general information security. To summarise their interrelationships: information security provides the broadest conceptual framework; data security focuses on protecting

data assets; cybersecurity focuses on protecting networked digital systems and the data they contain; and privacy addresses the rights and expectations associated with personal or sensitive information. In the health care domain, for instance, protecting patient health information requires adequate data security controls implemented through cybersecurity measures, all situated within an information security governance framework, while simultaneously respecting privacy expectations (Åhlfeldt et al., 2005). There is a discourse that the boundaries of cybersecurity as a concept are wider than those of information security in terms of definitions, which is supported by an international standard (ISO/IEC 27032: 2012). For example, Von Solms and Van Niekerk (2013) argued that both humans in their personal capacity and society at large can be directly harmed or affected by cybersecurity attacks, whereas this is not necessarily the case with information security, where harm is always indirect.

The increasing breaches of health information and cyberattacks show that health care is lagging behind (Gordon, Wright, Glynn, et al., 2019; He et al., 2021). In comparison to other industries, security duties in the health care industry are particularly broad and new, with their high complexities and vast amount of data for big data processing (Javaid et al., 2023). There is a need to implement cybersecurity measures in health care to protect sensitive information.

2.4 Theoretical background

2.4.1 Sociotechnical systems theory and cybersecurity

The concept of sociotechnical systems theory was developed during World War II to treat construction workers and wounded soldiers in English coal mines at the Tavistock Institute in London. The concept emphasizes the interrelatedness of social (people, society) and technical aspects of an organization (structure, processes) or systems as a whole (F. Emery, 1982; Trist & Bamforth, 1951). The concept was established as a system of technology and people to ensure that the organization is effective and efficient (Mumford, 1983). Thus, the ideas of sociotechnical systems perspectives for health care systems, which include human-systems integration (Booher & Minninger, 2003; F. E. Emery & Trist, 1960; Kaberuka & Johnson, 2020) play crucial roles in influencing the cybersecurity environment inside healthcare organisations and propelling technological advancement on a larger scale (Zoto et al., 2019).

Sociotechnical design is identified as an approach to integrating systems while ensuring that the multifaceted challenges and complexities in smart health care are

well managed (Altman, 1997; Atkinson et al., 2001). This approach concerns three primary dimensions: the social environment, the technical environment, and the organizational environment (Palvia et al., 2001). The idea of classical sociotechnical systems theory emphasizes the combination of the social and technical dimensions, which are vulnerable to their operating environments (Appelbaum, 1997). In the same context, other scholars described the application of sociotechnical systems as involving a high level of social intricacy and technical complexity intended to fulfill an organization's important functions (Baxter & Sommerville, 2011).

Security of health care systems from cyberattacks and threats requires the avoidance of these security design reality gaps, which requires approaching the security functionality of a health information system as a sociotechnical system and not as a technical system (F. Emery, 1982; Heeks, 2006; Mumford, 2006; Taddeo et al., 2023). This notion, as embedded in this dissertation for developing health care system cybersecurity, will enhance successful health care management by protecting health information, patient safety, and other critical health care infrastructure from vulnerability to cyberattacks. This, in turn, will sustain health care digitalization efforts and reliance on new technology integration for managing overall healthcare service delivery in the event of cyberattacks.

Therefore, the review of the literature at the convergence of cybersecurity and health care is necessary, given the growing significance of cybersecurity for the delivery of safe, efficient, and sustainable health care (Al-Qarni, 2023; He et al., 2021; Vukotich, 2023).

2.4.2 Sociotechnical perspective of vulnerabilities to cyberattacks

This dissertation presents new perspectives, interpretations, and views on the conceptualization of cybersecurity in health care, considering vulnerability areas of occurrence and analyzing them through a sociotechnical lens. Furthermore, it goes beyond the traditional approach of protecting the privacy and security of health information from unauthorized users. Instead, it views that cybersecurity in health care is about protecting health care systems that require factoring the rudiments of the three areas of the sociotechnical systems theoretical dimensions for the vulnerability factors that affect health care systems in technology, humans, and processes as an approach for a holistic system security design for health care organizations (Alhammad et al., 2022; Heeks, 2006; Whitworth, 2011). This emphasises that to protect health care systems, security design should factor the social and technical side of cybersecurity in a joint optimization, which refers to the best approach to allow both the technical and human factors and organizational process environment aspects of security to interplay with equal emphasis (Malatji et

al., 2019; Mumford, 2006). There is a need to develop cybersecurity in health care, factoring in technology, Human behaviour, and processes in an integrated or holistic approach to address health care systems' vulnerability to cyberattacks (Coventry & Branley, 2018).

Social (S): dimension focuses mainly on human, cultural, behavioral, or organizational determinants (e.g., training, insider threats, ethics, governance) and has little technical analysis. An example signifier: work with the staff attitudes, training intervention, consent, legal, and ethical analyses.

Technical (T): dimension refers to technological components, system vulnerabilities, devices, and architectures, and cryptographic or network-level controls. Example indicators: formal security vulnerabilities (e.g., OS flaws), intrusion-detection algorithms, and encryption techniques.

Sociotechnical (ST) dimensions refer to the interplay between social and technical factors (humans, technology, and processes), offering solutions involving joint optimization or providing a framework for empirical results connecting human behavior to technical arrangements and organizational activities. Examples of indicators include the application of STS theory, cross-sectional studies examining the connection between system design options and user behavior, and the frameworks of policy, training, and technical control.

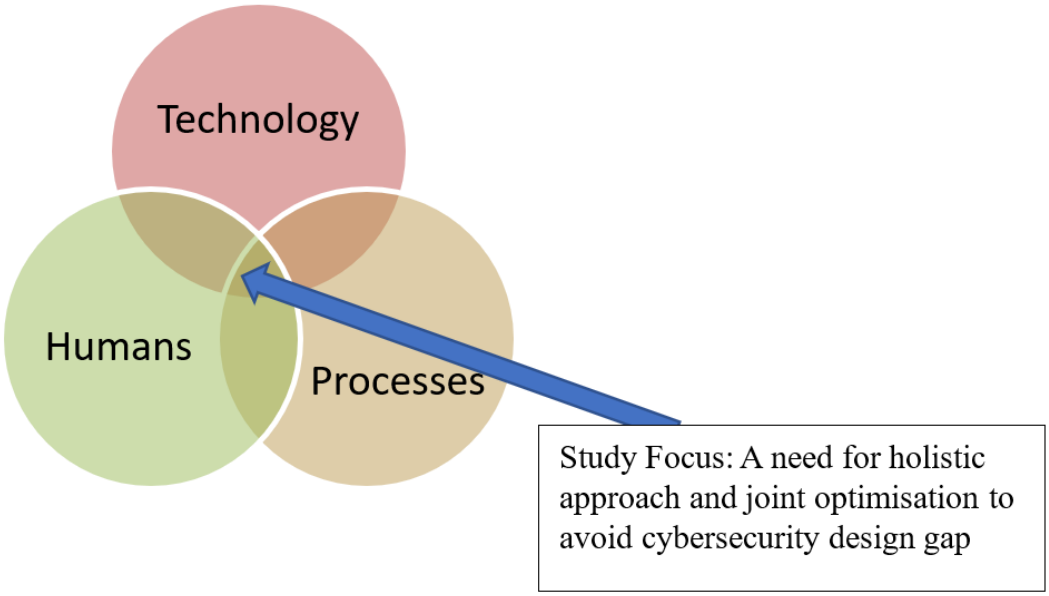


Figure 3. Sociotechnical interplay

Limited studies have been conducted on cybersecurity in the context of health care vulnerabilities from a sociotechnical perspective, and a sociotechnical framework is

necessary in health care systems (Ewoh & Vartiainen, 2024; Malatji et al., 2020). The cybersecurity vulnerabilities in health care systems are a complex sociotechnical problem, and as such, must be addressed using a sociotechnical approach (Anastasopoulou et al., 2020; Offner et al., 2020). Furthermore, this dissertation examines three-dimensional areas, including technology, humans, and processes, aligned with the study of sociotechnical systems (Zimmermann & Renaud, 2019), which is derived from sociotechnical theory. It highlights the need for this dissertation in the context of health care. Table 5 provides an overview of studies conducted from a sociotechnical perspective to address the vulnerabilities of health care systems to cyberattacks and their associated limitations.

Table 5. Research overview on the sociotechnical lens and cybersecurity vulnerabilities

Authors	Methods	Domain	Study contributions	Limitations
(Kaberuka & Johnson, 2020)	Qualitative interview	Health care	The study contributed to improving PACS cybersecurity by validating sociotechnical security challenges using the Systems Theoretic Accident Model and Processes (STAMP) with NIST integration at a Rwandan hospital.	The study also acknowledges that it serves as a starting point for the sociotechnical method, requiring analysts to be familiar with its application. Also, it focuses on developing nations.
(Kaberuka & Johnson, 2023)	Case study and Stamp techniques	Health care	The study highlighted that organizational and operational vulnerabilities, as well as governance structures, create systematic and sociotechnical risks and proposes STAMP techniques.	The study integrates NIST and STAMP as a starting point. However, there is a call for further research to develop a sociotechnical cybersecurity framework to address cybersecurity vulnerability challenges. It was a starting point.
(Malatji et al., 2020)	Mix method	Enterprise systems security	The study validates a sociotechnical management process and addresses sociotechnical security gaps in an enterprise systems security framework.	The study applied to any organization and also called for a sociotechnical framework for health care.
(Malatji et al., 2019)	Qualitative review	Enterprise systems	The study developed a conceptual process model for analyzing organizational information security practices in terms of social, technical, and environmental influences by addressing sociotechnical gaps.	The study was generic for any organization and requires validation of the sociotechnical concept.

Authors	Methods	Domain	Study contributions	Limitations
(Nicho & McDermott, 2019)	Mix Method	organisations	The study explored multiple dimensions of socio factors of vulnerabilities, namely (organizational management and environmental), that contribute to successful APT attacks in an organization to assist IT managers and personnel.	The study developed the social aspects of vulnerability factors to apply sociotechnical approaches. However, the approach was generic to any organisation and excluded the technical perspective. Health care was not among the organizations selected.
(Offner et al., 2020)	Literature review	Health care	The authors examine healthcare cybersecurity breaches and propose a proactive approach to establishing a culture of maturity.	The study did not focus on vulnerability from a sociotechnical lens. However, they acknowledge that the issues of cyberattacks and health care vulnerabilities constitute a complex sociotechnical problem.
(Ogunniye et al., 2024)		Educational Research Centre	The study provides an understanding of the interplay between social and technical aspects of IoT research and development, as well as sociotechnical requirements, to enable IoT research conceptualized for human-centered design and evaluation in a new research center.	The study focuses on the IoT devices research and development center and acknowledges integrating sociotechnical requirements for successful IoT research. Additionally, it primarily focuses on all IoT devices.
(Perrotin et al., 2022)	Case study and Machine learning	Maritime and health	The paper proposed using a behavioural model to describe the propagation of human vulnerabilities in sociotechnical systems and using systems-of-systems to capture the increasing attacks on STS.	The study focuses solely on the propagation of human factors between maritime and healthcare, and is not specific.

Authors	Methods	Domain	Study contributions	Limitations
(Taddeo et al., 2023)	Concept paper	Education	This study proposes a sociotechnical research agenda for examining the role of AI in cybersecurity.	The study acknowledges the benefits of AI to cybersecurity, providing a generic understanding for anyone. Also, they said it is emerging yet and called for the application of the sociotechnical method.
(Sittig & Singh, 2016)			The study provides an understanding of the sociotechnical approach to address ransomware attacks and provides steps to secure electronic health record systems and computing infrastructure.	The focus was mainly on ransomware attacks, although they call for the application of sociotechnical frameworks to prevent or mitigate such attacks.

2.5 Technology factors of vulnerabilities

Vulnerabilities in technology often stem from the **health care IT infrastructure**, such as legacy systems, medical devices, and outdated software. They are the key sources of technological factors of vulnerabilities. The health care sector frequently depends on older systems and applications, which can lead to security weaknesses (Cartwright, 2023). The primary issue with outdated technology is the absence of updates and security patches, making it vulnerable to cyberattacks. These attacks on health care systems are becoming increasingly worrisome due to the threats they pose to the security of patient electronic data and the overall integrity of health care operations (Williams & Woodward, 2015). While technology enhances precision and brings positive changes to health care delivery, outdated technologies or legacy systems create opportunities for cybercriminals to exploit health care systems. Additionally, technological weaknesses or vulnerabilities may arise from the integration of interconnected medical devices, cloud-based computing (such as data storage), mobile devices, and policies that permit the use of personal devices without proper configuration. Each of these factors plays a significant role in making health care systems vulnerable to cyberattacks, creating exploitable weaknesses if not adequately managed or implemented (Vukotich, 2023). The Analysis of these

components mentioned highlights how vulnerabilities are embedded in the current technological environment.

2.5.1 Integration of interconnected medical devices

The **integration of interconnected medical devices** for patient monitoring and diagnosis has expanded the potential attack surfaces due to their inherent complexities, thereby increasing the risk of cyber threats within health care systems (Clarke & Martin, 2023). Furthermore, technological vulnerabilities arise because many of these devices are designed with minimal security features, which makes them susceptible to exploitation (Mejía-Granda et al., 2024). Once a cyberattack is launched against a health care system, cybercriminals exploit network vulnerabilities to access sensitive patient data for financial gain or to disrupt critical health care infrastructure through denial-of-service or distributed denial-of-service attacks.

2.5.2 Cloud-based computing and data storage

The Emergence of **cloud-based computing and data storage solutions** has remarkably advanced big-data processing in the health care sector (Joshi & Kadhiwala, 2017). Cloud computing offers numerous benefits, including cost efficiency, enhanced data availability, and improved accessibility. However, this burgeoning technology also introduces vulnerabilities, particularly through the Internet of Things (IoT) or medical Internet of Things (MIoT) networks, thereby presenting new security risks to medical networks (Gupta et al., 2023; Harries & Yellowlees, 2013). If a cloud-based storage environment is improperly configured, it may expose patient information to unauthorized access on the network. Consequently, robust security measures should be implemented to safeguard the sensitive data stored in cloud networks or environments (S. J. Choi et al., 2023; Garcia-Perez et al., 2023; Thantilage et al., 2023).

2.5.3 Mobile devices and the adoption of policies for personal devices

The Introduction of **mobile devices and the adoption of policies allowing personal device** use in health care service delivery are another factor that increases the risk of health information breach when the policies do not support security coverage within and outside base stations (M. B. Ali et al., 2020). Mobile devices, unlike medical devices that are designed for long-term durability, typically have shorter product lifecycles (Arafa et al., 2023; Z. Wang et al., 2015). For instance, mobile device applications often incorporate third-party applications to provide

health care services (Arora et al., 2014). However, integrating third-party telemedicine applications into health care systems frequently fails to ensure user anonymity during cyberattacks (Loughlin et al., 2014; Z. Wang et al., 2015).

Ackerman (2013) Demonstrated that some mobile applications, such as those of medical fitness apps on Android systems, hosted by some third-party companies or individual hosts, are potentially a risk when downloaded or accessed, leading to privacy violations and the leakage of sensitive information, which was also corroborated by the study findings for (Arora et al., 2014; DeFord, 2022). When employees use mobile devices to access information, they become particularly vulnerable to cyberattacks if the devices are not correctly configured or if the organization lacks a policy governing personal device use, as these devices serve as access points to sensitive information that may not be adequately protected. The lack of comprehensive security for mobile devices can lead to unauthorized access to EHRs.

Research indicates that health care organizations can implement network segmentation and access control measures to mitigate cyberattacks in health care systems, thereby achieving digital maturity and effectively safeguarding the critical infrastructure (He et al., 2021; Kruse et al., 2017). The protection of digital and wireless medical networks is crucial. Intrusion detection and prevention systems play a vital role in identifying, blocking, and isolating malicious activities within a medical network by monitoring network traffic for unusual or suspicious patterns and automatically preventing such threats (Vukotich, 2023). Table 6 below presents studies that have addressed vulnerabilities arising from technology within health care systems.

Table 6. Summarizes recent studies on technology factors of vulnerability to cyberattacks

Authors	Methods	Domain	Study Contributions	Limitation
(Vukotich, 2023)	Literature review and conceptual	Health care	The study provides an understanding of the zero-trust approach as the most efficient way to protect health care from cyberthreats using the pillars framework.	The study lacks empirical data and case scenarios that emphasize industries beyond health care.

Authors	Methods	Domain	Study Contributions	Limitation
(C. J. Dameff et al., 2019)	Mixed methods	Health care	The study contributed to the development of a novel high-fidelity clinical simulation, providing insight into the fact that medical devices can be hacked without health care staff's knowledge.	Sample sizes for simulated cases were N = 3, limiting generalizability. Also, there are artificial constraints of simulation due to adherence to a scripted pathway.
(Burns et al., 2016)	Literature review	Health care	The paper provides a chronology of medical security, offering valuable understanding of the evolution of challenges to medical device security and responses to regulation and legislation.	The article concludes with a brief discussion of the future of medical device security, but does not provide a detailed roadmap or specific recommendations for addressing ongoing and emerging challenges.
(Zhan et al., 2024)	Quantitative method, deductive reasoning	Health care	This study examines the impact of various cybersecurity threat factors on the adoption of health information systems (HIS) in healthcare organizations, categorizing these factors into external attacks, employee-related factors, and technology-related factors. Furthermore, provides insights on how it can be mitigated.	Due to the limited scope of the study, the article did not discuss important areas such as integration, resource constraints, and communication. It cannot be generalized as it is restricted to Pakistan.

Authors	Methods	Domain	Study Contributions	Limitation
(Kioskli et al., 2021)	Narrative review and the use of Network living lab.	Health care	The paper provides a detailed analysis of the current landscape of cybersecurity challenges in the health care sector, highlighting the specific vulnerabilities that make healthcare organizations targets for cyberattacks; furthermore, it proposes a living lab.	Lack of empirical data and implementation of the proposed living lab
(Lopatina et al., 2021)	Narrative review (Risk analysis tool)	Health care	The paper presents an analysis of vulnerabilities, risks, and potential mitigation strategies related to IoMT tools and systems, particularly in the context of cloud infrastructure.	Absence of quantitative data and limited qualitative analysis on the practical challenges health care may face during implementation
(Szczepaniuk & Szczepaniuk, 2023)	Multiple study designs (Blockchain, software modeling, literature review)	Health care	The paper presents a blockchain framework for implementing cryptographic proof of smart contracts in the data processing of health care systems.	The authors acknowledged that blockchain networks remain vulnerable to various threats, including 51% attacks, node count, and network computing power.
(Svandova & Smutny, 2024)	Scoping review	Health care	The review identifies progress in designing a security framework for IoMT risk assessment, with an emphasis on the sociotechnical perspective and management, as well as frameworks for evaluating the security level of information systems that utilize IoMT in health care.	Authors also emphasized the need for comprehensive operational security frameworks for IoMT and privacy risk management, with a focus on a sociotechnical perspective.

Authors	Methods	Domain	Study Contributions	Limitation
(Alhammad et al., 2022)	Literature review	Health care	The paper reviews existing literature on cyber threats affecting the integration of medical devices with electronic medical records and highlights various types of cyber threats and impacts. and provides understanding of security, safety, and privacy issues.	The study is a literature review and did not address empirical issues or undergo validation testing.
(Giansanti, 2021)	Literature review	Health care	The study offers a comprehensive overview of cybersecurity challenges in the health care sector, particularly regarding digital health technologies and their impact on patient safety and health, as well as the need for security in non-medical device technologies.	It does not provide specific solutions to the issues and lacks empirical data and quantitative assessments of the cybersecurity risks or the effectiveness of proposed solutions.

This thorough review of the literature on the technological factors contributing to vulnerabilities in health care systems reveals that the challenges identified and discussed in the tables and the previous paragraph are critical technological issues within the field of health care (C. J. Dameff et al., 2019; Ewoh & Vartiainen, 2024; Giansanti, 2021). However, these technological vulnerabilities should not be addressed in isolation from other contributing factors, nor should they be approached as purely technocentric solutions, given the essential role of users (Davis et al., 2014; Le & Hoang, 2017). Therefore, as technology applications continue to evolve in this era of IoMT, there is an urgent need for a comprehensive operational security framework to protect health care systems (Svandova & Smutny, 2024). Implementing such a framework could lead to the robust protection of health care systems against technological vulnerabilities that have led to cyberattacks (Burns et al., 2016; Vukotich, 2023).

2.6 Human factors of vulnerabilities

The human factors play a crucial role in managing health care systems, which consist of individuals, such as physicians, nurses, administrative staff, IT teams, and patients involved in delivering and receiving health care diagnostics and services(Nifakos et al., 2021). Advancements in technology have introduced new risks, particularly impacting human employees, patients who use health care systems for health care and service delivery (Sardi et al., 2020). Notably, it is not just hackers or malware that pose a significant threat to health care. Research has indicated that humans in health care operations are the most vulnerable link in the context of cyberattacks (Nifakos et al., 2021).

Human factors, such as employees interacting with malicious phishing emails without awareness, using weak passwords, and delaying updates to medical devices and software, can create vulnerabilities that lead to breaches of sensitive health information (Branley-Bell et al., 2020). Although technological vulnerabilities have emerged as a primary source of breaches, they cannot be separated from human factors when designing technologies for health care use. Humans play a pivotal role in facilitating and perpetuating such attacks within health care (Gabriel et al., 2018). Some of the human factors contributing to the vulnerabilities in health care include a lack of cybersecurity awareness and training, human error and negligence, insider threats, social engineering, workarounds, convenience, leadership and security culture (Coventry et al., 2020; He et al., 2021). This human perspective of vulnerabilities to cyberattacks is discussed as follows;

2.6.1 Lack of cybersecurity awareness and training

Inadequate awareness and training among health care personnel significantly contribute to vulnerabilities (Haukilehto, 2024; Khando et al., 2021). In health care settings, employees are primarily trained to prioritize life-saving measures for patients, with their training focusing on clinical activities specific to health care delivery rather than recognizing fraudulent or harmful emails related to cyber threats(Coventry & Branley, 2018; C. J. Dameff et al., 2019; Offner et al., 2020). This emphasis has led to many healthcare workers lacking awareness and familiarity with essential cybersecurity practices, such as detecting phishing attempts or understanding the importance of using multifactor authentication for secure login access (Giansanti, 2021; He et al., 2021). Consequently, this lack of training and awareness often places them in insecure environments, making them susceptible to cyberattacks or breaches of health information (Arain et al., 2019; Haukilehto, 2024). Insufficient training and awareness can result in inadvertent errors that compromise the security of health care systems and the confidentiality of patient health records.

2.6.2 Human error and negligence

Human error-related vulnerabilities often arise from inadequate preparation for managing cyberattacks, which impedes the ability to identify unsafe environments or threats when cybercriminals use phishing schemes to distribute ransomware through deceptive emails (Carayon, 2006; Filipec & Plášilb, 2021). Such errors or negligence may result from improper handling of patient information and incorrect security protocol configurations (Jalkanen, 2019; Sittig & Singh, 2016). For example, an employee who fails to comply with necessary measures may disregard security protocols or overlook warning signs, thereby creating opportunities for cybercriminals to exploit vulnerabilities in health care operations to execute extensive attacks(Slayton, 2021; Wilner et al., 2021). Furthermore, fatigue and stress significantly contribute to these vulnerabilities. In scenarios with insufficient funding for security investments and understaffing, health care workers often work long hours and experience exhaustion due to work pressure, which can lead to suboptimal decision-making (Gordon, Wright, Glynn, et al., 2019; Jalali, Razak, et al., 2019). Under these conditions, health care employees may inadvertently commit errors, such as clicking on unsafe links or leaving computer systems unsecured(Gordon, Wright, Aiyagari, et al., 2019). Cybercriminals can exploit these mistakes to launch ransomware attacks on critical health care infrastructure, thereby compromising sensitive patient health records. The consequences include public information breaches, regulatory fines, and exposure of sensitive data.

2.6.3 Insider-based threats

Insider threats or employee-based vulnerability factors refer to risks that originating from individuals within a health care organization, such as health care workers, administrative staff, or IT personnel, who have legitimate access to health care information systems and sensitive data (Chua, 2021; Cybersecurity Insider, 2024; Luna et al., 2016). While technological and complex systems significantly contribute to vulnerabilities in health care systems, human factors, particularly employee-based threats present complex and unpredictable risks due to the nature of attacks and incidents arising from trusted employees (Arafa et al., 2023; Cybersecurity Insider, 2024). Insider employees or external actors can instigate breaches of patient data. Although many breach incidents are attributed to external parties. The most undetected and damaging incidents often originate from insiders within a health care organization (S. Choi et al., 2018). These employees may compromise the security of the health care system either intentionally or unintentionally (Anti & Vartiainen, 2024). In a health care environment where substantial amounts of patient and medical information are stored in the cloud and accessed routinely to provide health services, minor security lapses such as password sharing among employees,

misplaced devices, or failure to adhere to standard security protocols can lead to significant cyberattacks and breaches (Branley-Bell et al., 2020; Coventry et al., 2020). A review of the literature indicates that over 70% of breaches and data fraud are caused by employee-based insiders within an organization (Bhuyan et al., 2020). Although it is less common, it cannot be excluded that malicious employees pose a greater risk, as they may be motivated by financial gain, personal grievances against the organization, or external coercion (Anti & Vartiainen, 2024). These types of employees may exploit authorized access to steal sensitive information and manipulate or expose patient-sensitive data to public networks. Employee-based threats are perilous as they can bypass undetected perimeter defences, with their actions often appearing as routine work activities or authorized by health care organizations.

2.6.4 Leadership and culture.

Leadership and organizational culture play crucial roles in shaping employee-related factors that contribute to lapses in security culture, which can lead to vulnerabilities and cyberattacks in health care systems (Coventry et al., 2020). Health care organization that cultivates an inclusive security culture through intentional and effective leadership enhances awareness, promote adherence to protocols, and mitigate the risk of cyberattacks and human errors (Triplett, 2022). Health care organization leaders need a strong cultural understanding of cybersecurity, as a lack of top-level emphasis on security within the operational framework can impede health care professionals' compliance (Nicho & McDermott, 2019; Sittig & Singh, 2016). This may lead to reluctance to report security issues due to fear of blame, thereby increasing vulnerability and the risk of cyberattacks. In health care organizations, IT teams typically focus on addressing common vulnerabilities and applying patches, whereas senior clinicians prioritize patient flow and meeting turnover targets. This cultural divide may lead to the underprioritization of cybersecurity risks until a cyberattack or breach affects the entire health care system. Leadership is vital to shaping an organization's cybersecurity posture, as leaders are responsible for fostering a culture that includes shared values, beliefs, and norms that guide employee behavior (Sari et al., 2022). An exemplary security culture is characterized by visionary leadership that enhances resilience against cybersecurity vulnerabilities and protects health care systems from cyberattacks and breaches.

In summary, existing literature reviews and studies have shown that the social dimension of vulnerabilities, particularly those rooted in the human aspect, remains underexplored (Davis et al., 2014; He et al., 2021). To bridge these gaps, researchers such as (Nicho & McDermott, 2019; Zimmermann & Renaud, 2019) have proposed

humans as part of the solution rather than the problem. The human factors of vulnerability will continue to be apparent when health care management or leadership fails to prioritize cybersecurity culture to address these issues highlighted, this may cause employees to misunderstand their responsibilities (Albalawi et al., 2017; Feeley et al., 2022). Consequently, many employees may disregard security policies and engage in practices that compromise security. While the likelihood of human error may increase owing to insufficient awareness and training, resulting in unintentional mistakes and deliberately calculated insider threats (Abraham et al., 2019). A holistic approach is essential to address human cybersecurity factors effectively (Pollini et al., 2022). This dissertation adopts a comprehensive sociotechnical approach to address these issues, which is discussed in subsections. Table 7 presents studies conducted on human factors related to vulnerabilities in health care.

Table 7. Summaries of recent studies on human factors of vulnerability to cyberattack

Authors	Methods	Domain	Study contributions	Limitations
(Wasserman L. & Wasserman Y., 2022)	Qualitative Narrative Review	Health care training for non-cybersecurity health care professionals	The study provides an understanding of hospital cybersecurity risk for non-health care professionals and analyzes vulnerabilities through the evaluation of current mitigation strategies.	The study is country-focused on the United States and cannot be generalized for a global perspective, and lacks a quantitative assessment.
(Kaberuka & Johnson, 2020)	Qualitative interview	Health care sociotechnical cybersecurity training and method for radiology	The study contributed to improving PACS cybersecurity by validating sociotechnical security challenges using STAMP with NIST integration in a Rwandan hospital.	The study also acknowledges that it serves as a starting point for the sociotechnical method and requires analysts to be familiar with its application. Also, it focuses on developing nations.
(Khando et al., 2021)	Qualitative systematic review	Health care & Others, training for information security awareness	The study identifies and classifies Information security awareness methods and factors in the organizational context of both the private and public sectors through a systematic review of	The method was literature. its limited in the factors of implementation and evaluation of ISA elements.

Authors	Methods	Domain	Study contributions	Limitations
			content development methods and factors for enhancing employee awareness.	
(Sardi et al., 2020)	Qualitative systematic review	Health care	The authors provide insight through a review of cybersecurity risks in the health care sector and highlight the need for cybersecurity risk management that currently lacks attention.	The study necessitated an empirical approach and the provision of practical solutions for health care facilities.
(Sari et al., 2022)	Qualitative: Literature review	Health care cybersecurity policy management, cultural development programs, and training	The study provides managers and policymakers with an understanding of individual and organizational factors to consider when developing effective information security policies and programs. The study also revealed that human factors play a significant role in the effectiveness of information security, which is rooted in management support, cues to action, and organizational culture.	There is a lack of an established model, and the focus was on identifying a research gap. Additionally, there is a lack of patient controls in information security policies and programs.
(Abraham et al., 2019)	Qualitative Interviews	Health care cybersecurity challenges and practices	The study provides insight into cybersecurity challenges and practices in US health care, revealing systemic shortcomings, including poor IT governance, limited risk awareness, and ineffective leadership.	Country focus and lack of quantitative validation, which may require further studies for generalization.
(Hijji & Alam, 2021)	Multivocal Literature Review	Health care social engineering attacks and national security	The studies provide an understanding of social engineering cyberattacks and identify the rising scam emails, phishing, and misinformation campaigns	The study scope is limited to the COVID-19 context, which may restrict the longevity of the insights.

Authors	Methods	Domain	Study contributions	Limitations
			in health care amid COVID-19.	
(Feeley et al., 2022)	Qualitative case study	Health care National cyberattacks and orthopedic services	The study identifies challenges in Ireland's hospital orthopedic departments and recommends adopting secure messaging, hard-copy imaging, and local triage systems in the event of a cyberattack. Also recommends training and charging the leaders with proper vigilance and awareness	The study focused on Irish health care systems, and the findings are based on observational experience and cannot be generalized to other countries' contexts.
(Gordon, Wright, Glynn, et al., 2019)	Quantitative	Health care Training for Phishing and Vulnerabilities	The study contributed to the development of an evaluation phishing training program for US healthcare system employees through a gamification approach using simulation, and identified that a high risk of cyberattacks is associated with high-risk employees who lack phishing training.	The training method relied on an online video approach, which may have lacked engagement and limited generalization due to the limited demographic data available.
(Coventry et al., 2020)	Qualitative Interview	Health care organizational cybersecurity behavioral training	The study provides insight into insecure behavior among health care staff and the key factors that facilitate it. It offers a method for promoting effective, secure behavior to enhance cybersecurity in health care.	The study focuses on the European region; however, generalization may not be fully applicable to other regions, as the work culture contexts across the continent may differ.

2.7 Process factor of vulnerabilities

The Proper management of cybersecurity-related organizational processes within health care information systems can significantly improve healthcare providers'

performance and support the delivery of secure, uninterrupted services (Al-Qarni, 2023; Filipec & Plášilb, 2021). Poorly managed systems can result in cyber threats or attacks (Abbou et al., 2024; Harrison et al., 2022). The inadequacy and inefficiency of cybersecurity controls within health care systems' operational processes are critical weaknesses that contribute to their vulnerability to cyberattacks and breaches of sensitive patient information. While technology and human factors are essential components or factors, the processes and workflows within health care systems also play a significant role in creating vulnerabilities in the health care organization's environment (Heeks, 2006; Malatji et al., 2020). Some of the inadequacies that lead to operational process vulnerabilities include a lack of standardized security procedures, poor incident response planning, inadequate risk management processes, and insufficient backup and recovery procedures(Jalali, Russell, et al., 2019; Sullivan et al., 2023).

2.7.1 Lack of standardized security procedures

Standardizing security procedures is essential to ensure the safety of health care operations, prevent operational errors, and adhere to regulatory best practices (C. J. Dameff et al., 2019). It is also vital to protect the cybersecurity of the health care infrastructure. The literature reveals that many health care organizations lack standardized security operating procedures, leading to inconsistent practices and increased vulnerability to cyberattacks (Abraham et al., 2019; Arafa et al., 2023). In the absence of well-defined guidelines for sensitive data handling, access control, and incident response, health care professionals may lack clarity about appropriate standard procedures, especially when confronted with emergency cyber threats.

2.7.2 Poor incident response planning

Effective incident response processes are crucial for mitigating breaches of sensitive information and addressing cyber threats(Jalali, Russell, et al., 2019; Sullivan et al., 2023). However, incident response management planning is still insufficiently studied and implemented by many health care organizations (Haukilehto, 2024; He et al., 2022a). This dissertation employed qualitative surveys, including open-ended questionnaires, to enhance the resilience of health care organizations against cyber incidents. Health care organizations with well-defined incident planning and reporting, which regularly conduct incident response security drills and plans, experience fewer breaches of health information and reduced data loss compared to those without proactive incident response planning(Ireland et al., 2019; Jalali, Russell, et al., 2019). This inefficiency can be attributed to inadequate training, insufficient resources, and poor implementation. A proactive incident response plan

is essential to minimize the impact of cyberattacks (Bhuyan et al., 2020; Haukilehto, 2024). Health care organizations that lack incident response management and planning processes may struggle to mitigate cyberattacks and breaches, restore systems to a secure state, and comply with notification requirements for affected patients in the event of breaches or incidents reporting, and data protection as mandated by the GDPR and HIPAA omnibus rule.

2.7.3 Inadequate risk management processes

Risk management processes are crucial for safeguarding against cyber threats in the rapidly evolving digital health care landscape (Sullivan et al., 2023). Numerous health care organizations fail to conduct regular risk assessments of their critical systems, resulting in significant vulnerabilities (Arafa et al., 2023). Failure to implement risk assessment protocols and conduct regular checks can compromise operational processes, thereby increasing susceptibility to cyberattacks and data breaches (Ewoh & Vartiainen, 2024). The lack of comprehensive cyber-risk assessments complicates the mitigation strategies and proactive measures, thereby exposing sensitive data and critical infrastructure within health care systems to potential threats (Sardi et al., 2020). When organizations overlook risks, delay remediation processes in response to cyber threats (Dissanayake et al., 2023), and use unsupported devices without clear policies and regular assessments, the ability of health care systems to detect advanced persistent threats and vulnerabilities is weakened, thereby increasing the risk of data breaches and cyberattacks.

2.7.4 Poorly structured data backup and recovery

Inadequate data backup and recovery procedures present a significant risk to health care operations, potentially resulting in substantial data loss and prolonged downtime in the event of cyberattacks (Aldosari, 2025). Deficiencies in the data structure and architecture of cloud-based systems can increase vulnerability, especially when system protocols and compliance standards are not regularly updated (Dias et al., 2021; Kandasamy et al., 2022). The primary factors contributing to these vulnerabilities include outdated systems and servers, single point of failure, redundancy, insufficient storage, infrequent backups, insecure data exchange and processing. All of these problems can enable access to health care to be exploited by cybercriminals (Filipec & Plášilb, 2021). Adequate data backup and recovery procedures are crucial in ensuring business continuity during a cyberattack because they enable rapid restoration and minimize disruptions (Bhuyan et al., 2020; Jalali, Russell, et al., 2019). The rise in data breaches and data loss resulting from inadequate backup and recovery structures underscores the critical need for regular

data backups, a tested recovery plan, and a comprehensive health care policy governing data restoration to maintain cybersecurity hygiene. Conversely, health care organizations that neglect data backup and recovery face significant risks, including financial losses, reputational damage, legal liabilities, and compromised patient safety (Mohammed, 2022). The absence of comprehensive data backup and recovery strategies exacerbates the impact of cyberattacks, turning cyber incidents into full-blown crises. Table 8 summarises studies conducted by various authors and the solutions provided for the process factors of vulnerabilities and their limitations.

Table 8. Summarizes recent studies on the process factors of vulnerability to cyberattacks

Authors	Methods	Domain	Study contributions	Limitations
(Abbou et al., 2024)	Qualitative observational study	Health care cybersecurity for clinical and operational health services	The study contributed by providing an understanding of how quantified ransomware attacks can be halted in hospital systems, with a proposition of empirical evidence of patient care effects.	The study also acknowledges that it serves as a starting point for the sociotechnical method and requires analysts to be familiar with its application. Also, it focuses on developing nations.
(Filipec & Plášilb, 2021)	Qualitative case study	Health care, cybersecurity, emergency hospital response, and crisis management.	The study provides a detailed account of how a hospital should respond to a crippling ransomware attack on a case hospital, evaluate the organizational weaknesses, recovery measures, and draw broader cybersecurity preparedness lessons.	The study is a single-case study and specific to the Czech context, which may limit generalizability.
(Harrison et al., 2022)	Qualitative descriptive	Health care cybersecurity preparedness, continuity, and clinical IT systems	The study provides real-time mitigation of ransomware impacts using direct DICOM transfers, paper charting, and hospital EMR, detailed committee-based response, and documented phased restoration of services.	The study focuses on radiation oncology systems and may not be generalized to the broader hospital environment.

Authors	Methods	Domain	Study contributions	Limitations
(Mohammed, 2022)	Qualitative exploration studies	Health care organization recovery strategies for breaches and cyberattacks	The authors identify recovery strategies for breaches in governance, communication, technical remediation, legal and regulatory compliance, stakeholder engagement, and rebuilding trust for post-breaches.	The study is conceptual and requires empirical validation.
(Bhuyan et al., 2020)	Qualitative narrative review	Health care cybersecurity emergency and incident response	The study provides an understanding of the primary cyber threats in health care and proposes multi-stakeholder, proactive policy and organizational recommendations for governance, training, and investment.	The study focuses on narrative reviews and may lack comprehensive insights, as well as primary data collections.
(He et al., 2022b)	Qualitative case study	Health care cybersecurity center for incident response improvement and threat intelligence management	The study identifies intelligence and threat gaps and proposes a cyber threat intelligence-enhanced incident response framework.	The concept remains to be implemented in a real organizational environment and has yet to be tested.
(Arafa et al., 2023)	Qualitative literature, narrative review	Digital health care, cybersecurity, and implications for innovative health care systems.	The paper provides a comprehensive overview of emerging digital technologies for health care and catalogs various vulnerabilities. And proposes a cybersecurity framework for risk assessment, controls, and management for health care systems.	The study recommendation is broad and is mainly a narrative review, which may be challenging to implement, test, and apply. At the same time, solutions may be narrower within a broader context of coverage in line with the findings.
(Jalali, Russell, et al., 2019)	Qualitative systematic review	Health care incident response planning and strategy design	The student provides an understanding of incident pre- and post-planning strategies and develops eight aggregated response	The framework has not been tested for validation in real-world health care systems

Authors	Methods	Domain	Study contributions	Limitations
			strategies. A framework for managerial and technological response to cyberattacks management.	
(Al-Qarni, 2023)	Qualitative narrative review	Health care operations, cyberattacks, and impacts on the organization	The study identifies types of cyberattacks, their impact, and proposes mitigation strategies	Some of the types of attacks may be obsolete due to newer trends and technologies landscape evolving, and require further research and empirical testing.
(Patel & Makaryus, 2024)	Qualitative narrative review	Health care implanted and wearable devices cybersecurity	Provides understanding of the cybersecurity risk posed by implanted and wearable devices and proposes protection methods for policymakers, manufacturers, and patients to enable secure access and data literacy.	The study judgment is based on expert opinion and lacks empirical data for validation
(Sullivan et al., 2023)	Mix method	Health care cybersecurity emergency preparedness	The report provides an understanding of Hospital cyberattacks, preparedness, and mitigation strategies. Additionally, the study reveals that the case organization lacks an emergency operational plan and fails to activate it during attacks.	The anonymity prevents analysis by hospital type. Moreover, the sample size distribution via listservs may introduce bias.
(Haukilehto, 2024)	Mix methods (dissertation thesis)	Health care cybersecurity incident management	The study enhanced the understanding of cybersecurity in healthcare by introducing the PAR model for cybersecurity management, encompassing policies, user awareness, and incident reporting.	The study acknowledges a lack of studies on incident management. Additionally, the author advocates for a sociotechnical approach to address healthcare cybersecurity challenges.

2.8 Sociotechnical cybersecurity framework

Based on the literature above, it is evident that cybersecurity in health care has been a significant concern in this era of digitalization and technological advancement. Most importantly, when factoring in the rate of vulnerabilities of health care systems to cyberattacks or breaches of health information. Health care organizations have to pay the enormous cost and bear these consequences that lead to the compromise of sensitive patient data and disruption of health care services (Kioskli et al., 2021). Different authors have approached cybersecurity in health care using various theories, contexts, and solutions to curb vulnerabilities and cyberattacks in health care systems, as shown in the tables above.

This dissertation highlights persistent gaps in understanding health care cybersecurity challenges, which likely contribute to the rise in health information breaches and cyberattacks. Based on the facts above, this dissertation consistently argues that addressing vulnerabilities in health care, which led to the breaches and attacks, requires recognizing that these vulnerabilities arise from humans, technology, and organizational processes (Kaberuka & Johnson, 2023). This concept was categorized in published articles 1, 2, and 4, as well as in Tables 6, 7, and 8 above, under the themes for technology, processes, and humans that contribute to the vulnerabilities and cyberattacks. The study conducted by Coventry & Branley, 2018) revealed that in order to mitigate these vulnerabilities, there is a need for comprehensive transformation in human behavior, technology, and processes. This dissertation firstly interprets this issue as a sociotechnical problem and advocates for a sociotechnical cybersecurity framework as a holistic solution for health care systems (Ewoh & Vartiainen, 2024).

Malati et al. (2019) explored organizational cybersecurity, underscoring the necessity for joint optimization and proposing a sociotechnical cybersecurity framework to safeguard enterprises against cyberattacks. However, the framework was primarily generic and aligned with United States energy systems, suggesting a need for future research validation. Subsequently, Malati et al. (2020) advanced this research by validating the sociotechnical cybersecurity framework derived from the US energy sector and by calling for a health care specific sociotechnical framework to solve health care cybersecurity vulnerabilities.

Offner et al., (2020) Identified health care system vulnerabilities as a complex sociotechnical issue, advocating for a sociotechnical approach, although their study did not fully address this perspective. Kaberuka & Johnson, (2023) adopted a sociotechnical approach called STAMP for cybersecurity analysis, with the integration of the NIST cybersecurity method in health care for staff training and

cybersecurity risk management of PACS within the radiology department, and acknowledged it as the initial step to inform cyber risk management. Haukilehto, (2024) a dissertation study published by the University of Vaasa in 2024 proposed a PAR model for incident reporting and handling, focusing on policies, awareness, and reporting, and called for a sociotechnical approach as a way forward in addressing health care cybersecurity challenges.

To avoid security design gaps and failures, Heeks (2006) states that these issues must be resolved holistically, with technology, humans, and processes interdependent and jointly optimized (Appelbaum, 1997; Coventry & Branley, 2018; Malatji et al., 2019, 2020). The study conducted by Zimmermann & Renaud (2019), closely aligned to this dissertation concept, however, its focus was on the social perspective (humans' inclusion solely), neglecting the technical perspective in the study. The domain of study was generic and not in the context of health care systems.

None of these studies has developed a comprehensive or sociotechnical cybersecurity framework for health care systems that addresses vulnerabilities, cyberattacks, and threats by considering technology, humans, and processes as an integrated whole. This dissertation addresses this gap and the underlying cybersecurity issues in health care by proposing a sociotechnical cybersecurity framework and solutions to prevent vulnerabilities, cyberattacks, and breaches of sensitive health information in health care systems.

3 RESEARCH METHOD

3.1 Research approach

According to (Saunders et al., 2009), research approach refers to the steps in the research process that explain how research data are collected, analysed, and interpreted. Inductive, deductive, and abductive reasoning are three distinct research approaches that offer different pathways to understanding and developing knowledge. The deductive approach refers to the testing of a theory after forming hypotheses and conducting data collection, whereas the inductive approach involves the development of a theory after data collection (Silverman, 2013a). In research, an abductive approach is a strategy that involves making informed guesses or hypotheses based on available observations, then testing those hypotheses to see if they provide a plausible explanation for the observed phenomena. Figure 4 briefly explains the research approaches and adopted method for this study.

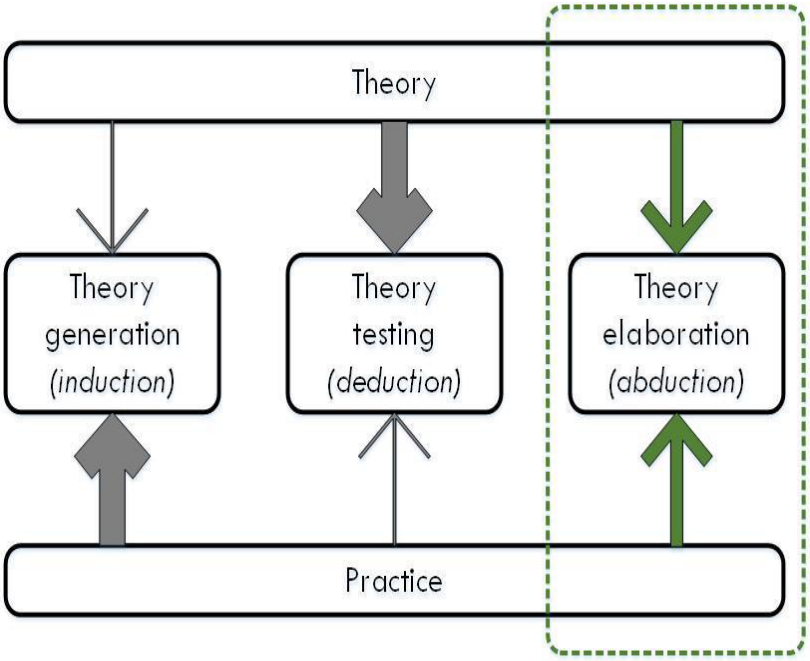


Figure 4. Inductive, deductive, and abductive research and selected approach (Adapted from (Ketokivi & Choi, 2014)

Since cybersecurity problems in health care systems are complex and constantly evolving, this study uses an abductive research approach to investigate and explain how technological vulnerabilities, human factors, and organizational practices interact. Abduction is an effective technique for solving problems when existing theories do not fully explain what people see in the real world. This allows

researchers to move back and forth between real-world data and theoretical constructs to develop the most likely explanations (Tavory & Timmermans, 2014). This study does not start with a hypothesis (as in deduction) or conclude from the data (as in induction). Instead, it starts with surprising or troubling cases, such as recent breaches of EHRs or cyberattacks in hospitals, and seeks to identify patterns or mechanisms that best explain these events.

The research uses case studies, literature reviews, expert interviews, and analyses of cyber incidents to better understand why health care systems remain vulnerable to cyberattacks despite technological improvements. Abduction allows for the combination of existing sociotechnical theories, like actor-network theory or system-of-systems thinking, with new empirical data to create a more nuanced understanding of what makes people vulnerable and how they respond (Benbasat et al., 1987). The method helps build a conceptual framework in stages, changing theoretical assumptions when real-world events do not align, such as when users behave in unexpected ways or systems fail during cyber incidents.

It is important to note that abductive reasoning can handle the uncertainty and context-specificity inherent to cybersecurity problems. For example, when trying to figure out how to improve operational practices in EHRs data exchange and breach prevention, abduction can help bring together conflicting results and come up with plausible solutions that are both technically sound and possible for the organization to implement (Reichertz, 2007). So, this method is very useful and helpful for building a sociotechnical framework that is both grounded in theory and able to respond to the changing threats that healthcare systems face.

3.2 Definition of qualitative methods research

Qualitative research methods are a set of approaches to studying social phenomena by examining non-quantitative data such as words, literature reviews, texts, interviews, and observations. The goal is to explore, understand, and interpret these phenomena. Quantitative research uses statistical tools to measure and test hypotheses, but qualitative research is more interested in capturing the richness and depth of human experience. It often focuses on how people make sense of their surroundings, relationships, and actions (Denzin & Lincoln, 2011). This method is especially useful in areas that are difficult to understand or are highly complex, such as cybersecurity in health care, where humans, processes, and technology are all closely intertwined.

Qualitative methods are always interpretive and constructivist, and they are often used inductive or abductive logic to build theories or frameworks from the ground

up (Creswell & Poth, 2016). Semi-structured interviews, online open-ended questionnaire, focus groups, case studies, and thematic analysis are all standard methods. Each one gives you flexible, context-sensitive tools to look into research questions that need depth instead of breadth (Silverman, 2013b). Qualitative methods enable researchers to uncover the lived realities, motivations, and challenges of stakeholders, such as IT professionals and health care providers, in studies of sociotechnical vulnerabilities and security practices. These insights may not be available from purely quantitative data.

3.3 Rationales for qualitative methods research

This dissertation uses qualitative research methods to investigate the deeply rooted sociotechnical aspects of cybersecurity weaknesses in health care systems. The research questions aims to understand why health care systems are vulnerable, how operational practices affect data security, and which frameworks can help address these problems. Qualitative methods are best for capturing the contextual, human-centered, and processual aspects of these issues (Tisdell et al., 2025). Cybersecurity in health care is not just a technical issue; it is a complicated mix of technology, people's actions, how institutions work, and how they are run. So, just looking at numbers would not be enough to get to the details needed for building theories and frameworks.

3.4 Philosophical world views and paradigms

A researcher's philosophical worldview or paradigm guides every research project. It affects how they see reality, build knowledge, and make sense of data. These paradigms are fundamental in qualitative research because they affect the methods used and how the results are understood (Creswell & Poth, 2016). Qualitative research is typically classified as positivist, interpretive, or constructivist (Myers & Avison, 2002). Positivist research underscores rational and systematic approaches for objective inquiry (Carson et al., 2001). A positivist approach assumes that the world is uniform for all individuals and substantiates its reasoning through regularities, classifications, frameworks, and causal connections. Interpretive studies prioritize interpretation and comprehensive subject knowledge. (Burnell & Morgan, 1979) assert that this approach is founded on the premise that individuals interpret their experiences uniquely. Moreover, the researcher’s findings and theory are congruent in interpretative analyses. Ultimately, constructive studies aim to contest the status quo, perceiving contemporary social conditions as restrictive and alienating (Orlikowski & Baroudi, 1991). This dissertation is primarily informed by

the interpretivist paradigm, which posits that reality is socially constructed and context-dependent. From this perspective, knowledge is co-created through interaction between the researcher and participants, making it particularly well-suited to exploring complex sociotechnical problems such as cybersecurity in health care (Guba & Lincoln, 1994).

People who believe in interpretivism do not believe in a single, objective truth. Instead, it values different points of view and meanings that emerge through conversation, reflection, and context. This is important for understanding the different experiences of stakeholders, such as IT professionals, doctors, and hospital administrators, whose use of technology and institutional structures shape how they handle security. The research also uses parts of the pragmatic paradigm, especially its abductive logic and its focus on solving real-world problems. Pragmatism lets researchers use different methods and focuses on results, relevance, and the usefulness of findings (Morgan, 2007). This is particularly important when dealing with real-world threats such as data breaches and cyberattacks in health care systems. These paradigms work together to give the study's qualitative, exploratory, and adaptive approach a philosophical basis. They ensure the researchers remain aware of the situation while seeking solutions that are both theoretically sound and useful in high-stakes contexts such as digital health care.

3.5 Research design and methods

This dissertation uses a multi-article qualitative research design that combines complementary methods to examine the sociotechnical weaknesses of health care systems that make them vulnerable to cyberattacks. The interpretive paradigm is the basis for the overall methodological structure. The sociotechnical system (STS) lens guides both theoretical development and empirical investigation. Each article helps to reach the overall research goals by using a unique qualitative design that includes literature synthesis, conceptual modelling, and empirical data analysis.

The first article uses a systematic literature review as a qualitative method to identify the main reasons why health care is vulnerable to cyberattacks. This design includes structured data collection, coding, and synthesis of peer-reviewed academic sources. It fits with the study's global scope and aims to find common sociotechnical patterns and problems. The second article builds on this by using a scoping review, which adds to the body of literature to create a conceptual framework for cybersecurity in health care. Both articles use secondary data and analytical tools to develop ideas applicable to the global context, which gives them a strong theoretical base.

Table 9. Methodological overview of articles

Research objective (dissertation-level)	Study method / article	Data source(s)	Analysis procedure (as)	Output (article/artifact)
Explored and Identify why healthcare systems are vulnerable to cyberattacks	Article 1: systematic literature review	Peer-reviewed articles (2012–2022), =70 studies	PRISMA-guided selection; thematic analysis (Braun & Clarke)	Taxonomy of vulnerability themes; and a sociotechnical solution
Examined the dynamics of factors of vulnerabilities and cyberattacks in the context of sociotechnical systems theory	Article 2: scoping review & conceptual modelling	Peer-reviewed articles (2012–2024), =76 studies	Scoping ynthesis; abductive model-building;	CKMIR-based-model, Sociotechnical framework (conceptual model)
Identify security and privacy concern with EHRs	Article 3: integrative review	Peer-reviewed articles on EHR privacy/security 2012-2024 = 57	Thematic synthesis; TOE mapping; checklist development	EHR security & privacy assessment Checklist (operational tool)
Examined management of cyberattacks incident within Finnish health care organization	Article 4: qualitative interviews (Finland)	12 open-ended online questionnaire data; national incident reports	Memo, sticky note thematic analysis; member-checking	Sociotechnical incidents respond framework

The third study used a qualitative conceptual research design, grounded in an integrative literature review, to identify cybersecurity and privacy issues in EHR systems and to develop a practical assessment checklist for health care organizations. Thematic analysis was used to identify common patterns of operational weaknesses, such as sharing data in risky ways, failing to follow the law, and not providing enough ways for people to give their consent. The study did not need ethical approval because it was based entirely on secondary data. However, scholarly integrity was upheld through careful sourcing and adherence to international data protection standards. The fourth article is a qualitative survey based on 12 open-ended online survey conducted in Finnish health care organizations. This research design allows us to examine how cyberattack incidents are handled in practice, using primary data and using sticky note to analyze the results.

The qualitative methods used in all four articles are carefully chosen to allow iterative theory-building, conceptual refinement, and analysis that takes context into account. All this work will help create a sociotechnical cybersecurity framework for health care. The unit of analysis ranges from global literature to national , giving the dissertation's methods depth and breadth. Table 3.1 summarizes the research design adopted for all four studies.

3.6 Data collection and procedure

The data collection and analysis for this dissertation were guided by qualitative principles, with different strategies used for each article's research goals and design. The first, second, and third articles used systematic, scoping, and integrative literature reviews, respectively. Data for the studies was collected through a structured search across six academic databases (PubMed, Web of Science, ScienceDirect, Scopus, Institute of Electrical and Electronics Engineers, and Springer) and a journal (Management Information Systems Quarterly). We established inclusion and exclusion criteria to ensure the sources were relevant, and we followed PRISMA guidelines to be clear about how we selected and combined them. The studies used thematic analysis, synthesis of results, and identification of new patterns related to weaknesses and sociotechnical factors affecting cybersecurity in health care systems.

Search Keyword

The following search strategy was used in the various databases to collect the articles for the reviews of article 1, 2, and 3 respectively.

Article 1: "(cybersecurity OR cybercrime OR ransomware) AND (healthcare) OR (cybersecurity in healthcare)."

Article 2: "Computer Security"[Mesh] OR Cyberattack*[tw] OR Cybercrime*[tw] OR "Cyber Crime"[tw] OR Cyberthreat*[tw] OR "Cyber Threat"[tw] OR "Cyber Crises"[tw] OR "Cyber Risk"[tw] OR "Cyber Incident"[tw] OR Cyber Operation[tw] OR Cyberspace[tw] OR "Cyber Infrastructure"[tw] OR "Data Breach"[tw] OR "Data Security"[tw] OR "Firewall"[tw] OR "Information Security"[tw] OR "Information Technology Security"[tw] OR "Information Systems Security"[tw] OR "Security Incident"[tw] OR "Network Security"[tw] OR Ransomware[tw] OR Malware[tw] OR Phishing[tw]) AND ("Health care Facilities, Workforce, and Services"[Mesh] OR "Delivery of Health care, Integrated"[Mesh] OR "Health care"[tw] OR "Health Information"[tw] OR "Health Information Management"[tw] OR "Health care Systems"[tw] OR "Health Systems"[tw] OR "Health System Infrastructure"[tw] OR "Medical Devices"[tw] OR Medical Technolog*[tw] OR Health Technolog*[tw] OR Health care Technolog*[tw].

Article 3:"Electronic Health Records"[MeSH] OR EHR[Title/Abstract] OR "Electronic Medical Records"[Title/Abstract]) AND("Cybersecurity"[Title/Abstract] OR "Data Security"[Title/Abstract] OR "Information Security"[Title/Abstract] OR "Data Privacy" [Title/Abstract] OR "Confidentiality[MeSH]) AND ("Data Sharing"[Title/Abstract] OR "Health Information Exchange"[MeSH] OR "Interoperability" [Title/Abstract]) AND ("Workflow"[MeSH] OR "Risk Management"[MeSH] OR Management [Title/Abstract] OR Process*[Title/Abstract] OR Administrat*[Title/Abstract] "

The fourth article's data collection involved conducting qualitative survey through online questionnaire (Prolific survey tool) to elicit information from health care IT and administrative staff in Finnish health care organizations. 12 participants filled the open-ended questions. Each participant took between 45 to 60 minutes to fill in the online questionnaire. Secondary data from Finnish national cybersecurity policies and incident reports backed these up. Memo sticky and content analysis was used for data analysis and grouped into themes.

A constant comparative approach was used throughout the dissertation to affirmed result and categories across studies. Using secondary literature, expert input, and field data together made the results more reliable and trustworthy. This approach used a range of methods to ensure the dissertation remained both theoretically deep and practically applicable.

3.7 Validity and reliability

In qualitative research, the concepts of validity and reliability are examined using criteria such as credibility, dependability, confirmability, and transferability (Guba & Lincoln, 1994). Using systematic methods for data gathering and analysis maintained high dependability. For instance, using established guidelines like PRISMA for literature reviews, sticky note and a spreadsheet for analysis to ensure that thematic development were clear and could be repeated. Detailed records of the search methods, inclusion criteria, qualitative data collection procedures, and coding frameworks made the process even more consistent.

The research used a reflexive approach to improve confirmability. This meant that the researcher critically looked at their own biases and kept a record of their analytic decisions throughout the process. Direct quotes from the data and clear explanations of what they mean show that the data and conclusions are consistent. Finally, transferability was supported by providing detailed descriptions of situations, such as the Finnish hospital cases, so readers could decide whether the results could be used in other health care systems . When combined, these methods ensure that the dissertation's qualitative findings are rigorous and reliable. This provides a solid basis for creating a sociotechnical cybersecurity framework that can be used across many health care settings.

4 ARTICLE SUMMARIES

4.1 Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review

This article uses a systematic literature review (SLR) to investigate why health care systems are becoming increasingly vulnerable to cyberattacks and proposes sociotechnical solutions to reduce these risks. To collect data, we did a structured search across six academic databases (PubMed, Web of Science, ScienceDirect, Scopus, Institute of Electrical and Electronics Engineers, and Springer) and a journal (Management Information Systems Quarterly). Researchers set up inclusion and exclusion criteria to ensure the sources were relevant and followed PRISMA guidelines to be clear about how to choose and combine them. The review examines 70 articles published between 2012 and 2022. It uses a sociotechnical systems perspective, which looks at how human behaviour, technology, and organizational structures (processes) interact. The review is based on the urgent need for a comprehensive understanding of health information security, given that threats such as ransomware, data breaches, and the hacking of medical devices are on the rise.

The SLR found five main themes that make health care systems more vulnerable to cyberattacks: human error, old legacy systems, lack of investment, complex network-connected end-point devices, and technology advancement (digitalization). Here is a short description of each of the five themes.

1. ***Human error*** is the most common reason for security breaches. This is because people are not trained, unaware, or lack a cybersecurity culture.

2. ***Old legacy systems*** are technologies that are no longer supported and do not have modern security features. They are also very easy to hack.

3. ***Lack of investment*** indicates that the healthcare sector suffers from underfunding, with critical infrastructure and cybersecurity training often neglected, contributing significantly to the rise in breaches of sensitive health information.

4. ***Complex end-point devices*** that are connected to a network, especially IoMT (Internet of Medical Things), which makes the attack surface much bigger.

5. ***Technology advancement (digitalization)*** – fast digital transformation without secure-by-design development or risk management that is built into the system.

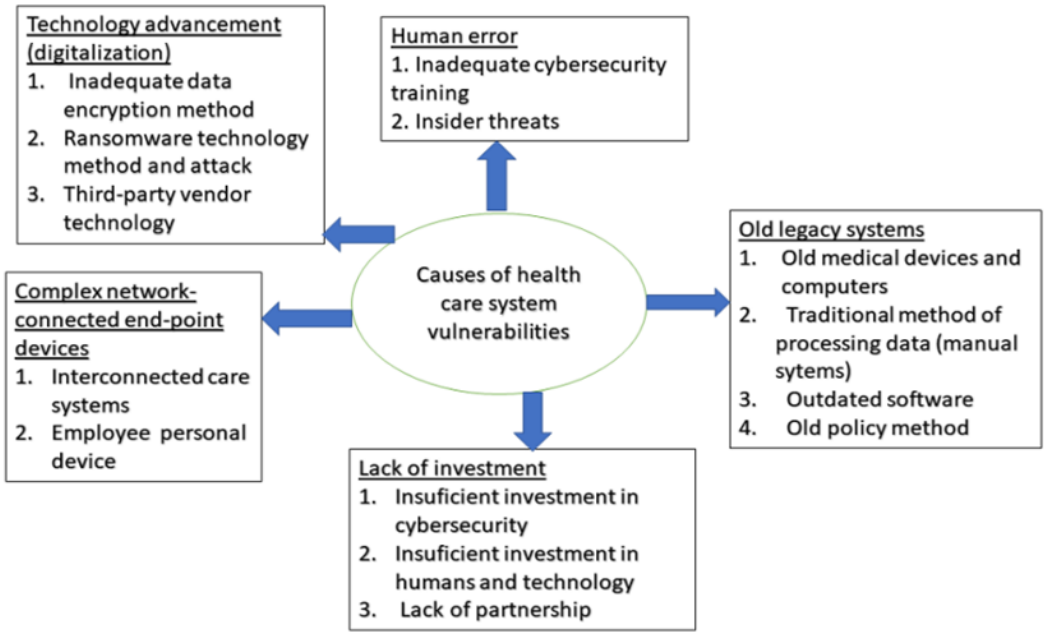


Figure 5. Themes: Causes of vulnerabilities in health care systems

Each theme is investigated from social, technical, and sociotechnical perspectives, underscoring the importance of integrated, cross-disciplinary responses. The article explained that traditional technical methods alone are not enough and must be combined with social strategies such as training, raising awareness, working together, and changing the way the government operates.

The results suggest several sociotechnical actions, including creating cybersecurity curricula, investing in secure infrastructure, eliminating legacy systems, adopting security-by-design approaches, and fostering cooperation among healthcare providers, IT developers, and policymakers. The study shows that, even though some solutions, such as training and policy changes, are being used, many interventions are still not being used enough or in the right way. The article concludes that a robust sociotechnical cybersecurity framework is essential for safeguarding health care systems.

4.2 Sociotechnical cybersecurity framework for securing health care from vulnerabilities and cyberattacks: Scoping review

The second article examines how health care systems are becoming increasingly vulnerable to cyberattacks, particularly as technology becomes more integrated and digitalized in medical settings. The study uses sociotechnical systems (STS) theory to investigate and categorize these vulnerabilities, recognizing that cybersecurity threats arise not only from technical flaws but also from how people act and how organizations operate. The main goal is to develop a conceptual sociotechnical cybersecurity framework that integrates humans, technology, and processes to prevent and address threats in health care settings.

Using databases such as PubMed, Scopus, and Web of Science, the review examined 76 peer-reviewed articles published from 2012 to 2024. The study identifies 12 main sub-factors of vulnerability, grouped into three main sociotechnical domains.

1. ***Technology***: including new technology integration, complex system design, third-party applications, limited monitoring, and weak access control.

2. ***Humans***: such as insider threats, inefficient training, and lack of cybersecurity professionals and security culture.

3. ***Processes***: including poor incident response plans, outdated policies, and a lack of audits.

Different types of cyberattacks can exploit different types of vulnerabilities. These attacks can harm health care organizations in many ways, including data theft, service disruptions, financial losses, and loss of patients' trust. The study suggests adopting the Proposed framework and its model: CKMIR (Cybersecurity Knowledge Management and Intelligence Response) model to address these complex problems.

This model is part of the larger sociotechnical cybersecurity framework. The main parts of CKMIR are:

1. ***Intrusion Detection***: watches system traffic and finds threats.

2. ***Monitoring User Behaviour***: Looks for unusual patterns in how people access and interact with things.

3. ***Threat Intelligence***: Gathers and combines information about new cyber threats.

4. ***Vulnerability Scanner***: Looks for known weaknesses in devices, systems, or user behaviour all the time.

5. ***Alert Sensor***: Sends automatic alerts to IT staff when it sees strange behaviour.

6. ***Cloud-Based Repository & Recovery***: Keeps backups safe and makes it easy to get them back quickly in case of an attack.

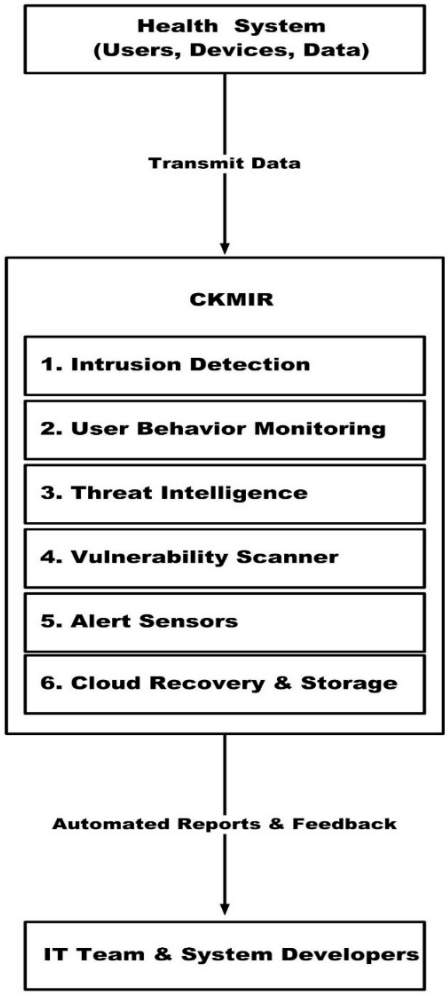


Figure 6. Sociotechnical cybersecurity model illustration

Figure 6. Sociotechnical Cybersecurity Model Illustration (Depicts the proposed CKMIR-based model with bidirectional interactions between healthcare systems, IT teams, and cybersecurity tools)

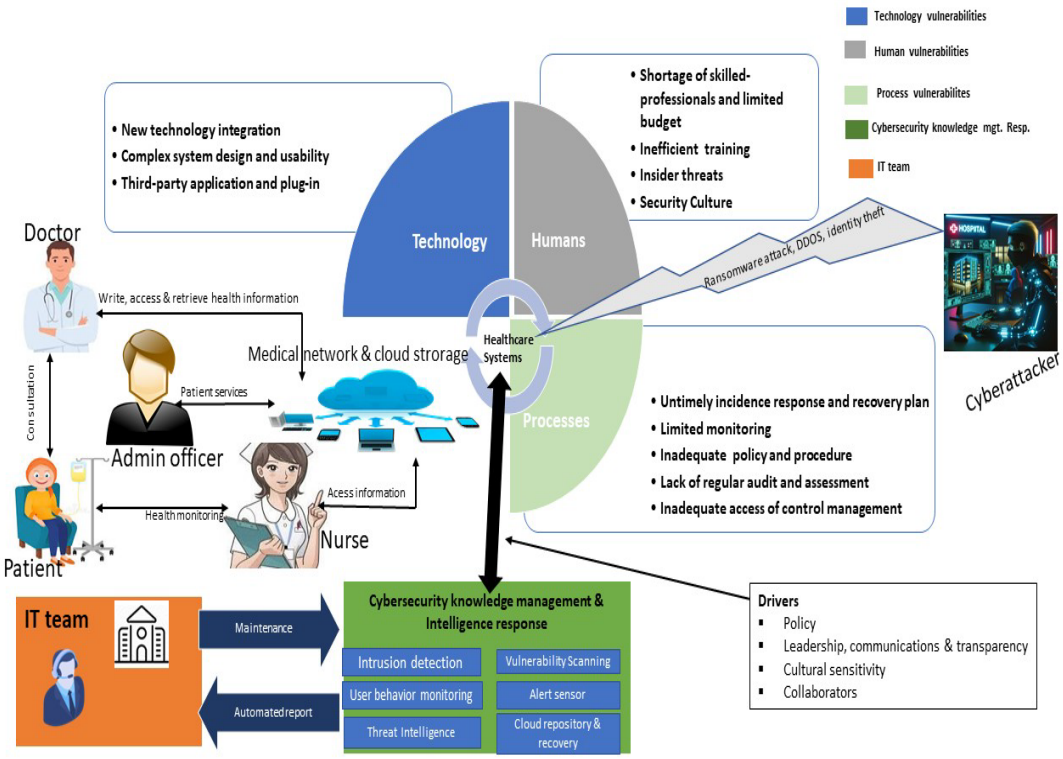


Figure 7. Sociotechnical cybersecurity conceptual framework

4.2.1 Linking the CKMIR system to the NIST model

The CKMIR elements align with the core functions of the NIST framework. The core functions of the NIST framework involve identifying, protecting, detecting, responding, and recovering. The CKMIR elements involve intrusion detection, vulnerability scanning, user behavior monitoring, alert sensors, threat intelligence, and cloud repository and recovery.

The unique value proposition of the CKMIR model lies in its configuration, dynamic integration, and real-time incident response optimization. Specifically, its unique value proposition is the provision of threat intelligence, human behavior analytics, and cross-component integration in the health care system. The CKMIR model applies to the health care system in its capacity to address complex health care problems in vulnerable areas, such as those arising from IoMT devices, cloud, EHRs, health care professionals, and patients. The model-specific sociotechnical contributions encompass the optimal identification and mitigation of vulnerabilities arising from technology, humans, and processes.

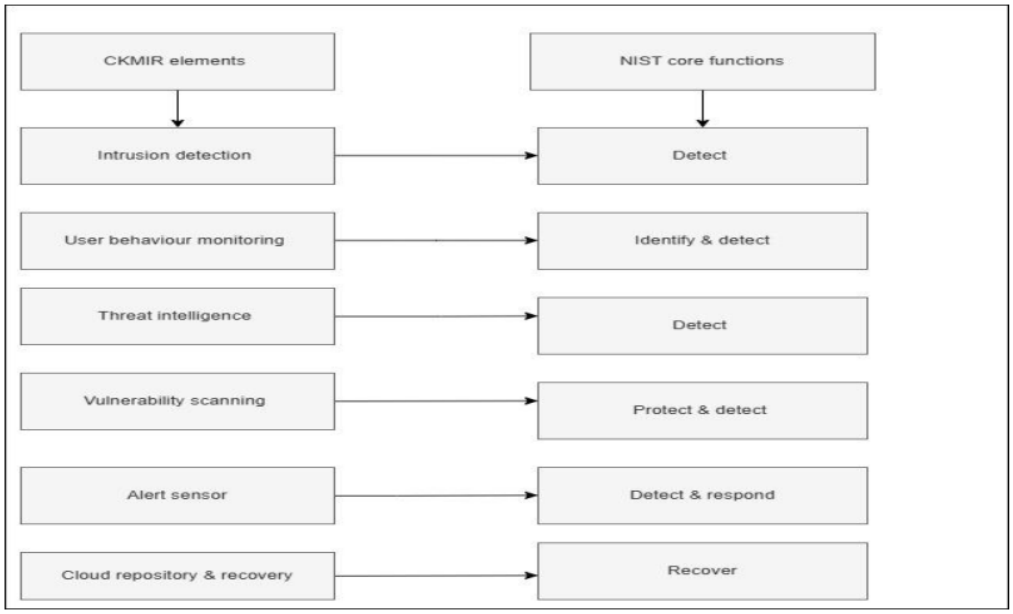


Figure 8. CKMIR element alignment with the NIST model

This article also provides health care organizations with guidelines to follow for the application of the sociotechnical cybersecurity framework, grouping vulnerabilities into three main areas: technology, humans, and processes. It outlines the necessary compliance steps and action plans, and identifies the individuals responsible for addressing each vulnerability in Table S1.

4.2.2 Implementation plan

In this dissertation, I developed an implementation plan to guide validation of the sociotechnical cybersecurity framework (see Fig. S2), Sociotechnical cybersecurity framework implementation steps.

4.2.3 Operationalization and compliance

1. Technological vulnerabilities encompass problems such as insufficient audits, insecure third-party integrations, and intricate system architectures, which are mitigated through secure design, routine evaluations, and access controls.

2. Challenges associated with human factors, including skill deficits, insufficient training, insider threats, and security culture, are addressed through educational programs, the cultivation of a cybersecurity culture, and the implementation of behavioral controls.

3. Process-oriented deficiencies such as inadequate policies, restricted oversight, and the absence of incident response strategies which are mitigated through collaborative alliances, immediate monitoring, and organized recovery procedures.

In conclusion, the article makes a strong case that cybersecurity in health care is a sociotechnical problem that requires more than just technical fixes. The proposed sociotechnical solutions consider how humans, processes, and technologies interact dynamically to provide a comprehensive, actionable approach to fixing cybersecurity holes in health care systems. This contribution is beneficial because most existing frameworks do not adequately address interventions focused on humans and processes. The study suggests that health care organizations should use the proposed model to strengthen their operations, keep patients safe, and comply with data protection rules.

4.3 Cybersecurity in health care: A checklist for security and privacy

This study examined the challenges associated with implementing and using EHRs in health care systems, focusing on operational, security, and privacy issues. EHRs make it easier to get care, keep it going, and make clinical decisions. Because they are digital, they carry significant risks, including data breaches, unauthorized access, and misuse of personal health information. As the IoMT makes it easier for health data to move between connected systems and cloud environments, worries about data security, compliance, and patient trust have grown.

To address these issues, the study uses the PRISMA method for an integrative literature review and searches 57 carefully selected articles from Scopus, Web of Science, and PubMed. The review uses the TOE framework (Technology, Organization, and Environment) to examine health care cybersecurity from the perspectives of operations, management, and ethics. The study finds that five main operational issues lead to health information breaches: poor data security management, failure to comply with legal standards, unsafe data sharing, insufficient privacy measures, failure to enforce confidentiality, and failure to obtain informed patient consent.

TOE-Based Thematic Analysis

Under the TOE framework, the study found five critical operational practices that cause EHR breaches:

1. Technical Operational Factors

- Poor Data Security Management: Weak access control, outdated encryption, and insecure infrastructure.
- Insecure Data Sharing: Unprotected channels, poor governance, and weak interoperability.

2. Operations of the organization

- Privacy and confidentiality gaps: Poor internal policies, staff misconduct, and a lack of audits.
- Training deficiencies: Lack of cybersecurity staff sensitisation and technical preparation.

3. Environmental Operations Factors

- Legal and regulatory noncompliance: GDPR, HIPAA, and HITECH violations, especially during third-party data exchange.
- Poor Patient Consent: Ethical and legal violations in obtaining patients ' informed consent before sharing data.

The author proposes a security and privacy assessment guide checklist, a conceptual tool for health care organizations to assess and improve their ability to protect sensitive health information. This checklist will help protect data, manage consent, encrypt it, ensure policies are in line, and train staff. Its goal is to help businesses comply with rules such as HIPAA, GDPR, and HITECH, and to encourage cooperation among system developers, policymakers, patients, and health care managers.

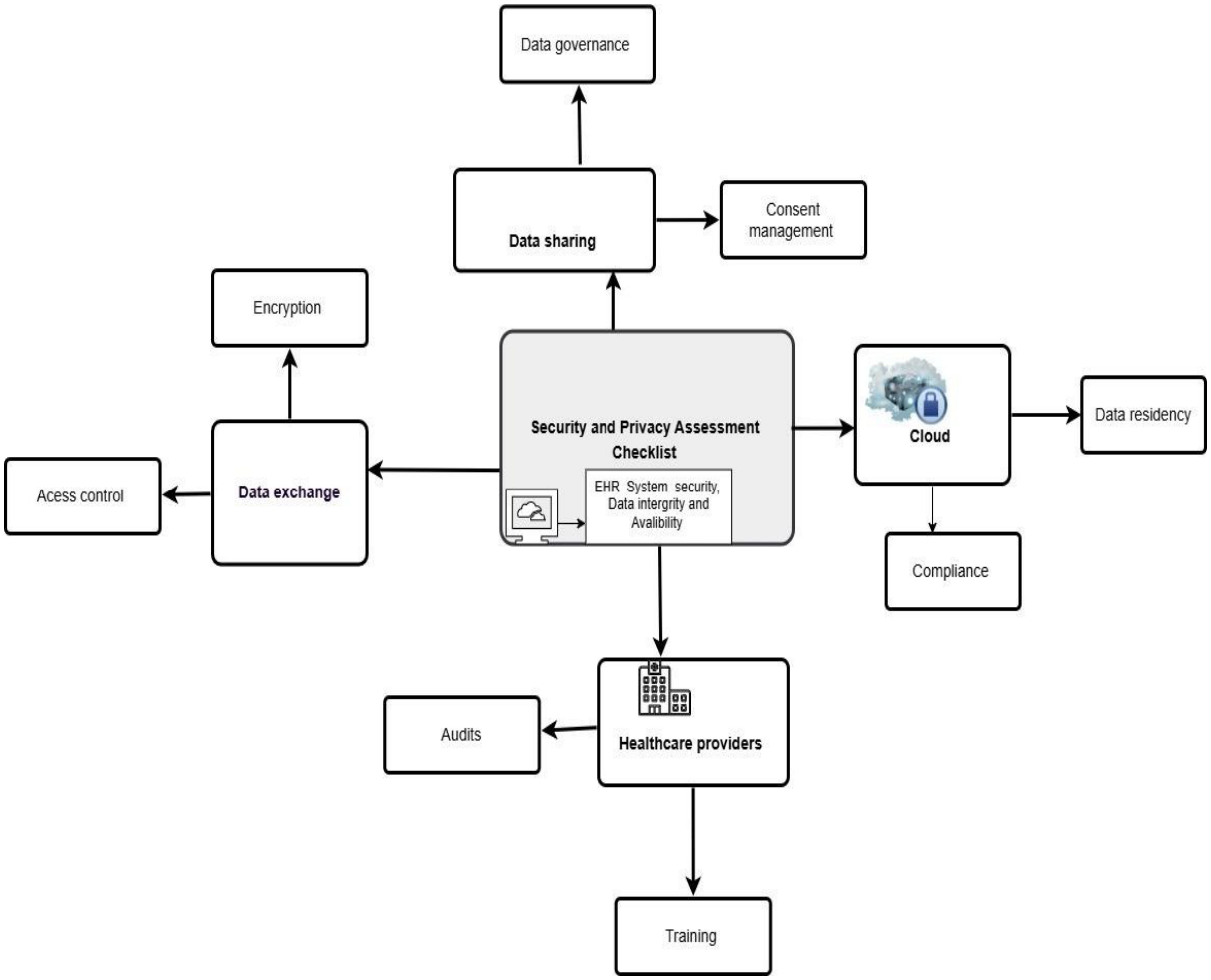


Figure 9. Security and privacy assessment guide checklist

There are four main themes in the EHR security and privacy assessment model: Data Exchange, Data Sharing, Health care Providers, and Cloud. Each one examines a different aspect of protecting electronic health records (EHRs).

1. Data Exchange

This theme focuses on keeping health care data safe during transmission. As health care goes digital, sensitive data is becoming increasingly vulnerable to cyberattacks. The model suggests utilizing encryption standards (such as ISO/IEC 27001:2022) and role-based access control (RBAC) to facilitate this. RBAC controls who can view what data based on their role, such as a physician, nurse, administrator, or patient. This ensures that users can only view information relevant to their role. This model adheres to the "least privilege" principle and incorporates patient consent into access policies. This keeps data private, protects privacy, and builds trust between patients and providers.

2. Data Sharing

The second theme is the importance of organizations that share data having aligned policies. When the receiving organization's rules are less strict than the sender's, security risks often arise. To fix this, the model suggests establishing robust data governance frameworks and effective systems for managing consent. These tools ensure that privacy and data-sharing permissions are protected when data is shared between organizations, mainly when older systems are used.

3. Health Providers

Involving internal stakeholders is crucial to keeping data safe. The model asserts that companies should conduct regular internal security audits, train their staff, and involve employees in policymaking. These steps help protect the organization from cyberattacks and reduce the risk of internal threats arising from human error or technical issues.

4. Cloud

As more health data is stored in the cloud, this theme stresses the need to comply with the law, protect data sovereignty, and adhere to regional legal standards. Organizations need to ensure their cloud practices comply with the law, such as HIPAA in the U.S. and GDPR in the EU. Lack of these compliances could lead to data breaches and legal problems. The model asserts that people should make informed decisions about where to store their data, choose cloud providers with good compliance records, and make rules for how to protect and access data across borders

The study concludes by stressing the importance of privacy-by-design, informed consent protocols, regular audits, and cultural shifts within organizations to protect health data better. It also points out areas where more research is needed in interoperability and cross-border law, and it suggests that these areas be investigated further in the future.

4.4 Sociotechnical cybersecurity response framework for managing incidents in Finnish health care

Cybersecurity challenges are becoming a growing source of concern in health care systems worldwide, including Finland. This is because health services are becoming more digital, and sensitive patient data is very valuable. This theoretical study examines how Finnish health care organizations can better manage cyberattacks by

employing a sociotechnical approach that integrates people, technology, and organizational processes. The author conducted a qualitative exploratory study using open-ended online questionnaires administered to 12 healthcare and IT professionals in Finland. Out of these, 12 participants completed the survey. Qualitative content analysis was used to examine the data, leading to the identification of four main sociotechnical barriers that make it more challenging to respond to incidents effectively.

1. Inadequate Awareness Training - Many health care workers do not get enough training to spot and deal with cybersecurity threats like phishing or malware. Traditional training that fails to account for the current situation does not prepare staff for evolving cyber threats.

2. Incident Alert Detection Delay - Many organizations experience delays in detecting intrusions due to insufficient or outdated systems, staff shortages, and overreliance on manual tools, especially during off-hours.

3. Ineffective Communication - Fragmented communication between IT, clinical, and security teams often leads to delays in reporting and responding to incidents, especially during staff shift transitions.

4. Ambiguous Cybersecurity Policies - Obsolete, ambiguous, or excessively technical cybersecurity policies hinder prompt decision-making and inadequately direct personnel during emergencies

The study proposes a Sociotechnical Cybersecurity Incident Response Framework (see Figure 10) to address these problems. This conceptual model underscores a comprehensive response strategy that incorporates human factors, technology, organizational processes, communication, post-incident recovery, and cyber risk insurance.

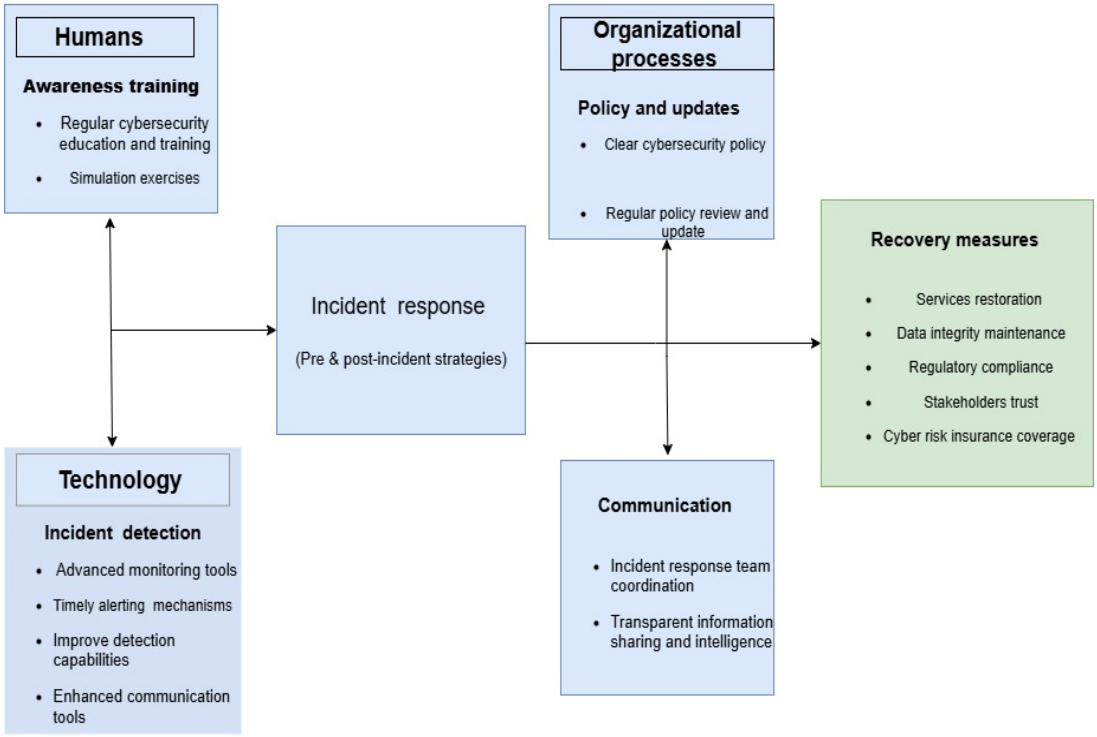


Figure 10. Conceptual sociotechnical cybersecurity incident response framework

- *Human Factors*: Role-specific, simulation-based training to raise awareness of and improve cybersecurity behaviour; fostering a culture of shared responsibility.
- *Technology*: Putting money into automated intrusion detection systems, secure communication tools, and technologies that protect endpoints.
- *Organisational Processes*: establishing policies that are clear, up-to-date, and relevant to the situation; encouraging centralised and coordinated incident response teams.
- *Communication*: Setting up clear and safe ways for departments and stakeholders to share information quickly.
- *Post-Incident Recovery*: Setting up strong data recovery systems, audit trails, following GDPR and Finnish data laws, and building trust through openness.
- *Cyber Risk Insurance*: Getting patients and staff to get insurance as part of a proactive plan for dealing with incidents after they happen.

This study advances sociotechnical systems theory by demonstrating how discrepancies among human, technical, and policy components shape incident response outcomes. It promotes a transition from solely technical remedies to holistic sociotechnical approaches in cybersecurity management. Health care leaders must prioritise sociotechnical integration by harmonising training, tools, and policies. The proposed framework serves as a diagnostic and planning tool to enhance incident response readiness and resilience. The authors propose investigating the role of AI and automation in real-time threat detection and conducting comparative analyses across Nordic countries to validate and enhance the framework.

5 DISCUSSION AND CONCLUSION

5.1 Article 1. Vulnerabilities and sociotechnical cybersecurity solutions

Cybersecurity research in health care has focused on technical issues like firewalls, encryption, and system vulnerabilities. It has often ignored the social and organizational factors that lead to system breaches (Coventry & Branley, 2018). For example, prior research stressed the importance of resilience and behavioral aspects, but it did not give a complete framework that brought together human behavior, processes, and technology (Coventry & Branley, 2018) . Also, it provided narrative insights into the intersection of technology and processes, but lacked a structured theoretical synthesis. On the other hand, this study explored and identified the weaknesses in health care systems through the application of a sociotechnical systems theory. By combining social (human error and training gaps) and technical (IoMT vulnerabilities and outdated infrastructure) aspects of cybersecurity, we can better understand STS theory. This theoretical approach goes beyond earlier technocentric models and showed that cyber risk in health care settings is complex and multifaceted.

Many studies, including those by (Jalali, Russell, et al., 2019) and (He et al., 2021), found that human error is a significant cause of cyber breaches, especially when people use social engineering tactics such as phishing. However, the proposed interventions in those studies were limited and often consisted only of calls for awareness or training, without being part of a larger systemic framework. This study goes a long way beyond that by linking human-related vulnerabilities to specific intervention areas, like gamified training (Khando et al., 2021), situational awareness models (Walker T, 2017), and digital literacy programs (Holst et al., 2020). It also explained that human error is not just an individual failure but a social vulnerability shaped by factors such as an organization's culture, a lack of formal education, and poor cybersecurity protocols. This nuanced point of view showed how important it is to use sociotechnical tools, such as behavioral testing, across departments, and to make cybersecurity part of the culture at all levels of the organization.

(Kruse et al., 2017) and other studies have shown that health care organizations spend less than 5% of their IT budget on cybersecurity, leaving their digital infrastructure weak. There has not been much research into how this lack of investment affects other areas of vulnerability or how social and organizational factors affect investment decisions. This study bridges the gap by showing that lack of investment is a cross-cutting sociotechnical vulnerability that worsens other

problems, such as legacy systems that will not go away, poor training, and the inability to detect threats. It also suggests that public-private partnerships and changes to government policy (Baranchuk et al., 2018; Chua, 2021) can help improve cybersecurity skills. These insights offer decision-makers valuable insights and underscore the importance of ensuring that budget allocations align with overall security strategies.

The Cybersecurity risk literature has often discussed legacy infrastructure. For instance, Sweeney E., (2017) and (Fu & Blum, 2013) pointed out that hospitals still use old systems like Windows XP, which makes them very vulnerable. These studies identified technical risks but did not investigate organizational inertia, policy limitations, or purchasing decisions that kept these systems in place. This study is new because it reclassifies legacy systems as a sociotechnical vulnerability, driven by both technical obsolescence and structural resistance to change. It further supports this argument by suggesting policy-based solutions, such as adhering to GDPR and HIPAA rules, and by encouraging the gradual removal of systems no longer supported through incentive-based procurement reforms.

The IoMT has become more prevalent due to advances in healthcare technology. Researchers like (Karambelas, 2020) and (C. J. Dameff et al., 2019) have talked about the risks of these devices, such as how easy it is for hackers to get into them over the network. However, few studies have examined the fact that they were not designed with security in mind when they were developed and added to systems. This study addresses that problem by examining how digitalization without proper cybersecurity planning makes systems more vulnerable. It suggests several technical and sociotechnical responses, such as:

- Adding security needs to the criteria for buying medical technologies (Lechner, 2018),
- Using blockchain to verify devices and keep data safe (Abouelmehdi et al., 2018),
- Making security maintenance contracts required for updates and post-market surveillance.

5.2 Article 2. Sociotechnical framework for securing health care

The swift shift to digital technology in health care systems has brought incredible benefits and new security spaces that have never been seen before. Even though

various frameworks have been developed to address cybersecurity threats, there remains a significant gap in how these weaknesses are addressed from a sociotechnical systems perspective. In the past, the health care cybersecurity literature has mainly focused on either technical solution (such as firewalls and anti-malware software) or social solutions (such as employee training). Many authors have discussed frameworks such as NIST, ISO/IEC, COBIT, and IT-CMF. However, these frameworks addressed only some sociotechnical aspects and are mostly general, not specific to health care. (Malatji et al., 2020) and (Zimmermann & Renaud, 2019) are two examples of studies that have stressed the need for a joint optimization approach that combines technological and social factors. However, most of the proposed frameworks were not made with the unique complexity of health care systems in mind. In the same way, scholars like (Kaberuka & Johnson, 2020) suggested changing STPA-SEC to better fit the health care systems of developing countries, but they did not have a clear idea of how to use it in practice. Existing studies, like those by (Perrotin et al., 2022; Zimmermann & Renaud, 2019) and (Malatji et al., 2020), also recognize the need to optimize both technology and human systems together, but they do not adapt their frameworks to the specific and complicated weaknesses of health care systems. These include insider threats, systems that are rigorously to use, third-party plug-ins, policies that are not strong enough, and cybersecurity budgets that are not big enough. These are all well-known problems, but they are rarely put together into a working framework that shows how technology and society are complex.

The Cybersecurity Knowledge Management and Intelligence Response (CKMIR) model is the technical and operational heart of the proposed sociotechnical cybersecurity framework. It consists of six integrated features, namely: intrusion detection, user behavior monitoring, threat intelligence, vulnerability scanning, alert sensors, and cloud-based data recovery. These features interact together to enable a proactive and real-time automated defense regarding vulnerabilities and intelligent response in an event of a cyber threats and attacks in health care systems. CKMIR differs from previous models by combining behavioral monitoring with intelligence-driven automation. Previous models mainly focused on either technical tools or human factors. It recognizes that user behavior, technical settings, and outside threats are constantly changing and offers a model that is flexible, adaptable, and aware of its surroundings. This addresses a problem noted in the literature: existing frameworks either do not respond in real time or do not adequately incorporate human-system interaction (Hijji & Alam, 2021; Zimmermann & Renaud, 2019).

Another value of the CKMIR in the framework of this dissertation is that it categorizes vulnerabilities into technological, human, and process-related areas, thereby advancing understanding of how cybersecurity risks emerge within health care

systems. Furthermore, the taxonomy table in article 2 showed that internal threats in health care systems stem not only from health care professionals but also from IT staff and organizational practices, underscoring the sociotechnical interdependence of these factors of vulnerability.

5.3 Article 3. Security and privacy checklist for health service operations

This study adds to the growing body of research on health care cybersecurity by filling in important gaps in operational, managerial, and ethical areas that have not been well studied before. While previous research has shown that cybersecurity threats are common in EHRs systems, many of them have mostly looked at technological solutions like encryption, blockchain, or machine learning (Al-Issa et al., 2019; Zhu et al., 2020). These solutions have not been fully integrated into the daily operations of health care institutions. This study, on the other hand, takes a more comprehensive approach that includes not only technical but also managerial, legal, and ethical aspects. This moves the conversation from abstract theory to real-world application.

One of the most significant gaps in earlier research was its failure to explain clearly how operational practices can lead to privacy and security breaches. This study fills that gap by identifying five key reasons why information breaches occur in EHR systems. These include poor data security management, failure to follow rules, unsafe data sharing, and failure to obtain informed consent from patients (Costa Lima et al., 2023; Paul et al., 2023) .

Also, this study is unique because it explains the legal and moral issues that arise when people grant their consent, trust, and privacy in data governance. While works like (Coiera & Clarke, 2004) and (Kaplan, 2020) brought up important issues about patient consent and autonomy, they did not give enough information on how to incorporate these issues into the way the system works. This study facilitates consent models and integration strategies that enable safe, legal, and ethical data sharing within and beyond health care networks.

The study provides health care professionals with a way to assess and improve their cybersecurity posture and provides researchers with a framework for future empirical studies. This study fills an important gap between technical, managerial, and ethical fields that has long made cybersecurity solutions in health care less effective in the real world.

5.4 Article 4. Sociotechnical cyber incidents response framework

Traditional approaches to cybersecurity have focused solely on technical barriers. Drawing on sociotechnical systems theory, the study demonstrates how health care professionals, information systems, and institutional policies interdependently influence one another in complex ways. The empirical results support the belief that human and organisational factors, like policy clarity, communication practices, and awareness training, are crucial for the overall success of cybersecurity incident management (Haukilehto, 2024; Malatji et al., 2019, 2020).

This study provides a theoretical understanding of cybersecurity in health care by building on the sociotechnical systems perspective(Haukilehto, 2024; Looi et al., 2025). This study demonstrates that a comprehensive view, encompassing human behavior, organisational processes, and technological tools, is necessary for effective incident response.

The study fills a significant gap in the literature by not only addressing what makes a good cybersecurity response but also how different sociotechnical factors interact and affect outcomes (Fig. 10). This study adds to the body of work questioning the overuse of technical solutions and strengthens the case for integrated approaches in cybersecurity research and practice. It also applies sociotechnical systems theory to the high-risk, data-sensitive field of health care, where cyber incidents can have an enormous effect on patient safety, trust, and public health outcomes (Pranggono & Arabo, 2021; Tikanmäki & Ruoslahti, 2024).

5.5 Theoretical contributions

This dissertation makes multiple theoretical contributions, including the development of a sociotechnical solution to protect patient health information, medical devices, and the cyber-critical infrastructure of health care organizations from cyberattacks and threats.

The main contribution of this dissertation is the development of a sociotechnical cybersecurity framework for health care systems (Fig. 7). The framework identifies and prevents vulnerabilities and responds to threats and cyberattacks. The proposed framework provides the foundations for understanding the connections and integrations among the factors that contribute to vulnerabilities to cyberattacks and threats from a sociotechnical perspective. Another contribution is the provision of the thematic classification of technology, humans, and processes related factors of

vulnerabilities to cyberattacks in health care systems. Also, it provided an in-depth analytical synthesis of the taxonomy factors of vulnerabilities to cyberattacks.

This dissertation contributes to the theory by categorizing operational practices that impact EHR security and privacy within the robust TOE framework. Besides, a privacy and security checklist model for health care was developed to ensure that data security, privacy, trust, and compliance are built into the operations of EHR systems.

Another contribution is the development of a sociotechnical cybersecurity incident response framework for effective incident response management and guidance within a Finnish health care organization. The proposed framework functions as a diagnostic tool or blueprint for managing and enhancing incident response capabilities, protecting patient data, and ensuring business continuity within Finnish health care organizations.

5.6 Managerial contributions

This dissertation found that health care cybersecurity is underfunded, with IT budgets often covering only 5% of costs (Kruse et al., 2016, 2017). This is a clear call for managers to reallocate funds to strengthen cybersecurity infrastructure. This includes spending money not just on technical solutions such as firewalls, encryption, and secure cloud storage, but also on training, improving organizational processes, and collaborating with schools and cybersecurity experts. The findings highlight human error as a persistent cause of cyber breaches, often due to phishing, employee negligence, and lack of awareness. As a result, health care managers should create a culture of cybersecurity awareness in their organizations. This can be achieved by making cybersecurity training mandatory and regular, utilizing games and phishing simulations to reinforce skills, and implementing digital literacy programs and behavioral assessments to identify and assist individuals at risk. The dissertation showed that sharing intelligence and working together are still not used enough. Health care managers should foster collaborative relationships with government agencies, cybersecurity centers, and peer institutions to share threat intelligence and best practices. Health care managers should use evidence-based information and guidance to make cybersecurity a top priority for the entire organization.

Health care managers should leverage cybersecurity strengths by implementing risk assessments and an incident response plan that addresses current and emerging threats and cyberattacks. Health care managers should adopt compliance standards (Table S1) for applying the sociotechnical cybersecurity framework as a guide to maintain cybersecurity hygiene in health care systems. Health care managers should ensure the medical device security lifecycle is integrated into confidentiality,

integrity, and availability practices as a quality control measure (Szczepaniuk & Szczepaniuk, 2023). The dissertation will aid health care managers in conceiving of cybersecurity in health care from a sociotechnical perspective and in the joint optimization of technology, humans, and processes (Malatji et al., 2019).

This dissertation provides health care managers with important information and useful tools to help improve privacy and security when using and implementing EHR systems. Health care managers should create an operational assessment checklist system to find, evaluate, and reduce privacy and security risks when sharing and managing sensitive patient health information. Health care managers should implement the checklist model to ensure that their daily operations comply with laws such as GDPR, HIPAA, and HITECH. The dissertation also underscores the importance of creating a culture of security in the workplace. Also, the checklist provides health care organizations with a proactive, legally sound approach to addressing cybersecurity threats.

Health care managers should prioritize aligning sociotechnical elements within cybersecurity incident response plans. Health care managers should procure advanced automated tools, such as endpoint detection and response (EDR), which are crucial for significantly enhancing organizational resilience and ensuring rapid incident response. Managers and development stakeholders in health care should establish explicit guidelines and responsibilities for employees, eliminating ambiguous training methods, policies, and guidelines that may lead to confusion.

5.7 Limitations and future research direction

As is known in any research, limitations do exist; thus, this dissertation's limitations include difficulties in data collection due to the sensitivity of health care information and privacy concerns. Review papers included only papers published in English.

*R*esearch should investigate how cross-border data exchange is governed, especially under rules such as GDPR, and examine how international policies can make cybersecurity strategies work better together. Studies could also investigate patient-centered cybersecurity models that better integrate informed consent, user experience, and the ethical issues that arise when using digital health data. Researchers should also investigate new health technologies like AI-driven diagnostics, wearables, IoMT devices.

Further research should empirically validate the proposed framework for accuracy, feasibility, and effectiveness in health care organizations. Additional studies are also

needed to explore the cultural and organizational factors that influence cybersecurity behavior in health care.

5.8 Conclusions

This dissertation concludes that ensuring robust cybersecurity in health care necessitates more than technological solutions; it requires a comprehensive sociotechnical approach that thoroughly addresses the interactions among technology, humans, and processes. All reviewed studies indicate that human factors, including insufficient awareness, inadequate training, insider threats, and noncompliance, substantially increase the risk of cyber incidents. Concurrently, technological constraints such as outdated systems, inadequate encryption, and subpar incident response protocols further compromise system security. Organizational factors, such as ambiguous policies, ineffective communication, and insufficient investment, further exacerbate operational vulnerabilities.

This research recommends implementing sociotechnical cybersecurity frameworks and incident response models tailored for dynamic, complex health care systems to address these challenges. These models prioritise ongoing training, explicit cybersecurity protocols, efficient communication, immediate detection, and synchronised response initiatives. The suggested checklist and frameworks serve as diagnostic tools for identifying vulnerabilities and as pragmatic guides for risk reduction and regulatory compliance. Future resilience requires a proactive security culture that integrates patient-centered ethics, cross-sector collaboration, blockchain innovation, and AI-driven threat detection tools.

Ultimately, protecting health care data and essential infrastructure is crucial for sustaining trust, guaranteeing continuous care, and advancing digital health transformation. This dissertation findings advance both theoretical and practical domains of health care cybersecurity, and information security by establishing a framework for secure, resilient, and ethically accountable health care systems in a progressively digital environment.

References

Abbou, B., Kessel, B., Ben Natan, M., Gabbay-Benziv, R., Dahan Shriki, D., Ophir, A., Goldschmid, N., Klein, A., Roguin, A., & Dudkiewicz, M. (2024). When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. *Frontiers in Digital Health*, *6*. https://doi.org/10.3389/fdgth.2024.1321485

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data*, *5*(1). https://doi.org/10.1186/s40537-017-0110-7

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Ackerman, L. (2013). Mobile Health and Fitness Applications and Information Privacy. Report to California Consumer Protection Foundation. *Privacy Rights Clearinghouse*.

Åhlfeldt, R. M., Backlund, P., Wangler, B., & Söderström, E. (2005). Security Issues in Health Care Process Integration? a Research-in-Progress Report. In EMOI-INTEROP.

Albalawi, T., Ghazinour, K., & Melton, A. (2017). Security mental model: Cognitive map approach. *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, 74–79.

Aldosari, B. (2025). Cybersecurity in Health care: New Threat to Patient Safety. *Cureus*, *17*(5), e83614.

Alhammad, A., Yusof, M. M., & Jambari, D. I. (2022). A Review of Cyber Threats to Medical Devices Integration with Electronic Medical Records. *International Conference on Cyber Resilience, ICCR 2022*. https://doi.org/10.1109/ICCR56254.2022.9995984

Ali, K. A., & Alyounis, S. (2021). CyberSecurity in Health care Industry. *2021 International Conference on Information Technology (ICIT)*, 695–701. https://api.semanticscholar.org/CorpusID:236482874

Ali, M. B., Wood-Harper, T., Al-Qahtani, A. S., & Albakri, A. M. A. (2020). Risk assessment framework of mHealth system vulnerabilities: A multilayer analysis of the patient hub. *Communications and Network*, *12*(2), 41–60.

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). EHealth Cloud Security Challenges: A Survey. In *Journal of Health care Engineering* (Vol. 2019). https://doi.org/10.1155/2019/7516035

Al-Qarni, A. (2023). Cybersecurity in Health care: A Review of Recent Attacks and Mitigation Strategies. In *IJACSA) International Journal of Advanced Computer Science and Applications* (Vol. 14, Issue 5). www.ijacsa.thesai.org

Altman, R. B. (1997). Informatics in the care of patients: Ten notable challenges. *Western Journal of Medicine*, *166*(2).

Anastasopoulou, K., Mari, P., Magkanaraki, A., Spanakis, E. G., Merialdo, M., Sakkalis, V., & Magalini, S. (2020). Public and private healthcare organisations: A socio-Technical model for identifying cybersecurity aspects. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3428502.3428525

Anti, E., & Vartiainen, T. (2024). *Explanations of insider deviant behavior in information security: a systematic literature review*.

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. In *Management Decision* (Vol. 35, Issue 6). https://doi.org/10.1108/00251749710173823

Arafa, A., Sheerah, H. A., & Alsalamah, S. (2023). Emerging Digital Technologies in Health care with a Spotlight on Cybersecurity: A Narrative Review. In *Information (Switzerland)* (Vol. 14, Issue 12). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/info14120640

Arain, M. A., Tarraf, R., & Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *Journal of Multidisciplinary Health care*, 73–81.

Argaw, S. T., Bempong, N. E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. In *BMC Medical Informatics and Decision Making* (Vol. 19, Issue 1). https://doi.org/10.1186/s12911-018-0724-5

Arora, S., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mHealth) research. *Alcohol Research: Current Reviews*, *36*(1).

Aslan, Ö., & colleagues. (2023). A comprehensive review of cyber security vulnerabilities in digital systems. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333

Athinaiou, M. (2022). *Model-based management of cyber resiliency for healthcare systems* [Doctoral dissertation]. University of Brighton.

Atkinson, C., Eldabi, T., Paul, R. J., & Pouloudi, A. (2001). Investigating integrated socio-technical approaches to health informatics. *Proceedings of the Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2001.926578

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kutyifa, V., Upadhyay, G., Fisher, J. D., & Lakkireddy, D. R. (2018). Cybersecurity for Cardiac Implantable Electronic Devices: What Should You Know? In *Journal of the American College of Cardiology* (Vol. 71, Issue 11). https://doi.org/10.1016/j.jacc.2018.01.023

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers*, *23*(1). https://doi.org/10.1016/j.intcom.2010.07.003

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *MIS Quarterly*, 369–386.

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming Health care Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. In *Journal of Medical Systems* (Vol. 44, Issue 5). https://doi.org/10.1007/s10916-019-1507-y

Booher, H. R., & Minninger, J. (2003). Human Systems Integration in Army Systems Acquisition. In *Handbook of Human Systems Integration* (pp. 663–698). https://doi.org/https://doi.org/10.1002/0471721174.ch18

Branley-Bell, D., Coventry, L., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff. *Annals of Disaster Risk Sciences*, *3*(1). https://doi.org/10.51381/adrs.v3i1.51

Budzak, D. (2016). Information security–The people issue. *Business Information Review*, *33*(2), 85–89.

Burnell, G., & Morgan, G. (1979). *Sociological paradigms and organisational analysis, elements of the sociology of corporate life*. London: Heinemann.

Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Commun. ACM*, *59*(10), 66–72. https://doi.org/10.1145/2890488

Carayon, P. (2006). Human factors of complex sociotechnical systems. *Applied Ergonomics*, *37*(4 SPEC. ISS.). https://doi.org/10.1016/j.apergo.2006.04.011

Carayon, P., Hancock, P., Leveson, N., Noy, I., Sznelwar, L., & van Hootegem, G. (2015). Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework. *Ergonomics*, *58*(4). https://doi.org/10.1080/00140139.2015.1015623

Carson, D. J., Perry, C., & Gilmore, A. (2001). *Qualitative marketing research*.

Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. In *Journal of Clinical Monitoring and Computing* (Vol. 37, Issue 5). https://doi.org/10.1007/s10877-023-01013-5

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2018). Security-by-design in multi-cloud applications: An optimization approach. *Information Sciences*, *454–455*. https://doi.org/10.1016/j.ins.2018.04.081

Chiaradonna, S., Jevtić, P., & Lanchier, N. (2023). Framework for cyber risk loss distribution of hospital infrastructure: Bond percolation on mixed random graphs approach. *Risk Analysis*, *43*(12), 2450–2485.

Chinthapalli, K. (2017). The hackers holding hospitals to ransom. *BMJ*, *357*.

Choi, S. J., Chen, M., & Tan, X. (2023). Assessing the impact of health information exchange on hospital data breach risk. *International Journal of Medical Informatics*, *177*. https://doi.org/10.1016/j.ijmedinf.2023.105149

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, *44*(6), 752–767.

Choudhary, T., & Jagre, P. (2024). Ransomware: Hollywood Presbyterian Medical Center. In *Information Technology Security and Risk Management* (pp. 170–173). CRC Press.

Chua, J. A. (2021). Cybersecurity in the healthcare industry - A collaborative approach. *American Association for Physician Leadership*, *8*(1).

Clarke, Matthew, & Martin, Kevin. (2023). Managing cybersecurity risk in healthcare settings. *Health care Management Forum*, *37*(1), 17–20. https://doi.org/10.1177/08404704231195804

Coiera, E., & Clarke, R. (2004). e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment. *Journal of the American Medical Informatics Association*, *11*(2). https://doi.org/10.1197/jamia.M1480

Costa Lima, V., Alves, D., Andrade Bernardi, F., & Charters Lopes Rijo, R. P. (2023). Security approaches for electronic health data handling through the Semantic Web: A scoping review. *Semantic Web*, *14*(4). https://doi.org/10.3233/SW-223088

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. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12210 LNCS*. https://doi.org/10.1007/978-3-030-50309-3_8

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. In *Maturitas* (Vol. 113). https://doi.org/10.1016/j.maturitas.2018.04.008

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Cybersecurity Insider. (2024). *Insider Threat Report 2024*.

Dameff, C. J., Selzer, J. A., Fisher, J., Killeen, J. P., & Tully, J. L. (2019). Clinical Cybersecurity Training Through Novel High-Fidelity Simulations. *Journal of Emergency Medicine*, *56*(2). https://doi.org/10.1016/j.jemermed.2018.10.029

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

Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics*, *45*(2 Part A). https://doi.org/10.1016/j.apergo.2013.02.009

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review*, *35*(2), 60–67. https://doi.org/10.1177/0266382118773624

DeFord, D. (2022). Sustainable Digital Health Demands Cybersecurity Transformation. *Frontiers of Health Services Management*, *38*(3), 31–38. https://doi.org/10.1097/HAP.0000000000000137

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*. sage.

Determann, L. (2019). Healthy data protection. Mich. Tech. L. Rev., 26, 229. DOI https://doi.org/10.36645/mtlr.26.2.healthy

Dias, F. M., Martens, M. L., Monken, S. F. de P., Silva, L. F. da, & Santibanez-Gonzalez, E. D. R. (2021). Risk management focusing on the best practices of data security systems for healthcare. *International Journal of Innovation*, *9*(1). https://doi.org/10.5585/iji.v9i1.18246

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2023). An Empirical Study of Automation in Software Security Patch Management. *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*. https://doi.org/10.1145/3551349.3556969

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences (Switzerland)*, *11*(10). https://doi.org/10.3390/app11104580

Emery, F. (1982). New Perspectives on the world of work: Sociotechnical Foundations for a New Social Order? *Human Relations*, *35*(12). https://doi.org/10.1177/001872678203501203

Emery, F. E., & Trist, E. L. (1960). Socio-technical systems. *Management Science, Models and Techniques*, *2*, 83–97.

Ewoh, P., & Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health care Systems: Systematic Review. In *Journal of Medical Internet Research* (Vol. 26). JMIR Publications Inc. https://doi.org/10.2196/46904

Federal Bureau of Investigation. (2023). *FBI Internet Crime Report: 2022*.

Feeley, A., Lee, M., Crowley, M., Feeley, I., Roopnarinesingh, R., Geraghty, S., Cosgrave, B., Sheehan, E., & Merghani, K. (2022). Under viral attack: An orthopaedic response to

challenges faced by regional referral centres during a national cyber-attack. *Surgeon*, *20*(5), 334–338. https://doi.org/10.1016/j.surge.2021.09.007

Fernando, J., & Dawson, L. (2014). The natural hospital environment: A socio-technical-material perspective. *International Journal of Medical Informatics*, *83*(2). https://doi.org/10.1016/j.ijmedinf.2013.10.008

Filipec, O., & Plášilb, D. (2021). THE CYBERSECURITY OF HEALTHCARE The Case of the Benešov Hospital Hit by Ryuk Ransomware, and Lessons Learned. *Obrana a Strategie*, *21*(1), 27–51. https://doi.org/10.3849/1802-7199.21.2021.01.027-052

Fu, K., & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of the ACM*, *56*(10). https://doi.org/10.1145/2508701

Gabriel, M. H., Noblin, A., Rutherford, A., Walden, A., & Cortelyou-Ward, K. (2018). Data breach locations, types, and associated characteristics among US hospitals. *Am J Manag Care*, *24*(2), 78–84.

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, *121*. https://doi.org/10.1016/j.technovation.2022.102583

Ghanbari, Hadi, & Koskinen, Kari. (2024). When data breach hits a psychotherapy clinic: The Vastaamo case. *Journal of Information Technology Teaching Cases*, 20438869241258236. https://doi.org/10.1177/20438869241258235

Giansanti, D. (2021). Cybersecurity and the digital-health: The challenge of this millennium. In *Health care (Switzerland)* (Vol. 9, Issue 1). https://doi.org/10.3390/healthcare9010062

Gordon, W. J., Wright, A., Aiyagari, R., Corbo, L., Glynn, R. J., Kadakia, J., Kufahl, J., Mazzone, C., Noga, J., Parkulo, M., Sanford, B., Scheib, P., & Landman, A. B. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health care Institutions. *JAMA Network Open*, *2*(3). https://doi.org/10.1001/jamanetworkopen.2019.0393

Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association*, *26*(6). https://doi.org/10.1093/jamia/ocz005

Gourisetti, S. N. G., Mylrea, M., & Patangia, H. (2020). Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis. *Future Generation Computer Systems*, *105*, 410–431.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of Qualitative Research*, *2*(163–194), 105.

Gupta, B. B., Gaurav, A., & Kumar Panigrahi, P. (2023). Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *Journal of Business Research*, *162*. https://doi.org/10.1016/j.jbusres.2023.113859

Harries, D., & Yellowlees, P. M. (2013). Cyberterrorism: Is the US healthcare system safe? *Telemedicine and E-Health*, *19*(1), 61–66.

Harrison, A. S., Sullivan, P., Kubli, A., Wilson, K. M., Taylor, A., DeGregorio, N., Riggs, J., Werner-Wasik, M., Dicker, A., & Vinogradskiy, Y. (2022). How to Respond to a Ransomware Attack? One Radiation Oncology Department's Response to a Cyber-Attack on Their Record and Verify System. *Practical Radiation Oncology*, *12*(2). https://doi.org/10.1016/j.prro.2021.09.011

Haukilehto, T. (2024). *Cybersecurity management in healthcare: Policies, awareness and incident reporting*. https://urn.fi/URN:ISBN:978-952-395-140-2

Health care Information and Management Systems Society. (2018). *2018 HIMSS cybersecurity survey: Final report*.

Heeks, R. (2006). Health information systems: Failure, success and improvisation. *International Journal of Medical Informatics*, *75*(2). https://doi.org/10.1016/j.ijmedinf.2005.07.024

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. *Journal of Medical Internet Research*, *23*(4). https://doi.org/10.2196/21747

He, Y., Maglaras, L., Aliyu, A., & Luo, C. (2022a). Health care Security Incident Response Strategy-A Proactive Incident Response (IR) Procedure. *Security and Communication Networks*, *2022*(1), 2775249.

He, Y., Maglaras, L., Aliyu, A., & Luo, C. (2022b). Health care Security Incident Response Strategy - A Proactive Incident Response (IR) Procedure. *Security and Communication Networks*, *2022*. https://doi.org/10.1155/2022/2775249

Hijji, M., & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access*, *9*, 7152–7169. https://doi.org/10.1109/ACCESS.2020.3048839

HIMSS. (2019). *Cybersecurity in Health care*. https://www.himss.org/resources/cybersecurity-healthcare

HIPAA Journal. (2025, July 15). *Health care Data Breach Statistics*. HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Hippa J. (2023, January 1). What are the penalties for HIPAA violations. *Hippa Journal*. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

Hippa Journal. (2022). Health care Data Breach Statistics. *Hippa Journal* . https://www.hipaajournal.com/healthcare-data-breach-statistics/

Holst, C., Sukums, F., Radovanovic, D., Ngowi, B., Noll, J., & Winkler, A. S. (2020). Sub-Saharan Africa—the new breeding ground for global digital health. In *The Lancet Digital Health* (Vol. 2, Issue 4). https://doi.org/10.1016/S2589-7500(20)30027-3

Ireland, C. A., Ireland, J. L., Jones, N. S., Chu, S., & Lewis, M. (2019). Predicting security incidents in high secure male psychiatric care. *International Journal of Law and Psychiatry*, *64*. https://doi.org/10.1016/j.ijlp.2019.01.004

International Telecommunications Union (ITU). ITU-TX.1205:series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008.

ISO/IEC. ISO/IEC 27002: code of practice for information security management 2005.

ISO/IEC. ISO/IEC 27032:2012(E) information technology e security techniques e guidelines for cybersecurity. Geneva, Switzerland: ISO/IEC; 2012.

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. In *Journal of Medical Internet Research* (Vol. 20, Issue 5). https://doi.org/10.2196/10059

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: Bibliometric analysis of the literature. In *Journal of Medical Internet Research* (Vol. 21, Issue 2). https://doi.org/10.2196/12644

Jalali, M. S., Russell, B., Razak, S., & Gordon, W. J. (2019). EARS to cyber incidents in health care. *Journal of the American Medical Informatics Association*, *26*(1). https://doi.org/10.1093/jamia/ocy148

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems*, *28*(1). https://doi.org/10.1016/j.jsis.2018.09.003

Jalkanen, J. (2019). *Is human the weakest link in information security?: systematic literature review*.

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. In *Cyber Security and Applications* (Vol. 1). https://doi.org/10.1016/j.csa.2023.100016

Joshi, N., & Kadhiwala, B. (2017). Big data security and privacy issues-A survey. *2017 Innovations in Power and Advanced Computing Technologies, i-PACT 2017*, *2017-January*. https://doi.org/10.1109/IPACT.2017.8245064

Kaberuka, J., & Johnson, C. (2020). Adapting STPA-sec for Socio-technical Cyber Security Challenges in Emerging Nations: A Case Study in Risk Management for Rwandan Health care. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2020*. https://doi.org/10.1109/CyberSecurity49315.2020.9138863

Kaberuka, J., & Johnson, C. (2023). Case Studies in the Socio-technical Analysis of Cybersecurity Incidents: Comparing Attacks on the UK NHS and Irish Health care Systems. *Springer Proceedings in Complexity*. https://doi.org/10.1007/978-981-19-6414-5_21

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital Health care - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations. *IEEE Access*, *10*, 12345–12364. https://doi.org/10.1109/ACCESS.2022.3145372

Kaplan, B. (2020). REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19. *International Journal of Medical Informatics*, *143*, 104239. https://doi.org/10.1016/J.IJMEDINF.2020.104239

Karambelas, C. (2020). *Intensive Care*.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, *106*. https://doi.org/10.1016/j.cose.2021.102267

Kioskli, K., Fotis, T., & Mouratidis, H. (2021). The landscape of cybersecurity vulnerabilities and challenges in healthcare: Security standards and paradigm shift recommendations. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3465481.3470033

Kissel, R. (2013). Glossary of Key Information Security Terms Glossary of Key Information Security Terms. *The National Institute of Standards and Technology*, *NISTIR 729*(Revision 2).

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. In *Technology and Health care* (Vol. 25, Issue 1). https://doi.org/10.3233/THC-161263

Kruse, C. S., Kristof, C., Jones, B., Mitchell, E., & Martinez, A. (2016). Barriers to Electronic Health Record Adoption: a Systematic Literature Review. *Journal of Medical Systems*, *40*(12), 252. https://doi.org/10.1007/s10916-016-0628-9

Lechner, N. H. (2018). *Developing a Compliant Cybersecurity Process for Medical Devices*.

Lehto, M., Neittaanmäki, P., Pöyhönen, J., & Hummelholm, A. (2022). Cyber security in healthcare systems. In *Cyber Security: Critical Infrastructure Protection* (pp. 183–215). Springer.

Le, N. T., & Hoang, D. B. (2017). Can maturity models support cyber security? *2016 IEEE 35th International Performance Computing and Communications Conference, IPCCC 2016*. https://doi.org/10.1109/PCCC.2016.7820663

Loi, M., Christen, M., Kleine, N., & Weber, K. (2019). Cybersecurity in health – disentangling value tensions. *Journal of Information, Communication and Ethics in Society*, *17*(2). https://doi.org/10.1108/JICES-12-2018-0095

Looi, J. C. L., Allison, S., Bastiampillai, T., Maguire, P. A., Kisely, S., Reutens, S., & Looi, R. C. H. (2025). Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers. *Australasian Psychiatry*, *33*(1), 106–110. https://doi.org/10.1177/10398562241291340

Looi, J. C. L., Looi, R. C. H., Maguire, P. A., Kisely, S., Bastiampillai, T., & Allison, S. (2024). Psychiatric electronic health records in the era of data breaches – What are the ramifications for patients, psychiatrists and healthcare systems? *Australasian Psychiatry*, *32*(2), 121–124. https://doi.org/10.1177/10398562241230816

Lopatina, K., Dokuchaev, V. A., & Maklachkova, V. V. (2021). Data Risks Identification in Health care Sensor Networks. *2021 International Conference on Engineering Management of Communication and Technology, EMCTECH 2021 - Proceedings*. https://doi.org/10.1109/EMCTECH53459.2021.9619178

Loughlin, S., Fu, K., Gee, T., Gieras, I., Hoyme, K., Rajagopalan, S. R., Ransford, B., Vasserman, E., & Wirth, A. (2014). A roundtable discussion: Safeguarding information and resources against emerging cybersecurity threats. In *Biomedical Instrumentation and Technology* (Vol. 48, Issue HORIZONS SPRING). https://doi.org/10.2345/0899-8205-48.s1.8

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. In *Technology and Health care* (Vol. 24, Issue 1). https://doi.org/10.3233/THC-151102

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers and Security*, *95*. https://doi.org/10.1016/j.cose.2020.101846

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, *27*(2). https://doi.org/10.1108/ICS-03-2018-0031

McEvoy, T. R., & Kowalski, S. J. (2019). Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-technical Approach. *Complex Systems Informatics and Modeling Quarterly*, *2019*(18). https://doi.org/10.7250/csimq.2019-18.03

Mejía-Granda, C. M., Fernández-Alemán, J. L., Carrillo-de-Gea, J. M., & García-Berná, J. A. (2024). Security vulnerabilities in healthcare: an analysis of medical devices and software. *Medical & Biological Engineering & Computing*, *62*(1), 257–273.

Mitnick, K. D., & Simon, W. L. (2003). The art of deception: Controlling the human element of security. John Wiley & Sons.

Mohammed, Z. (2022). Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. *Organizational Cybersecurity Journal: Practice, Process and People*, *2*(1). https://doi.org/10.1108/ocj-05-2021-0014

Morgan, D. L. (2007). Paradigms lost and pragmatism regained: Methodological implications of combining qualitative and quantitative methods. *Journal of Mixed Methods Research*, *1*(1), 48–76.

Mumford, E. (2000). A socio-technical approach to systems design. Requirements engineering, 5(2), 125133. https://link.springer.com/article/10.1007/PL00010345

Mumford, E. (1983). Designing human systems for new technology: the ETHICS method. *Manchester Business School.*

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. In *Information Systems Journal* (Vol. 16, Issue 4). https://doi.org/10.1111/j.1365-2575.2006.00221.x

Myers, M. D., & Avison, D. (2002). *Qualitative research in information systems: a reader*. Sage.

Nicho, M., & McDermott, C. D. (2019). Dimensions of "socio" vulnerabilities of advanced persistent threats. *2019 27th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2019*. https://doi.org/10.23919/SOFTCOM.2019.8903788

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. In *Sensors* (Vol. 21, Issue 15). https://doi.org/10.3390/s21155119

NIST. (2013). Glossary of key information security terms. In *NIST IR* (Vol. 7298, Issue Revision 2).

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA Journal of Business and Public Administration*, *9*(3), 71–88.

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, *35*(4). https://doi.org/10.1080/02684527.2020.1752459

Ogunniye, G., Hana, A., & Watson, J. (2024). PETRAS: a socio-technical framework for Internet of Things research and development. *Frontiers in the Internet of Things*, *3*. https://www.frontiersin.org/journals/the-internet-of-things/articles/10.3389/friot.2024.1336564

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1), 1–28.

Palvia, S. C., Sharma, R. S., & Conrath, D. W. (2001). A socio-technical framework for quality assessment of computer information systems. *Industrial Management and Data Systems*, *101*(5). https://doi.org/10.1108/02635570110394635

Passmore, J. (2019). Mindfulness in organizations (part 1): a critical literature review. *Industrial and Commercial Training*, *51*(2), 104–113. https://doi.org/10.1108/ICT-07-2018-0063

Patel, B., & Makaryus, A. N. (2024). The implications of cardiac device cybersecurity responsibilities and challenges faced by policymakers, manufacturers, and patients. *Expert Review of Pharmacoeconomics & Outcomes Research*, 1–5.

Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. In *ICT Express* (Vol. 9, Issue 4). https://doi.org/10.1016/j.icte.2023.02.007

Perrotin, P., Belloir, N., Sadou, S., Hairion, D., & Beugnard, A. (2022). Using the architecture of Socio-Technical System to analyse its vulnerability. *2022 17th Annual System of Systems Engineering Conference, SOSE 2022*. https://doi.org/10.1109/SOSE55472.2022.9812648

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.

Pranggono, B., & Arabo, A. (2021). COVID -19 pandemic cybersecurity issues . *Internet Technology Letters*, *4*(2). https://doi.org/10.1002/itl2.247

Rajamäki, J., & Pirinen, R. (2017). Towards the cyber security paradigm of ehealth: Resilience and design aspects. *AIP Conference Proceedings*, *1836*. https://doi.org/10.1063/1.4981969

Reichertz, J. (2007). Abduction: The logic of discovery of grounded theory. *The SAGE Handbook of Grounded Theory*, 214–228.

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. *Sustainability*, *12*(17), 7002.

Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information Security Behavior in Health Information Systems: A Review of Research Trends and Antecedent Factors. In *Health care (Switzerland)* (Vol. 10, Issue 12). https://doi.org/10.3390/healthcare10122531

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students*. Pearson education.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Health care data breaches: insights and implications. *Health care*, *8*(2), 133.

Shukla, S., George, J.P., Tiwari, K., Kureethara, J.V. (2022). Data Security. In: Data Ethics and Challenges. SpringerBriefs in Applied Sciences and Technology(). Springer, Singapore. https://doi.org/10.1007/978-981-19-0752-4_3

Silverman, D. (2013a). *Doing qualitative research: A practical handbook*. SAGE publications limited.

Silverman, D. (2013b). *Doing Qualitative Research: A Practical Handbook*. SAGE.

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, Mitigating, and recovering from Ransomware attacks. *Applied Clinical Informatics*, *7*(2), 624–632. https://doi.org/10.4338/ACI-2016-04-SOA-0064

Slayton, R. (2021). Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. *Science Technology and Human Values*, *46*(1). https://doi.org/10.1177/0162243919901159

Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. (2023). A National Survey of Hospital Cyber Attack Emergency Operation Preparedness. *Disaster Medicine and Public Health Preparedness*, *17*(3). https://doi.org/10.1017/dmp.2022.283

Svandova, K., & Smutny, Z. (2024). Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review. In *Journal of Multidisciplinary Health care* (Vol. 17, pp. 2281–2301). Dove Medical Press Ltd. https://doi.org/10.2147/JMDH.S459987

Sweeney E. (2017). Health care data breaches haven't slowed down in 2017 and insiders are mostly to blame. *Fierce Health care*. https://www.fiercehealthcare.com/privacy-security/healthcare-data-breaches-haven-t-slowed-down-2017-and-insiders-are-mostly-to-blame

Szczepaniuk, H., & Szczepaniuk, E. K. (2023). Cryptographic evidence-based cybersecurity for smart healthcare systems. *Information Sciences*, *649*. https://doi.org/10.1016/j.ins.2023.119633

Taddeo, M., Jones, P., Abbas, R., Vogel, K., & Michael, K. (2023). Socio-Technical Ecosystem Considerations: An Emergent Research Agenda for AI in Cybersecurity. *IEEE Transactions on Technology and Society*, *4*(2). https://doi.org/10.1109/tts.2023.3278908

Tavory, I., & Timmermans, S. (2014). *Abductive analysis: Theorizing qualitative research*. University of Chicago press.

Thantilage, R. D., Le-Khac, N. A., & Kechadi, M. T. (2023). Health care data security and privacy in Data Warehouse architectures. In *Informatics in Medicine Unlocked* (Vol. 39). https://doi.org/10.1016/j.imu.2023.101270

Tikanmäki, I., & Ruoslahti, H. (2024). Insights on Human Factors Enhancing Cybersecurity. *Information & Security*, *55*(3), 225–235.

Tisdell, E. J., Merriam, S. B., & Stuckey-Peyrot, H. L. (2025). *Qualitative research: A guide to design and implementation*. John Wiley & Sons.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586.

Trist, E. L, & Bamforth, K. W. (1951). Some Social and Psychological Consequences of the Longwall Method of Coal-Getting: An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social Structure and Technological Content of the Work System. *Human Relations*, *4*(1), 3–38. https://doi.org/10.1177/001872675100400101

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

Verizon Enterprise. (2018). *2018 Data Breach Investigations Report*. https://www.verizon.com/business/en-gb/resources/2018-data-breach-investigations-report-dbir.pdf

Vukotich, G. (2023). Health care and Cybersecurity: Taking a Zero Trust Approach. *Health Services Insights*, *16*. https://doi.org/10.1177/11786329231187826

Walker T. (2017, December 10). Interoperability a must for hospitals, but it comes with risks. *Health care Executive*. https://www.semanticscholar.org/paper/Interoperability-a-must-for-hospitals%2C-but-it-comes-Walker/167780c53ddf0eaf4c33cf3a192cceedddb0bc62

Wang, S., & Wang, H. (2021). A sociotechnical systems analysis of knowledge management for cybersecurity. *International Journal of Sociotechnology and Knowledge Development*, *13*(3). https://doi.org/10.4018/IJSKD.2021070105

Wang, Z., Huo, Z., & Shi, W. (2015). A Dynamic Identity Based Authentication Scheme Using Chaotic Maps for Telecare Medicine Information Systems. *Journal of Medical Systems*, *39*(1). https://doi.org/10.1007/s10916-014-0158-2

Wasserman L., & Wasserman Y. (2022). Hospital cybersecurity risks and gaps Review for the non-cyber professional. *Frontiers in Digital Health*, *4*, 135–135. https://doi.org/10.3389/fdgth.2022.862221

Whitman, M. E., & Mattord, H. J. (2009). Principles of information security (p. 656). Boston, MA: Thomson Course Technology.

Whitworth, B. (2011). A Brief Introduction to Sociotechnical Systems. In *Encyclopedia of Information Science and Technology, Second Edition*. https://doi.org/10.4018/978-1-60566-026-4.ch066

Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. In *Medical Devices: Evidence and Research* (Vol. 8). https://doi.org/10.2147/MDER.S50048

Wilner, A. S., Luce, H., Ouellet, E., Williams, O., & Costa, N. (2021). From public health to cyber hygiene: Cybersecurity and Canada's healthcare sector. *International Journal*, *76*(4), 522–543. https://doi.org/10.1177/00207020211067946

Winton R. (2016, February 18). Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. *Los Angeles Times*.

https://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Woodward, J. (1965). Industrial organization: Theory and practice.

Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., Kumar, R., & Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Health care Technology Letters*, *8*(3). https://doi.org/10.1049/htl2.12008

Zhan, Y., Ahmad, S. F., Irshad, M., Al-Razgan, M., Awwad, E. M., Ali, Y. A., & Ahmad Ayassrah, A. Y. A. B. (2024). Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. *Heliyon*, *10*(1). https://doi.org/10.1016/j.heliyon.2023.e22947

Zhu, S., Saravanan, V., & Muthu, B. A. (2020). Achieving data security and privacy across healthcare applications using cyber security mechanisms. *Electronic Library*, *38*(5–6). https://doi.org/10.1108/EL-07-2020-0219

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human Computer Studies*, *131*. https://doi.org/10.1016/j.ijhcs.2019.05.005

Zoto, E., Kianpour, M., Kowalski, S., & Lopez-Rojas, E. A. (2019). A Socio-technical Systems Approach to Design and Support Systems Thinking in Cybersecurity and Risk Management Education. *Complex Systems Informatics and Modeling Quarterly*, *0*, 65–75. https://doi.org/10.7250/csimq.2019-18.04

JOURNAL OF MEDICAL INTERNET RESEARCH Ewoh & Vartiainen

Review

Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review

Pius Ewoh, MBA; Tero Vartiainen, PhD

School of Technology and Innovations, Information Systems Science, University of Vaasa, Vaasa, Finland

Corresponding Author:
Pius Ewoh, MBA
School of Technology and Innovations
Information Systems Science
University of Vaasa
Wolffintie 32
Vaasa, 65200
Finland
Phone: 358 414888477
Email: pius.ewoh@uwasa.fi

Abstract

Background: Health care organizations worldwide are faced with an increasing number of cyberattacks and threats to their critical infrastructure. These cyberattacks cause significant data breaches in digital health information systems, which threaten patient safety and privacy.

Objective: From a sociotechnical perspective, this paper explores why digital health care systems are vulnerable to cyberattacks and provides sociotechnical solutions through a systematic literature review (SLR).

Methods: An SLR using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) was conducted by searching 6 databases (PubMed, Web of Science, ScienceDirect, Scopus, Institute of Electrical and Electronics Engineers, and Springer) and a journal (*Management Information Systems Quarterly*) for articles published between 2012 and 2022 and indexed using the following keywords: "(cybersecurity OR cybercrime OR ransomware) AND (healthcare) OR (cybersecurity in healthcare)." Reports, review articles, and industry white papers that focused on cybersecurity and health care challenges and solutions were included. Only articles published in English were selected for the review.

Results: In total, 5 themes were identified: human error, lack of investment, complex network-connected end-point devices, old legacy systems, and technology advancement (digitalization). We also found that knowledge applications for solving vulnerabilities in health care systems between 2012 to 2022 were inconsistent.

Conclusions: This SLR provides a clear understanding of why health care systems are vulnerable to cyberattacks and proposes interventions from a new sociotechnical perspective. These solutions can serve as a guide for health care organizations in their efforts to prevent breaches and address vulnerabilities. To bridge the gap, we recommend that health care organizations, in partnership with educational institutions, develop and implement a cybersecurity curriculum for health care and intelligence information sharing through collaborations; training; awareness campaigns; and knowledge application areas such as secure design processes, phase-out of legacy systems, and improved investment. Additional studies are needed to create a sociotechnical framework that will support cybersecurity in health care systems and connect technology, people, and processes in an integrated manner.

(J Med Internet Res 2024;26:e46904) doi: 10.2196/46904

KEYWORDS

health care systems; cybersecurity; sociotechnical; medical device; secure systems development; training; ransomware; data breaches; protected health information; patient safety

Introduction

Background

Cybersecurity in health care systems entails the safeguarding of electronic information and assets against unauthorized access, use, and disclosure [1]. The main objective of cybersecurity in health care systems is to protect the privacy, integrity, and accessibility of health information to provide secure health care services. Despite the digital transformation in health care delivery, health care organizations are facing increasing challenges and crises, which include data breaches of patient health information and vulnerability in their critical infrastructure [2]. Research has highlighted that health care systems are becoming more vulnerable to cyberattacks as technology advances [3]. Furthermore, the internet and its diverse nature and connection to the delivery of telehealth and continuous health care services create multiple points of access for cyberattacks [4,5].

In high-income countries such as Finland, the United States, and the United Kingdom, integrated technology is used to monitor and manage health care systems. For instance, at least 10 to 15 medical devices are linked to each patient's electronic bed in a public hospital [6]. These complexities increase the susceptibility of health care networks to cyberattacks [6,7]. Studies conducted through the simulation of medical devices have similarly revealed that pacemakers and pulse oximeters can be hacked and compromised without a physician's knowledge [8,9]. Ransomware is another type of man-made malware that can disrupt health care systems by infecting computer systems, locking people out of their files, and then demanding a ransom payment in exchange for access to those files [10,11]. Cyberattackers can publish the exposed health information to the web or sell it on the dark web [12]. This type of attack can result in breaches of patient privacy, subjecting health care organizations to fines that are consistent with human health service regulations and European General Data Protection Regulation (GDPR) policies for data breaches. For example, research has shown that, between 2012 and 2022, more than US $128,244,290 million in fines were paid in the United States alone for violations of Health Insurance Portability and Accountability Act laws on data breaches against health care organizations [13]. Although these fines were derived from no less than 111 health care organizations, many organizations have failed to report breaches.

Cybersecurity education is seriously lacking [14,15]. Moreover, a critical problem with cybersecurity in health care systems is the lack of involvement or recruitment of people with expertise and training in cybersecurity [16], resulting in considerable neglect of the cybersecurity infrastructure [17]. A systematic literature review (SLR) revealed that, between 2018 and 2019, more than 24% of the data breaches in all industries happened within the health care context [18,19].

Between 2009 and 2021, the US Department of Health and Human Services office reported 4419 health care data breaches, resulting in >314 million health care records being lost, stolen, or exposed [20]. In 2015, an estimated 113.27 million records were stolen and exposed, and in 2021 alone, the US Department of Health and Human Services also reported at least 2 health care data leaks daily [13]. The statistics clearly show an upward trend in health care data breaches over the past 10 years [21]. When considering this trend on a global scale, the number of health information breaches could potentially reach into the billions of health records. Organizations such as Vaastimo Oy Finland; National Health Service trusts in the United Kingdom; Anthem, Inc; Premera Blue Cross; and Excellus Health Plan have been victims of these threats and breaches of health information. Breaches and vulnerabilities in health care delivery, human safety, and protection of sensitive information are deeply disconcerting. However, it can be argued that research solutions are fragmented and sparse. There is a gap in the knowledge areas of health care cybersecurity in the literature and in practice regarding the vulnerability of health care systems and the reasons for cyberattacks. The argument and motivation are that a holistic approach to security is needed because humans are the weakest link in the cyberattack chain [11,22].

Coventry and Branley [6] have highlighted the need for resilience and changes in their studies on human behavior, technology, and processes as part of a holistic solution to the problem of health care system vulnerability. The information, technology, processes, objectivity and values, skills and knowledge, management systems and structure, and other resources dimensions by Heeks [23] also point out that avoiding security design reality gaps requires approaching the security functionality of a health information system as a sociotechnical system and not as a technical system. Security by design, or secure design, is an approach to cybersecurity that enables organizations to automate their data security controls and formalize the design of their infrastructure so that they can build security into their IT management processes [24,25].

In this study, a sociotechnical approach is defined as the interaction between humans and technology with the aim of creating technically efficient organizational information systems and user satisfaction [26]. Furthermore, conceptualizations of this approach are concerned with 3 primary dimensions: the social environment, technical environment, and organizational environment [27]. Sociotechnical design is identified as an approach to connect the integration of systems while ensuring that the multifaceted challenges and complexities in smart health care are well managed [28,29]. Smart health care can be defined as care that is equipped with smart IT, such as Internet of Medical Things (IoMT) devices that have the capabilities to anticipate and diagnose patient diseases; respond to treatments; guide, manage, and improve user comfort; and provide security and entertainment via hospital management systems. According to Coiera [30], "if healthcare is to evolve at a pace that will meet the needs of society, it will need to embrace the science of sociotechnical design." Therefore, the application of a sociotechnical perspective in health care cybersecurity in this study aimed at better understanding and mitigating the multifaceted challenges and poor uptake and performance of health care system security within health care organizations.

This existing gap in knowledge and practice was a major motivation for this SLR. It is necessary to connect the fragmented research and manage this knowledge gap regarding why health care systems are vulnerable to cyberattacks as the

study by Coventry and Branley [6] did not address this aspect in detail. An SLR was conducted to develop proactive cybersecurity strategies to mitigate threats and vulnerabilities that result in health care data breaches by proposing sociotechnical solutions and recommendations. Furthermore, to link human behavior, technology, and processes as highlighted by Coventry and Branley [6] and supported by the narrative review by Mohan et al [31] for further research, these 3 core areas can be interpreted as a sociotechnical framework [27]. It is essential to mitigate the increase in breaches of health information and protect health care from cybercrime and cyberattacks on critical health care infrastructure. However, none of these studies have examined why health care systems are vulnerable to attack through a sociotechnical lens. On the basis of this knowledge gap identified in the literature, the following research questions (RQs) were raised: (1) Why are health care systems vulnerable to cyberattacks? (RQ 1) (2) How can health care systems be protected? (RQ 2).

The objective of this review was to explore from a sociotechnical approach why digital health care systems are vulnerable to cyberattacks, provide sociotechnical solutions, and identify the areas of health care systems that need further improvement.

Previous Literature Review

Regarding the existing literature on health care cybersecurity, our previous SLR identified the following review themes: (1) cybersecurity threats and trends: studies that provide solutions and insights into threats and trends have been conducted to address cybersecurity threats and trends in health care systems [2,6,11,17,32,33]; (2) cybersecurity vulnerability: some studies have also investigated the cybersecurity vulnerability of health care systems to provide solutions and future directions for health care services [22,34-36]; and (3) cybersecurity interceptions in health care: studies have also investigated cybersecurity interceptions with health care systems to protect the security posture of these systems [12,19,37]—Coventry and Branley [6] have highlighted the need for further studies on human behavior, technology, and processes to further investigate why health care systems are vulnerable and provide a holistic solution to this problem.

Therefore, there is a need for further studies to identify the reasons behind the increase in health information breaches in health care systems. This area of study through a sociotechnical lens is lacking. Accordingly, our SLR critically investigated why health care systems are vulnerable to cyberattacks and expanded this area of study from a sociotechnical point of view. This review is significant given the lack of SLRs on the areas linking human behavior, technology, and processes using a holistic approach from a sociotechnical viewpoint in this context and as the studies by Coventry and Branley [6] and Mohan et al [31] were based on narrative reviews.

Methods

Protocol and Registration

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines were followed to conduct our SLR using the checklist guide [38] (Multimedia Appendix 1). The aim of this review was to identify the reasons why health care systems are vulnerable to cyberattacks and provide sociotechnical solutions. In the planning stage of this review, a protocol for the sources of information, search strategies, study selection, criteria for eligibility, and data collection processes was created, and this review was not registered.

Eligibility Criteria

A paper was selected for inclusion if it was published in English and comprised a full-text version of the manuscript, review paper, conference proceeding paper, report, news article or website, or white paper published between 2012 and 2022. The introduction, abstract, results, and discussion sections of the paper were checked by the authors for conformity with the study objectives and critical appraisal using the checklist guidelines before inclusion. Research papers were excluded if they were not relevant to the research areas—cybersecurity, cybercrime, ransomware, and health care. These criteria are presented in Textbox 1.

Textbox 1. Article inclusion and exclusion criteria.

Inclusion criteria

- Study types: published peer-reviewed and original research papers (empirical and conceptual papers)
- Bibliometric study types: white papers and cybersecurity news reports in line with health care and cybersecurity
- Period: papers published between 2012 and 2022
- Language: English
- Subjects and domain: computer sciences, health care, and cybersecurity
- Requirements for paper inclusion: full-text papers.

Exclusion criteria

- Study types: unpublished work, editorial letters, textbooks, and research in progress
- Language: any other languages
- Subjects: studies outside the domain of cybersecurity and health care

Information Sources

To identify original research papers and review papers on cybersecurity in health care systems published between 2012 and 2022, a total of 6 databases (Web of Science, ScienceDirect, Scopus, PubMed, Springer, and the Institute of Electrical and Electronics Engineers) and a journal (*Management Information Systems Quarterly*) were searched. Furthermore, bibliometric records such as website reports, white paper reports, and magazine reports that supported cybersecurity in health care were also collected for the review. As a means of verifying the papers identified in our search, we searched Google Scholar using a search string.

Search Strategy

The following search string and keywords were used: ("cybersecurity" OR "cybercrime OR ransomware") AND ("health care") OR ("cybersecurity in healthcare"). Multimedia Appendix 2 provides more information.

Data Extraction

A total of 70 papers were extracted and recorded in a Microsoft Excel (Microsoft Corp) spreadsheet. The extracted data included information such as author or authors, year of publication, method, problem, and solution. The first author independently charted the data and updated the table to ensure the quality of the key findings drawn from the papers based on the recommendations of the second author. Critical appraisal was conducted to ensure the quality of evidence and the relevance of the articles. The data retrieved from the selected articles were analyzed.

Data Synthesis

The data from the literature were analyzed and synthesized using qualitative themes, which are presented in the following sections. The data were analyzed to identify the causes of vulnerabilities; solutions provided in the literature; and areas of classification based on sociotechnical, technical, and social perspectives in health care systems.

Results

Selection of Sources of Evidence

A total of 1257 papers were retrieved for the screening exercises. To determine whether the papers met our inclusion criteria regarding the topic domain, we began by scanning the abstracts and titles. The papers were reviewed by reading the full texts and determining their eligibility. Duplicated papers as well as those nonrelevant to cybersecurity, cybercrime, ransomware, and health care research were excluded. Furthermore, some papers were excluded after reading them in full and discovering that they were papers on research in progress. Finally, 70 papers were included in the analysis based on the eligibility criteria. Figure 1 illustrates the selection process.

The results of the SLR show the reasons why health care systems are vulnerable to cyberattacks and health care breaches. These reasons are the 5 vulnerability themes (Figure 2 and Table 1). Furthermore, the 5 vulnerability themes were classified into social, technical, and sociotechnical approaches.

Figure 1. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow diagram for paper selection.

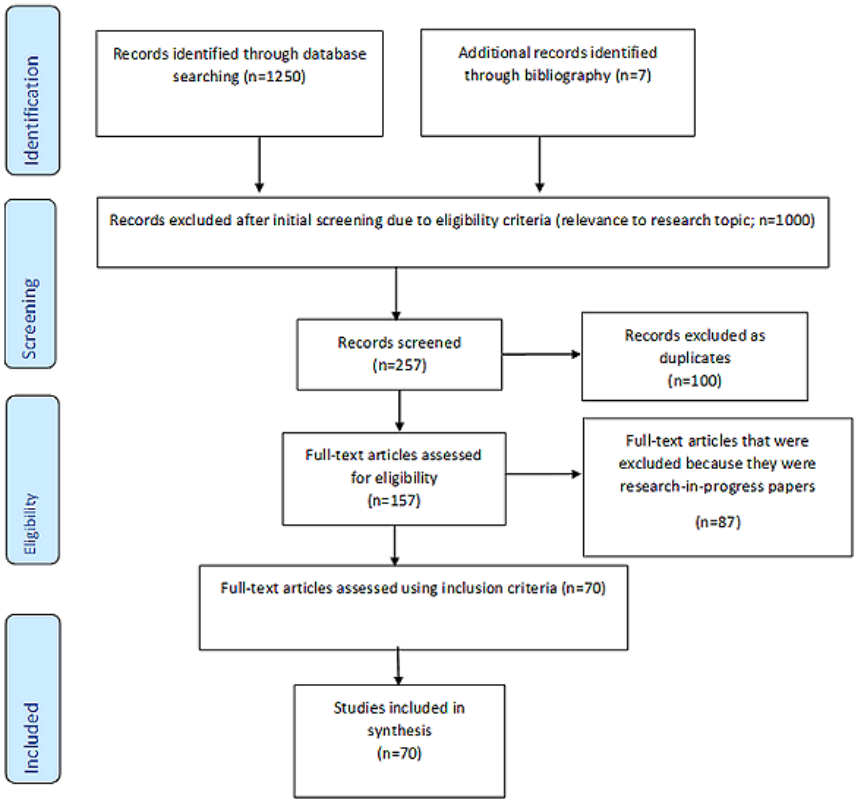


Figure 2. Results and insight into health care system vulnerability.

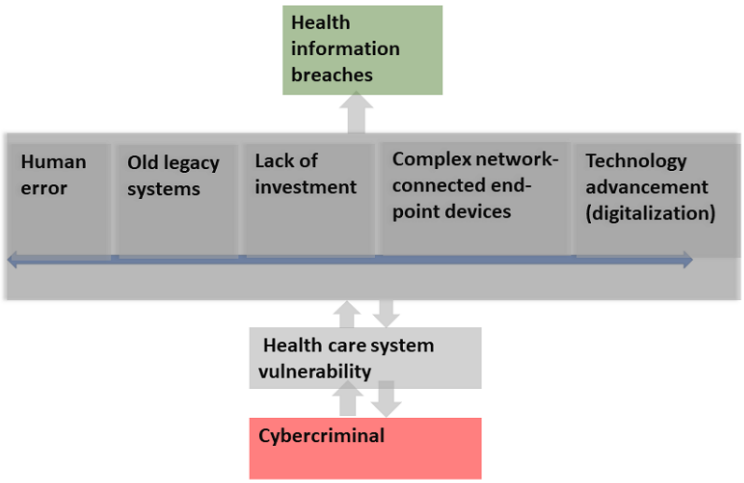


Table 1. Findings on health care system vulnerability categorized by themes and authors (N=70).

Vulnerabilities in health care	Type of approach	Studies, n (%)	References
Human error	Social	8 (11)	• Arndt [39] • Twitter [40] • Mukherjee [41] • Ponemon Institute [42] • IBM Security [43] • Scott and Wingfield [44] • Jalali et al [19] • He et al [36] • Gordon et al [45]
Old legacy systems	Sociotechnical	11 (16)	• Bouveret [46] • ECRI[a] Institute [47] • Sweeney [16] • Faruki et al [48] • Filkins [49] • Fu and Blum [50] • Offner et al [2] • McHugh [51] • Newman [52] • Scott and Wingfield [44] • Tully et al [53]
Lack of investment	Sociotechnical	15 (21)	• Argaw et al [11] • Emsisoft Malware Lab [54,55] • Branley-Bell et al [56] • Information Commissioner's Office, National Cyber Security Centre, and James M [57] • Kaspersky Inc [58] • PCEB[b] [59] • Rahman et al [60] • Gkioulos and Chowdhury [61] • Tully et al [53] • Williams and Woodward [34] • Coventry et al [62] • Jalali et al [19,33] • He et al [36] • Jalali and Kaiser [37]

Vulnerabilities in health care	Type of approach	Studies, n (%)	References
Complex network-connected end-point devices	Technical	36 (51)	• Burns et al [63] • Bouveret [46] • Chua [64] • Coventry et al [62] • Dameff et al [8] • Dienna et al [65] • ECRI Institute [47] • Filkins [49] • Francis [66] • Frost [3] • Twitter [40] • Giansanti [5] • Handa et al [67] • Offner et al [2] • Klonoff [9] • Lechner [68] • Lewis [69] • Lyon [70] • McHugh [51] • Mohan [71] • Newman [52] • Baranchuk et al [72] • Perakslis [73] • Peterson [74] • Sajedi and Rahbar Yaghobi [75] • Omotosho et al [76] • Singh et al [77] • Sittig and Singh [78] • Snell [79] • Tully et al [53] • Walker [7] • Williams and Woodward [34] • Jalali and Kaiser [37] • Jalali et al [19,33] • He et al [36]
Technology advancement (digitalization)	Technical	10 (14)	• Bhuyan et al [80] • Coventry and Branley [6] • Karambelas [4] • Kruse et al [17] • Raina MacIntyre et al [81] • Filkins et al [82] • PECB Insights [59] • Jalali et al [19,33] • Rodrigues et al [83]

[a]ECRI: Emergency Care Research Institute.

[b]PECB: Professional Evaluation and Certification Board.

The results also revealed that >24% of the data breaches from all industry clusters originated in the health care sector alone (Table 1) [19,21,84]. Other studies highlighted that organizations tend to spend more money on procuring new technology while committing only ≤5% of their budgets to the security of their critical health care systems [17,35]. Cybercriminals exploit health care systems due to the lack of investment, technology advancement as a result of digitalization, human error due to a lack of awareness and training, and old legacy systems, which enable cybercriminals to access valuable health information and sell it on the dark web for money and other gains [12]. The results reported a significant increase in data breaches and cyberattacks, with complex systems, IoMT devices, technology advancement, and network-connected end-point devices in complex connected heterogeneous health care systems identified as the major contributing factors.

The studies also identified a shortage of cybersecurity skills to contain cyberattacks or threats to health care organizations and systems [16]. The studies revealed that approximately 60% to 70% of health care organizations have witnessed breaches of health information without disclosure [85].

Human Error

Human error is a significant factor in the event of a cyberattack [11,22]. This shortcoming is one of the most crucial issues in health care systems as most cybercriminals use methods such as phishing to execute attacks with just a deceitful email. This is a social problem that can be addressed from a social approach. For example, human error posed a risk to the Geneva University

Hospitals [86]. Table 1 shows that 11% (8/70) of the studies acknowledged human error as the primary social reason for health care system vulnerability. Human error is attributed to a lack of skills and is a major trend in this ever-changing technological landscape, playing a role in several cybersecurity breaches [56]. From a technological point of view, a lack of expertise from humans and threats from human-related events are responsible for >70% of data fraud and breaches in business organizations (McCue, A, unpublished data, May 2008) [80] because of the value of health information on the dark web [6] and breaches in business organizations (McCue, A, unpublished data, May 2008) [80]. Furthermore, human-related threats have recently emerged as a growing concern.

Old Legacy Systems

Old legacy systems have been the basis of system development from the dawn of the medical device, operating system, and embedded mobile device era. Legacy operating systems such as Windows ME, Windows 2000, MS-DOS, UNIX, and firmware provide the foundation for system development. However, these systems pose a significant threat to health care sectors and organizations in our current era. Table 1 shows that 16% (11/70) of the studies acknowledged the vulnerability of health care systems to attacks due to old legacy systems. Such attacks occur from a sociotechnical approach, with cybercriminals exploiting humans and technology. Many data breaches, system incompatibilities, and security risks in health care systems and sectors are associated with legacy systems. Similarly, our SLR found that 85% of medical organizations use outdated operating systems or infrastructure [12,16]. Furthermore, Fu and Blum [50] raised concerns about organizations relying on unsupported software, alluding to medical devices that run on Windows XP operating systems with service packs but lack security updates. In addition, the case of the National Health Service 2017 WannaCry malware, which interrupted health care operations and shut down numerous hospitals by infecting thousands of computers, was caused by Windows XP software [87]. The authorities had been informed about the bugs but failed to act due to negligence. When a medical device is compromised, cybercriminals use it as a gateway to abuse hospitals, health care system networks, and health information or data. Perriello [88] and Meggitt [89] highlighted another issue, *Medijack*, referring to hackers hijacking medical devices to construct a back entrance into a hospital network. As a result, the use of a network of old legacy medical devices for administrative processes and care delivery increases the opportunities for an attacker or cybercriminal to easily intrude into hospital or health care organization networks and exploit and compromise the network of medical devices and health information. In this era of rapid medical technological advancement, health care systems also lack built-in security safeguards. Legacy systems do not support new technologies, and so the network of medical equipment in intensive care units, recovery rooms, operating rooms, and electronic health records (EHRs) will lack proper and secure communication and interoperability. Outdated legacy systems and unsupported operating systems are vulnerable to high-speed attacks. Furthermore, these problems are attributable to the lack of important updates to health care infrastructure. To support our point, health and human services should provide more guidance on applying the National Institute of Standards and Technology framework to the health care industry and consider appropriate incentives that would allow health care organizations to phase out old vulnerable legacy systems [16].

Lack of Investment

Investment in the health sector will yield better outcomes and quality health care delivery. According to our analysis and results, the health care sector suffers from underinvestment, and crucial infrastructure and training for health care cybersecurity are disregarded [6], which is one of the primary causes of the increase in sensitive health information breaches. Investment can be seen in social (human) and technical (technology) aspects. As shown in the analysis in Table 1, a total of 21% (15/70) of the studies acknowledged the lack of investment and advised both directly and indirectly regarding the necessity of cybersecurity investment in the health care industry [55,56]. The analysis acknowledged and revealed that the health care sector lagged more than other sectors in terms of health information protection and breaches. Furthermore, the findings of our SLR revealed that 80% to 85% of worldwide breaches occur in the health sector [4], whereas 45% to 90% of health care organizations have witnessed one or more threats or breaches [18,57]. Investment in critical infrastructure for health care and best practices in cyber hygiene will aid in the protection of health care systems from potential vulnerabilities. Proper investment will ensure the safeguarding of personal information and render health care systems more resilient to cyberattacks.

Complex Network-Connected End-Point Devices

Medical end-point devices have long served as a hospital's backbone for treatment, diagnosis, and precision-based technological applications to complement health care service operations and management. To fully exploit their potential, the medical device development pattern has shifted from traditional-based medical device system development to a network of wireless, connected end-point technological devices with built-in communications and remote connectivity. Complex network-connected end-point devices have increased the cyberattack surfaces in conjunction with their complexity and technological systems as heterogeneity in nature of medical technology has evolved. Complex network devices are classified as a technical challenge from the perspective of technical security system design. The analysis in Table 1 shows that 51% (36/70) of the studies acknowledged network-connected end-point medical devices as the most significant technical reason for health care systems' vulnerability to cyberattacks. The operational modes continue to evolve with more interconnections between new applications and devices such as cloud-based applications, third-party software, IoMT devices, and system networks in health care environments. Lechner [68] revealed that original equipment manufacturers are now creating interconnected medical devices without incorporating proper cybersecurity features into the development life cycle of medical and end-point device systems. The vulnerability of the end point requires urgent attention; otherwise, cybercriminals will continue to use the weakness of connected devices to access personal health information. According to research and cybersecurity

stakeholders, wearables, implanted devices, and sensors may become the new targets of future exploits [6,8]. As shown in Table 1, complex network-connected end-point medical devices also require medical technology security by design [72,90] as a solution strategy to protect critical health care infrastructure from breaches. In the past, medical device system development has primarily focused on critical performance and safety. Furthermore, the security aspects of these medical devices are not a factor during the planning and development process. The process indicates that developing traditional or stand-alone systems of noninterconnected devices was a suitable method for designing the traditional approach. These are the current legacy systems that lack interoperability, updates, security design, or compatibility. Furthermore, connected medical devices such as sensor-controlled drug infusion pumps, cardiac pacemakers, pulse oximeters, and network-connected x-ray machine components such as picture archiving and communication systems are vulnerable to cybersecurity threats and attacks [5]. To continue solving cybersecurity issues in medical devices, developers and actors must recognize the importance of the health care environment's complex operations. In addition, there should be incident reports, an audit trail in the device system database, and paper-based documentation of technical vulnerabilities [34]. Medical device manufacturers such as security experts or systems integrators must address this issue because, with a single cyber vulnerability, cybercriminals or hackers can exploit medical technology connected to the internet, compromising data integrity, wearable sensor readings, protected health information, patient safety, and care outcomes [2,50]. When cyberattackers manipulate systems or deposit a virus, this could cause medical device software or systems to malfunction, resulting in abnormal effects or different readings from the systems, such as implantable medical devices that take and display incorrect readings [5,8].

Technology Advancement (Digitalization)

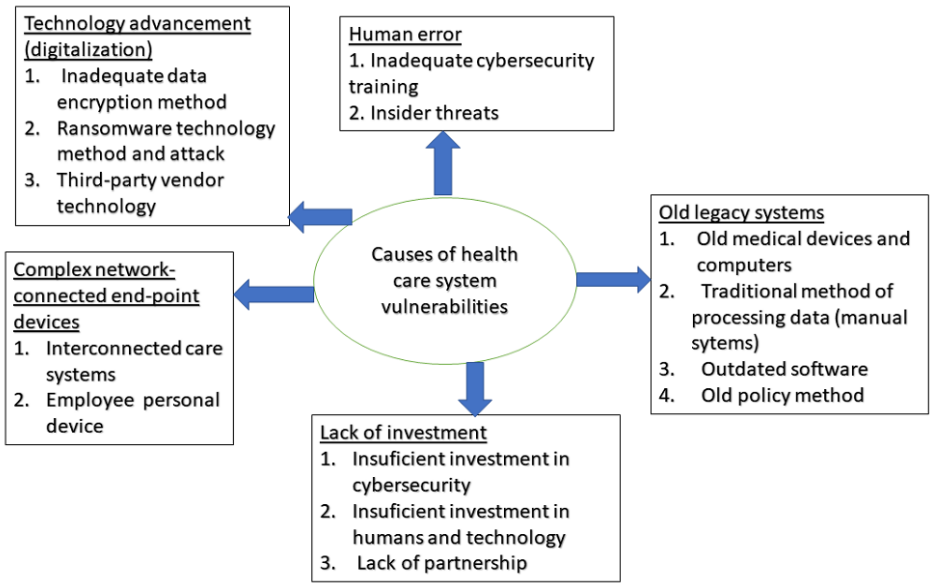
Technology advancement has enabled unique access and benefits to revolutionize health care systems in terms of precision. Modern medical care now relies on health care delivery organizations, including hospitals and clinics, built on a backbone of connected computer-based infrastructure. Over the past 30 years, the expansive integration of new health care technology has changed the face of medicine [53]. However, the rapid digitalization in health care delivery, where medical devices are intertwined in a digital network setting and system to ensure the precision of health care delivery with the use of IoMT and digital devices, has created gateway access for cyberattacks, risks, and vulnerabilities [37,81]. Table 1 shows that 14% (10/70) of the studies acknowledged technology advancement due to digital transformation as the reason why health care systems are vulnerable to cyberattacks. This type of attack and vulnerability usually occur from the technical areas of cyberattacks, for example, a technology error such as glitches and design errors. One example of vulnerability is St. Joseph Hospital in California, where the health information of 31,800 patients was made public through a basic internet search engine for >1 year without anyone noticing. The underlying issue was that security settings on the medical devices were not correctly configured [91]. As technology continues to evolve, IoMT will become more inseparable in health care service delivery, which will create more vulnerabilities if health care organizations continue to disregard cybersecurity threats without proactive readiness to address them in this era of Industry 4.0. These vulnerabilities pose threats to the security and privacy of human and health information.

Studies have shown the health care sector to be unequipped and lacking in investment [11,92]. For example, the use of electronic health technology, motivated by acts such as the Meaningful Use program introduced by the US government, has compelled many health care organizations to increase the use of digital technology in health care, such as EHRs and electronic data exchange, and comply with enhanced health care delivery management. Organizations began to focus on adopting new technology and spending less on security, creating part of the problem [32]. Technological advancements and a federal policy mandate ultimatum are 2 of the causes noted in this SLR that have increased health care industry exposure to cyberattacks and breaches of health information [17]. Therefore, an organization should have proper planning; be proactive instead of reactive; and ensure the protection of health technology, information, patient privacy, and security when implementing or adopting advanced technology [17,80]. One such process is to ensure that a medical technology statement of disclosure and liability is included during the procurement, integration, and adoption of a technology. Support services and maintenance during and after procurement and installation should be part of the procurement process. Furthermore, the device manufacturer should also consider security in product development planning. Digital technology should also have the capability to monitor and collate threats and patterns and log these in a risk assessment register for analysis and improvement or threat containment.

Causes of Vulnerabilities in Health Care Systems

Figure 3 shows the causes of vulnerabilities in health care systems, which complement the findings regarding health care vulnerability, and categorizes them accordingly. The following sections address these vulnerabilities.

Figure 3. Causes of vulnerabilities in health care systems.



How Can Health Care Systems Be Protected?

Overview

This study summarizes how health care systems can be protected from cyber threats and cyberattacks and presented in Table 2.

Table 2. Health care system protection.

Health care vulnerability and description of challenges	Proposed solutions	References	Health care cybersecurity sociotechnical areas of application
Human error			Social approach
Information breaches and identity theft	• Inform human health office and owners of the data, train staff, learn to encrypt information, and have a backup plan and rollover system.	• Tuttle [93]	
Insecure behavior	• Implement training.	• Coventry et al [62]	
Cyber warfare	• Foster awareness and implementation of cyber hygiene. • Implement data encryption, network defense solutions, and protection of premises.	• Mukherjee [41]	
Employee negligence and error	• Implement training, invest in new skills for staff, and launch awareness campaign.	• He et al [36]	
Cybersecurity ethical issues, such as the disclosure and use of health information without consent	• Seek patient consent and balance privacy and autonomy for health information and usability.	• Loi et al [94] • Christen et al [95]	
Old legacy systems			Sociotechnical approach
Interoperability issues and incompatible device challenges	• Procure modern devices to enable seamless synchronization of devices and networks.	—[a]	
Interoperability issues	• Implement health policy, regulation compliance, and upgrades.	—	
Inability to update software and medical devices	• Phase out legacy systems.	• Sweeney [16]	
Lack of investment			Sociotechnical approach
Disregard of health care cyber critical infrastructure	• Invest in cyber critical systems.	• Kruse et al [17]	
Protect data, operations, and valuables	• Invest in cybersecurity protection mechanisms for sensitive activities.	—	
Design and device usability issues for processes and data security management	• Invest in human behavior, technology, and organizational processes.	• Coles-Kemp and Williams [96]	
Complex network-connected end-point devices			Technical approach
Cyberattack on hospital health care systems	• Defend the hospital with network security solutions. Have a backup and a roll-back system. Ensure that all standard policy and comprehensive guidelines are in place and always train staff to respond.	• Argaw et al [11]	
In case network-connected medical devices through the IoMT[b] are exposed	• Protect devices through assessment and extreme network defender solutions. Encrypt networks.	• Frost [3]	
Vulnerabilities due to sensor and IoT[c] devices	• Implement device simulation, security assessment, and extreme network defender solutions.	• Dameff et al [8]	
Vulnerability of end-point devices	• Develop network and device security protection solutions.	• Lewis [69] • Singh Rayat et al [77]	
Technology advancement (digitalization)			Technical approach

Health care vulnerability and description of challenges	Proposed solutions	References	Health care cybersecurity sociotechnical areas of application
Lack of security in medical devices and critical infrastructure	• Ensure that medical devices are designed with security before procurement and ensure that device manufacturers maintain and manage security.	• Lechner [68]	
Health care big data protection challenges	• Secure life cycle model and encryption through blockchain.	• Khaloufi et al [97]	
Health care system digitalization and medical device vulnerability	• Implement cyber hygiene and security in designing devices.	• Coventry and Branley [6]	
Digitalization and technology advancement vulnerability gap (digital dark alley) challenges	• Update firewall installations and use a secure design approach, cloud recovery planning, and backup.	• Karambelas [4]	

[a]Not applicable.

[b]IoMT: Internet of Medical Things.

[c]IoT: Internet of Things.

Human-Related Case Type and Challenges

The protection of health care systems from cyberattack-related vulnerabilities caused by human error, such as identity theft and health information breaches, requires by law that health care organizations inform the human health office, regulatory bodies, and data owners [93] to ensure compliance with ethical and privacy standard regulations [94,95]. A security compliance officer should also be employed to guide and ensure that proper cyber hygiene measures are in place to avoid such occurrences. It is important to ensure that health information is encrypted to assure that data are unusable and back up data offline and on the web. Furthermore, in cases in which a health care organization is saddled with challenges due to insecure human behavior, such as employee negligence, a lack of skills, and cyber warfare, the organization must ensure proper training of all staff [62] and implement awareness programs using a comprehensive guide to avert cyber threats [36,41]. This proposed solution requires a social approach in designing guidelines and training programs.

Old Legacy Systems Case Type and Challenges

Interoperability and compatibility challenges in medical devices stem from human-related activities within health care systems, potentially impacting the persistence of outdated legacy systems [50]. Therefore, to holistically protect health care systems, proposed solutions involve sociotechnical measures due to the old legacy in human work processes, organizational structures, and technology tasks, as mentioned by Offner et al [2]. Organizations should adhere to policies and standards linked to the old legacy, ensure proper updates and upgrades, and implement patches. Modern equipment that supports security and carries out updates must be procured to avert crises and phase out legacy systems [16].

Lack of Investment Case Type and Challenges

Investment in critical health care infrastructure is very important to ensure a health care ecosystem that is secure from cyberattacks and vulnerabilities. The susceptibility of health care to cyberattacks is a result of the underinvestment in and neglect of cybersecurity infrastructures. Kruse et al [17] also highlighted that a health organization invests ≤5% in cybersecurity but tends to focus on integrating and delivering care. It is important for a health care organization to invest in technology, human behavior, and processes [96] to protect sensitive and valuable health information from breaches and attacks.

Complex Network-Connected End-Point Devices Case Type and Challenges

The increase in health information breaches in hospitals is attributed to complex network-connected end-point devices, which are vulnerable to cyberattacks because sensor-based medical devices and system networks are interlinked and connected to the internet [8]. Internet of Things devices are vulnerable because they can be controlled through a media access control address and network. A proposed solution identified in this SLR highlighted that health care can be protected though proper encryption of data and installation of network defenders [3]. It is important that medical device simulation and assessment be performed through vulnerability analysis to ensure that devices are not tampered with or compromised [8].

Technology Advancement (Digitalization) Case Type and Challenges

Technology advancement has revolutionized the health care delivery process using digital technological processes. Manufactured medical devices enable patients to be diagnosed remotely, and physicians can administer care using telemedicine. However, technological advancements still lack security in the design of these devices because security is an afterthought during development, which makes them vulnerable to cyberattacks [5]. A proposed solution is that health care organizations must ensure that medical device security starts from the planning stage [68] and that device manufacturers maintain and manage security in the pre- and postmarket phases. This solution paradigm must be catalogued as a technical

measure. Hospitals with modern-day smart care should leverage comprehensive guidelines and compliance with standards such as those of the International Organization for Standardization or International Electrotechnical Commission 27001 or 27002, as well as cyber hygiene to enable effective and efficient care delivery processes [4,11]. Therefore, the implementation of solutions should always adopt a sociotechnical approach [96].

Intervention Application Areas and Domain Counts for 2012 to 2022

The selected studies from this SLR that discussed and presented knowledge interventions and solutions applied in some health care sectors between 2012 and 2022 are categorized and presented in Table 3.

Table 3. Intervention application areas and domain count for health care cybersecurity between 2012 and 2022 (N=70).

Vulnerability and knowledge application domain	Solution papers published in this domain between 2012 and 2022, n (%)	References
Human error		
Training	12 (17)	• Karambelas [4] • Giansanti [5] • Dameff et al [8] • Argaw et al [11] • Bhuyan et al [80] • Offner et al [2] • Holst et al [98] • Branley-Bell et al [56] • Chowdhury and Gkioulos [61] • Khando et al [99] • Coventry et al [62] • Information Commissioner's Office, National Cyber Security Centre, and James M [57]
Awareness	4 (6)	• Walker [7] • Filkins et al [82] • Kaspersky Inc [58] • PCEB[a] [59]
Education	2 (3)	• Rahman et al [60] • Francis [66]
Intelligence information sharing	5 (7)	• Bouveret [46] • Winton [100] • Dobuzinskis and Finkle [101] • Scott and Wingfield [44] • Lewis [69]
Old legacy systems		
Health policy and standards	25 (36)	• Sweeney [16] • Bouveret [46] • Newman [52] • Coles-Kemp and Williams [96] • Snell [79] • Emsisoft Malware Lab [54,55] • Kruse et al [17] • Rajamäki and Pirinen [90] • The HIPAA[b] Journal [13] • Hippa [13] • Khaloufi et al [97] • Tuttle [93] • Perakslis [73] • Ponemon Institute [42,85] • Tully et al [53] • Bhuyan et al [80] • Williams and Woodward [34] • Lechner [68] • McHugh [51] • Burns et al [63] • ECRI[c] Institute [47] • Loi et al [94] • Information Commissioner's Office, National Cyber Security Centre, and James M [57] • Kaspersky Inc [58] • PCEB [59]
Lack of investment		
Partnership	3 (4)	• Baranchuk et al [72] • Raina MacIntyre et al [81] • Chua [64]

Vulnerability and knowledge application domain	Solution papers published in this domain between 2012 and 2022, n (%)	References
Complex network-connected end-point devices		
Participatory design science (sociotechnical)	1 (1)	• Coles-Kemp and Williams [96]
Network security	16 (23)	• Frost [3] • Sittig and Singh [78] • Twitter [40] • Arndt [39] • Bickers et al [102] • Ponemon Institute [42,43] • Filkins [49] • Williams and Woodward [34] • Zorabedian [103] • Sajedi and Rahbar Yaghobi [75] • Omotosho et al [76,104] • ECRI Institute [47] • Djenna et al [65] • Mohan [71] • Baranchuk et al [72] • Singh et al [77]
Encryption	4 (6)	• Mukherjee [41] • Filkins [49] • Mohan [71] • Singh et al [77]
Technological advancement (digitalization)		
Machine learning	8 (11)	• Omotosho et al [76] • Zarour et al [12] • Khaloufi et al [97] • Reshmi [10] • Faruki et al [48] • Handa et al [67] • Chen et al [105] • Sajedi and Rahbar Yaghobi [75]
Blockchain	1 (1)	• Bhuyan et al [80]
Security by design	6 (9)	• Coventry and Branley [6] • Lyon [70] • Coles-Kemp and Williams [96] • Lechner [68] • Fu and Blum [50] • Andrea [74]

[a]PECB: Professional Evaluation and Certification Board.

[b]HIPAA: Health Insurance Portability and Accountability Act.

[c]ECRI: Emergency Care Research Institute.

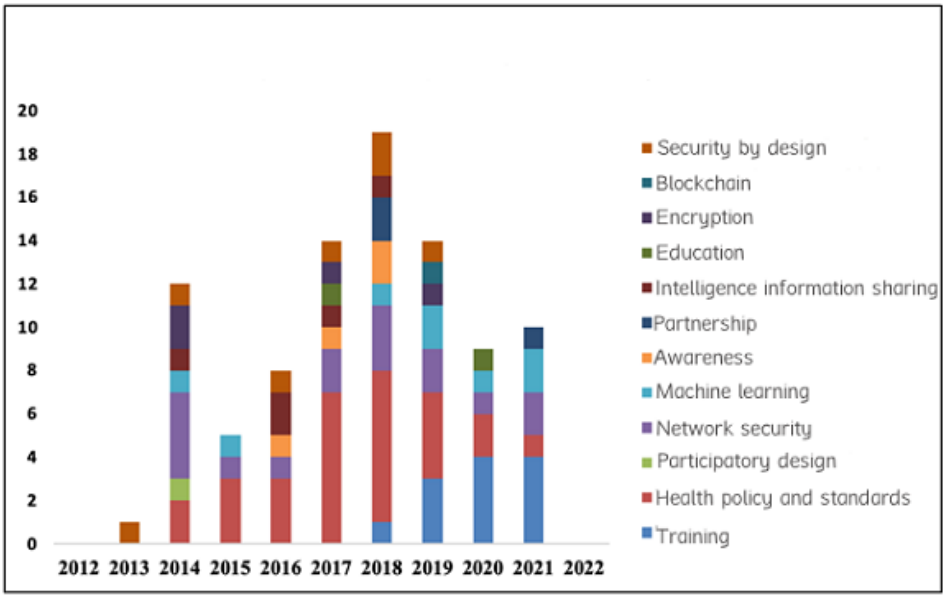
Knowledge Application Domains and Vulnerabilities

The vulnerabilities listed in Table 3 reveal that human error was associated with interventions linked to one of the knowledge application domains of training, awareness, education, and intelligence information sharing.

Training

Employee training is important to avoid human factors or error challenges in health care. Table 3 shows the proposed solutions and interventions for training from 17% (12/70) of the studies. Figure 4 shows that training emerged in 2018 at 1% and increased to its peak between 2019 and 2021. However, this finding suggests the need for cybersecurity training in health care to manage human vulnerability challenges. This need is supported by the literature highlighting the importance of cybersecurity skills and education for health care professionals [16] and the need for investment in this area [17].

Figure 4. Knowledge application areas and domain count for health care cybersecurity between 2012 and 2022.



Education

The solutions presented regarding educational intervention were derived from 3% (2/70) of the studies (Table 3). Figure 4 shows that educational solutions emerged in 2017 and declined until 2020, when studies on educational intervention emerged. This finding is supported by research that shows a lack of educational skills [16]. Organizations must invest in educational training and skills to curb social and technical cybersecurity vulnerability in health care.

Awareness

A total of 6% (4/70) of the studies in Table 3 presented solutions on awareness to address the vulnerability of human errors. This small number of studies has shown a decline and a lack of cybersecurity awareness program in health care systems. Figure 4 similarly shows that cybersecurity awareness emerged in 2016 and reached its peak at 2 studies. This has been validated by previous studies that indicate a lack of awareness programs and training [45,62].

Intelligence Information Sharing

Table 3 also shows that intelligence information sharing was a solution investigated in 7% (5/70) of the studies. It can be seen that information sharing emerged in 2014 and declined in 2015 before re-emerging in 2017 and 2018 at the rate of 1 study each year. This finding also shows that health care organizations should collaborate in training and intelligence information sharing to address cybersecurity challenges in health care.

The vulnerabilities listed in Table 3 reveal that old legacy systems were associated with interventions linked to the knowledge application domain of health policy and standards.

Health Policy and Standards

The knowledge intervention analysis indicates that 36% (25/70) of the studies acknowledged and were linked to health policy and standards (Table 3). The analysis shows that governments and health care organizations have proposed more interventions or solutions regarding health policy and standards to regulate health care organizations. The policy studies shown in Figure 4 emerged in 2014 and continued to increase to their peak in 2018. Policies such as the Health Insurance Portability and Accountability Act, the GDPR, and the Health Information Technology for Economic and Clinical Health Act to engineer has helped to mitigate data breaches and vulnerabilities in health care organizations in addressing old legacy systems to avoid sanctions and fines in case of breaches. However, full implementation or enforcement of day-to-day monitoring in hospitals or health care organizations remains challenging.

The vulnerabilities listed in Table 1 reveal that a lack of investment was associated with interventions linked to the knowledge application domain of partnership.

Partnership

Partnership is key to sustaining and protecting health care systems from cybersecurity vulnerability [72]. When organizations fail to invest in critical cyber infrastructure, skills, and partnerships with governments and expert security organizations, it is likely that they will be vulnerable to cyberattacks and breaches of health information and lack the capability to protect health care systems from the vulnerability of underinvestment. Table 3 shows that partnership solutions were provided in 4% (3/70) of the studies, whereas Figure 4 shows that partnership emerged in 2018 and declined in 2021. There is a need for health care organizations to partner for better capability and structure to protect health care systems [64].

The vulnerabilities listed in Table 1 reveal that complex network-connected end-point devices were associated with interventions linked to the knowledge application domains of participatory design, network security, and encryption.

Participatory Design

Health care organizations and medical device manufacturers must jointly participate in designing processes and systems to avoid a sociotechnical design gap. This collaboration will help protect health care systems and increase the acceptability of organizational systems and productivity. Table 3 shows only 1 pertinent study in 2014. This infer that participatory design is one of the reasons for the vulnerabilities in complex network-connected end-point devices in health care systems. Health care systems comprise a complex environment that requires a sociotechnical and collaborative approach to addressing challenges [2].

Network Security

Network security solutions were covered in 23% (16/70) of the studies (Table 3). A number of intervention solution studies were conducted in this domain. As shown in Figure 4, the first increase was observed in 2014 with 4 studies, a decline to 2 studies was observed in 2017, and then the number of studies increased to 3 before a final decline to 2 studies in 2021. These studies still attest to the vulnerability of complex network-connected end-point devices, which require increased interventions to solve health care vulnerability challenges.

Encryption

The encryption technological solution in this review was mentioned in 6% (4/70) of the studies. There was a limited number of solutions regarding encryption intervention in this review (Figure 4). Encryption only emerged in 2014 with 2 studies, and there was a gap in studies until 2017 and 2018. This finding shows that health care organizations need to implement encryption technology to protect valuable health information from breaches and attacks [77].

The vulnerabilities listed in Table 1 reveal that technology advancement (digitalization) was associated with interventions linked to the knowledge application domains of machine learning, blockchain, and security design.

Machine Learning

Machine learning is a new area in which cybersecurity in health care systems is evolving. However, solutions were provided in only 11% (8/70) of the studies (Table 3). This technology surfaced in 2014 according to Figure 4. There was only 1 study in 2014 and 2015. No solutions were provided until 2018, and the number of interventions categorized under technology advancement increased from 2019 to 2021.

Blockchain

Blockchain technology is new and still lacking solutions according to this SLR, where only 1% (1/70) of the studies showed an effective intervention. Blockchain surfaced in 2019, as shown in Figure 4. Additional solutions and interventions are needed as this area is promising and can be categorized under technology advancement (digitalization) as the key to protecting smart health care systems.

Security by Design

Security by design is a strategy that demands that health care organizations implement auto-based technology to protect digital health care systems. Table 3 shows that 9% (6/70) of the studies acknowledged security by design as a solution for technology advancement to prevent vulnerability in digital systems. Figure 4 shows studies on secure design in 2013 to 2014. There were no studies in 2015, whereas in 2016 to 2019, some studies provided interventions. There is a need for more solutions in this area to protect technological advancement or digital health care systems from vulnerability [68].

Summary of the Knowledge Application Domains and Vulnerabilities

In summary, the findings of this SLR indicate that interventions provided for the containment of health care cybersecurity vulnerabilities were limited over the past 11 years. This SLR also revealed that interventions regarding the rate of technological advancements in addressing health care cybersecurity challenges were inconsistent and lagging between 2012 and 2022. Findings also indicates that interventions in some of the mapped variables were scarce between 2012 and 2022 (Table 3). Few or no solutions are provided to address the challenges in many domains regarding health care vulnerabilities.

Discussion

Brief Summary of Findings

This SLR provided a synthesis of literature on cybersecurity in health care and identified the reasons why health care systems are vulnerable to cyberattacks. This review analyzed 70 published studies and identified 5 vulnerability themes of cybersecurity in health care systems and also proposed sociotechnical solutions for health care organizations.

The findings indicate that the extensive vulnerability of health care systems is due to internet-connected devices and software applications. Health care organizations face significant challenges, such as medical end-point device complexities and saturated wireless medical technology resulting in its difficulty in securing an interconnected technological landscape.

Importantly, many cyberattacks occur within this interconnected network without the health care organization's awareness, contributing to health information breaches.

Our findings also underscore that the crucial role of investment in health care organizations is a key panacea for addressing cyberattacks and threats. Thus, lack of investment leverages the other vulnerabilities.

In addition, this study found that lack of adequate preparation for the potential threats or vulnerability in shifting to the digitalization of health care is also a contributing factor to most successful cyberattacks on health care organizations.

We found that human activity also played a major role in subjecting health care systems to cybercrimes. The decision of humans to develop medical devices, health software applications, management systems, and processes in an effective and secured manner is vital in safeguarding health information. However, there is a bit of disconnect in the human-centric design in health care system development, most importantly during

the planning of procurement of medical technology and systems and the integration between health care organizations and stakeholders such as medical device developers, health care professionals, cybersecurity compliance officers, and system integration experts. Generally, the findings revealed that health care organizations lack adequate cybersecurity preparations during transitions to digitalization.

The findings also revealed that the health care cybersecurity knowledge application domain areas in Figure 4 depict that more intervention studies over the past 11 years were focused on health policy and standards.

In Table 4, solutions are proposed from a sociotechnical perspective to counteract cybersecurity vulnerabilities in health care organizations.

Further findings on the vulnerabilities and implications for future research are discussed in the following sections.

Table 4 is an integrated table that is presented in a stand-alone view for health care system solutions from a sociotechnical viewpoint.

To protect health care systems from attacks and vulnerabilities, as shown in Table 4, through the intervention of effective and noneffective studies, it can be seen that sociotechnical intervention studies classified invention most often and were the most effective. There are patterns and convergences between technical solutions and sociotechnical solutions in their domain of applications and solutions, such as a lack of investment, complex network-connected end-point devices, old legacy systems, and technology advancement, which lean toward interventions.

While we can consider human errors in human-computer interactions and technology usability from a human perspective, design and management can be approached through a sociotechnical perspective [96]. This approach also considers the final users of digital health care systems. Organizations would benefit from leveraging the sociotechnical solutions and guide in Table 4 in the case of cyberattacks attributed to human error by training all staff to respond using a comprehensive guide to avert cyber threats [62]. Challenges of technology, such as network-connected end-point devices and technology advancement for digitalization, should be addressed through network and security solutions and encryptions [6,67].

Hospitals with modern-day smart care should leverage their comprehensive guidelines and standard International Organization for Standardization or International Electrotechnical Commission 27001 and 27002 compliances.

Health care organizations should ensure and implement proper cyber hygiene to enable effective and efficient health care delivery processes [4,11]. They should increase their budget for critical cyber systems to address the lack of investment [17] and phase out old legacy systems by increasing investment. These actions will enable resilience and preparedness for future response plans and mitigations.

Table 4. Health care system solutions from a sociotechnical viewpoint.

Vulnerability, knowledge application domain, and description of challenge or case type	Sociotechnical lens	Effective	Not effective
Human error			
Training			
• Ransomware or email phishing attack	• Sociotechnical solution	• Train and educate health care staff to use encrypted solutions for data and virus risk register; stay up-to-date on trends of virus attacks for health care systems [4,5,57]	Review cyberattacks against hospitals worldwide via training workshops through teleconferences with experts; incorrect training approach and method of delivery via teleconference [11]
• Cyberattack on critical medical infrastructure and device breaches • Ineptitude of employees regarding cybersecurity in managing health records	• Sociotechnical solution • Sociotechnical solution	• Train and educate clinicians through simulations of hacked medical devices for patient care to heighten their awareness [8,61] • Implement training for cybersecurity culture and proactive maturity resilience via human-computer interactions [2]	Review cyberattacks against hospitals worldwide via training workshops through teleconferences with experts; incorrect training approach and method of delivery via teleconference [11]
• Insecure behavior of staff	• Social solution	• Assess behavior of health care staff regarding cybersecurity (insecure behavior) Apply AIDE[a] behavior change techniques to ensure secure behavior [56,62]	—[b]
• Health information attacks and identity theft	• Sociotechnical solution	• Provide employees with ISA[c] content development material and enhance and analyze security behavior in public and private sectors • Apply gamification • Develop prototype game and behaviorism theory and mental model for private-sector training Apply real game and ANT[d] for public-sector training [99]	—
• Protection of health care system infrastructure	• Sociotechnical solution	• Implement cybersecurity planning and training using the CERT RMM[e] [79]	—
• Low digital literacy skills of employees	• Sociotechnical solution	• Implement essential and advanced digital literacy training via computers and smart devices [98]	—
Awareness			
• Inadequate cybersecurity awareness regarding the IoMT[f] devices • Lack of data protection compliance awareness	• Sociotechnical solution	• Apply cross-situational awareness model of IoMT devices for employees and management [7] • Provide awareness training on HIPPA[g] and GDPR[h] guidelines [7,59]	—
Education			
• Employee cyberbullying • Hacking and vulnerabilities of medical devices	• Sociotechnical solution	• Provide gamification education for web-based cyberbullies [60] • Provide awareness and educational programs on the vulnerabilities of medical devices [66]	Report on pacemaker hack that led to a disconnection based on a study; the study was generalized with speculation [66]

Vulnerability, knowledge application domain, and description of challenge or case type	Sociotechnical lens	Effective	Not effective
Intelligence information sharing			
• Notification alert of threat to critical infrastructure protection • Hospital management afraid to report data breach and cyberattack to protect their image	• Social solution	• Implement threat intelligence solution [58]. • Recruit and contact compliance officer and information sharing center to report breach [46,59,100].	—
Old legacy systems			
Health policy and standards			
• How can we manage cybersecurity vulnerability risks	• Sociotechnical solution	• Implement cybersecurity risk framework [46].	—
• Our devices lack updates	• Sociotechnical solution	• Provide updates and patches for legacy systems [57]	—
• What is the lasting solution for legacy systems	• Sociotechnical solution	• Phase out legacy systems and procure devices with a security update that supports aftersales	—
• Curtailing health care breaches	• Sociotechnical solution	• Implement GDPR and HITECH[i] policy for medical devices and data [13,42,57,58,85].	—
Lack of Investment			
Partnership			
• We are concerned with the threat alerts for implanted cardiovascular medical devices. • Lack of support to manage implantable devices such as pacemakers • Managing threats with stakeholders to protect patients	• Sociotechnical solution	• Ensure security in design from manufacturers and partners for aftersales support to ensure updates with remote monitoring or interrogation [72] • Ensure a partnership for a safer cardiovascular implantable device with the manufacturer's electronic device and follow FDA[j] and NIST-CSF[k] guidelines [72] • Health care organization should partner and implement HICP[l] guidance [64]	Developed new biosecurity risk methods and surveillance tools from traditional methods; they lack validation [81]
Complex network-connected end-point devices			
Participatory design science (sociotechnical)			
• Information security design gap challenges for health care systems	—	• Resolve information security design reality gap using the ITPOSOM[m] framework by Heeks [96] and through collaboration [65].	—
Network security			

Vulnerability, knowledge application domain, and description of challenge or case type	Sociotechnical lens	Effective	Not effective
• Insecurity of connected medical devices in protecting health information • Managing network security for IoMT devices	• Sociotechnical solution	• Install extreme network defenders to secure the network and manage IoMT devices [3]	Health record breaches in Australia are reportedly sold on the dark web; the study does not offer a solution [102]
• Attack on critical health care cyber infrastructure	—	• Develop a collaborative security approach and cybersecurity guidelines [65]	—
• Managing complex health care network access control and authentication	• Technical solution	• Implement the attribute trust framework for aggregation of user attributes in a reputation system [71]	—
• Protection of EHRs[n] for patient safety challenge	• Sociotechnical solution	• Apply the 3-phase e-PSG[o] framework [78]	—
Encryption			
• Protection of IoT[p] devices from breaches and being compromised	• Technical solution	• Secure IoT devices through FHSS[q] and RSSI[r] techniques [77]	Anthem's insurance health record breach report; investigation revealed that a foreign government was behind the attack, which is speculation without evidence-based facts [41]
• Managing cloud security concerns • Managing employee and patient devices on the health care network	• Sociotechnical solution	• Assure investment and compliance with regulatory standards and monitoring • Implement policy on BYOD[s] and apply all-layer multifactor protections for cloud systems [49]	—
• Protecting sensitive health care data and exchange between the EHR and the cloud-based database	• Technical solution	• Encrypt data using lightweight cryptographic protocols; store on the cloud-based PHR[t] [71]	—
Technology advancement (digitalization)			
Machine learning			
• Protecting health care systems from ransomware and other malware attacks • Managing health care big data challenges	• Technical solution	• Implement antimalware solutions using the dynamic method [10] • Implement a big data life cycle model using blockchain [80,97]	Adopting clusters to split the OCSVM[u] machine learning algorithm; however, the study does not offer a preventative solution [67]
Blockchain			
• How can we secure health information and personal identifiable information to enable privacy and security	• Technical solution	• Implement information-hiding algorithms using blockchain technology [80,97]	—
Secure design			

Vulnerability, knowledge application domain, and description of challenge or case type	Sociotechnical lens	Effective	Not effective
• Formidable medical device protection • Protecting health care ecosystems	• Sociotechnical solution	• Build in security from design planning and compliance [47,68,96] • Implement stakeholder collaborative design using sociotechnical behavior [65,96]	Security trade-off on safer medical devices for patients with diabetes; proposed improvement plans are not yet implemented [70]

[a]AIDE: Assess, Identify, Develop, and Evaluate.

[b]Not applicable.

[c]ISA: information security awareness.

[d]ANT: actor-network theory.

[e]CERT RMM: Computer Emergency Response Team Resilience Management Model.

[f]IoMT: Internet of Medical Things.

[g]HIPAA: Health Insurance Portability and Accountability Act.

[h]GDPR: General Data Protection Regulation.

[i]HITECH: Health Information Technology for Economic and Clinical Health.

[j]FDA: Food and Drug Administration.

[k]NIST-CSF: National Institute of Standards and Technology Cybersecurity Framework.

[l]HICP: Health Industry Cybersecurity Practices.

[m]ITPOSOM: information, technology, processes, objectivity and values, skills and knowledge, management systems and structure, and other resources.

[n]EHR: electronic health record.

[o]e-PSG: electronic health record–specific patient safety goals.

[p]IoT: Internet of Things.

[q]FHSS: frequency-hopping spread spectrum.

[r]RSSI: received signal strength indicator.

[s]BYOD: bring your own device.

[t]PHR: personal health record.

[u]OCSVM: one-class support vector machine.

Implications for Future Research

Overview

Health care sectors have improved with policies and measures developed to control health information breaches and vulnerabilities. However, further research is needed in social and technical interception design, namely, the human factor. Managing complex end-point devices and investment on addressing health care vulnerability and breaches should be considered from a sociotechnical design and sustainability perspective.

Protecting Complex Network-Connected End-Point Devices

The protection of complex network-connected end-point devices for health care organizations involves several key measures. The network of interconnected medical end-point devices and the software systems that connect to the internet are becoming vulnerable to attacks and breaches. This is a growing issue; health care organizations tend to procure medical device technology without proper equipment planning and guidelines in place. This implies that security is overlooked and is not a major focus area. Examples include hospital beds connected to >10 medical devices, such as pulse oximeters, syringe pumps, and patient care monitors, which are connected devices and vulnerable to attacks [2,6].

To address this technical challenge, organizations can concentrate on developing advanced threat detection and mitigation techniques, such as network defenders tailored to intricate network-connected end-point devices in health care and the integration of artificial intelligence using machine learning algorithms to effectively identify and respond to emerging threats. Furthermore, the health care industry must take a sociotechnical approach [96] toward implementing standard guidelines and technical solutions via the protection of health care networks through planning and integrating network security protection and segmentation. In addition, health information exchange over the network should undergo steganography and encryption as a solution using blockchain technology. Therefore, the integration of a complex end-point medical device should use built-in security with alert response and communication in processes to monitor health care cybersecurity ecosystems for a healthy security posture.

Health care organizations should collaborate with security experts and health care professionals and implement user education and incidence response to catalog cyber vulnerability incidences for further analysis. The implication is that, if networks and end-point medical devices are not properly secured, this will lead to breaches of health information through the network, which will cause patient information to be hijacked by cybercriminals for political gains. Sponsored state actors may use this weakness to seize networks and systems of care

delivery, demanding money from an organization before the latter can regain access. This approach will expose the health information of patients while they are receiving treatment and accessing health care services. This is an evolving challenge of the digital consequences of connected care. Building security through a design solution should be achieved from a sociotechnical approach as the human is the final user of systems of care.

Future research should focus on security by design before integrations of complex technology and design a simpler flow process with the disaggregation of complex network connections.

Increasing Investment in Cybersecurity

Investment in health care systems is critical to ensure the proper safeguarding of health care ecosystems from cyberattacks and vulnerabilities. To ensure efficient and secure health care, organizations should invest in human capital and technology to function effectively. An evaluation through research reveals that health care is lagging behind other sectors in terms of investment. This finding was confirmed by Kruse et al [17], who found that only 5% of health care investment is earmarked to protect health care, whereas a large percentage is allocated for health care delivery.

Insufficient investment in cybersecurity experts, awareness, and investment partnership plans will continue to subject health care employees to insecure behavior and result in a health care organization that is unprepared to mitigate cyber threats and other tactics used by attackers to disrupt evolving health care trends and patterns, particularly ransomware attacks.

Similarly, old legacy systems pose another security risk. Malicious actors can continue to exploit these systems to expose personal health information due to their limited capabilities and outdated organizational structure. Such vulnerability is worsened by a lack of investment in new cybersecurity infrastructure and computer devices to protect or process health information in a secure manner.

Health care organizations can engage in partnership with medical technology providers, application developers, and network solution integrators to develop strong systems and structures with seamless integration. Health care organizations should also develop and implement a framework for prioritizing cybersecurity investment based on risk assessments and threat intelligence. This approach can help identify the most critical areas of vulnerability within different departments, aiding organizations and policy makers in directing investments where they are most needed. Health care organizations should invest in humans and technology through training to ensure the development of necessary skills and investment in critical cyber infrastructure.

Awareness campaigns for patients and staff will help organizations recover from errors and breaches, whereas investment in technological security systems for health care will prepare health care organizations with the appropriate structure and system for resilience.

The findings presented in this paper are also highlighted in Table 4. Investment challenges in health care cybersecurity should focus on a sociotechnical approach that involves human behavior, technology, and organizational processes and should not be segregated as a separate technical or social problem. Future research should focus on security and investment in smart health care for attaining sustainability and resilience.

Managing Technological Advancement

Health care industries and organizations have improved over the years and are continuing to forge the development of new capabilities, technological advances, and processes to manage the multifaceted challenges of health care cybersecurity. Complexity in technology advancement and networks of digital systems increase the number of attack surfaces, where cybercriminals take advantage of the digital gateway access and execute malicious software programmed with code, such as malware to compromise digital technology and health care system networks. However, technological development necessitates a proactive approach to cybersecurity, particularly when considering security-by-design principles.

Future research projects must concentrate on important areas to protect networks, systems, and applications against vulnerabilities. Health care organizations should collaborate with medical device manufacturers as part of the planning phase of procurement requirements to ensure specifications needs before the development of medical devices technology for seamless integration. Implanted devices, for instance, should be built with security by design and continuously updated when necessary. A 2-factor authentication security for critical medical technology is also necessary. In addition, it is important that health care organizations quantify the risk, ensure that proper National Institute of Standards and Technology and GDPR standard guidelines are followed, and conduct threat modeling and simulation to evaluate the protectability of health care systems as a guideline in managing cybersecurity vulnerability.

Collaborative (sociotechnical) efforts among academia, industry, and policy makers are essential to drive this research agenda forward and create a safer digital landscape for the future.

The technology procurement requirement and collaboration should consider the integration of social and technical processes during digital technology development with health care delivery processes.

Health care organizations can adopt a blockchain technology solution for the protection of health information and other applications such as EHR systems from malicious use and insider threats.

Future research should examine the use of blockchain for health care big data protection and processes to manage cybersecurity vulnerability.

Containing Human Error in Cybersecurity

Humans are at the receiving end of the cyberattack chain. An example is the case of the WannaCry attack that affected 150,000 computers. It was attributed to human error because humans were warned of the attack on Windows server legacy systems but they ignored the warning by clicking on malicious

email links [38,43]. When an organization fails to train humans, cybercriminals take advantage of human weakness to exploit health care systems. Today, medical device manufacturers are building devices without considering humans as the final users or a participatory (sociotechnical) design approach. This is one factor of the clinical process and security dimension to protect critical infrastructure. Another factor is that, if a system is developed and does not start with security and support human usability, it becomes stressful for a human user to navigate the systems, which could cause them techno-stress, with the likelihood of mistakes. The health sector should use the Assess, Identify, Develop, and Evaluate technique to identify areas of human weakness, develop a new training method through simulations, and offer gamification training on issues such as phishing email deception and ransomware attacks. The implication is that, if humans are not trained, they will lead organizations to disaster because cybercriminals will continue to exploit the weakness of humans to cause more damage to health care systems. The consequences will include legal issues, fines, and possibly bankruptcy for health care organizations. Proper training and awareness campaigns should be implemented. Future research should focus on developing futuristic health care cybersecurity curriculums and training.

Practical Implications

Inadequate systems will cause health care systems and organizations to face increasing cyberattacks and setbacks in health information and patient safety. Moreover, a new trend reveals that, if implanted medical devices and technology are not protected, humans will be targeted by hackers seeking to make money or gain political power for ransom. However, implementation and adoption of the medical device security life cycle model [68] will protect medical devices, health information, patients, and organizations from harm and against future emerging threats. Thus, there is a need for the design of a cybersecurity sociotechnical framework toward sustaining smart health care systems.

Comparison With Prior Work

Previous narrative literature reviews by Coventry and Branley [6] and Mohan et al [31] highlight the need for an integrated approach in health care systems to address cybersecurity vulnerabilities. They emphasize the need for a comprehensive approach that connects human behavior, technology, and processes in a holistic way as a best strategy to tackle vulnerabilities, although the authors did not classify human behavior, technology, and processes from a sociotechnical lens. This systematic review supports their view by building and extending the literature on cybersecurity case challenge descriptions in all the tables in this paper to integrate human behavior, technology, and processes as a sociotechnical approach [2,23,26-28]. For example, an SLR conducted by Offner et al [2] reported that health care system vulnerability is a complex sociotechnical problem. Furthermore, for a health care organization to build resilience against cyberattacks and threats to avoid cybersecurity design gaps and vulnerabilities in the health care system, a strategic approach that integrates people, technology, and processes must be adopted [23,27,31]. The aforementioned aligns with the approach adopted in this study. Different schools of thought have highlighted the key importance of investment in technology and humans to protect health care systems from cyberattacks and threats [6,8,11,19,36,56]. This corroborates our findings that cybersecurity investment plays a main role in health care systems.

This study also revealed that complex network-connected end-point devices were mentioned several times by different schools of thought. Moreover, existing literature has opined that complex network-connected end-point devices were the most mentioned vulnerability [5,17,18,35,53].

Furthermore, technology advancement through a digital transformation evolution has created precision, and managed health care delivery [32,94]. However, more effort is still required in designing security features in health care technology. This study highlighted that security by design is required for medical device technology in health care systems [9,34,68].

Health care organizations must ensure that the design of technology evolves with a secure design approach from conception to avoid breaches of health information by external and internal attackers [24,32,68].

The sociotechnical solutions in Table 4 will aid health care organizations in being resilient in dealing with vulnerabilities and cybersecurity breaches in health care systems through a comprehensive and holistic approach. The sociotechnical perspective defines the meaning and constructs of technology, humans and processes [6,19,31,36,37]. This approach is promising and effective in dealing with health care system and cybersecurity vulnerabilities.

Limitations

For this study, non–English-language articles on cybersecurity and health care were not included. Closed-access articles directly related to cybersecurity and health care were also not included. Textbooks linked to cybersecurity and health care were excluded. In addition, as cybersecurity is a broad topic, more time was needed for data analysis.

Conclusions

This study conducted an SLR (PRISMA guidelines) to investigate the body of literature on cybersecurity in health care systems because of the exponential increase in health information breaches and vulnerability issues surrounding medical device technology and networks. This study also examined why health care systems are vulnerable to cyberattacks and threats.

In this review, sociotechnical solutions and mitigation strategies were proposed to protect patient health information, medical devices, and the critical cyber infrastructure of health care organizations from attacks and threats. We identified human error, lack of investment, complex network-connected end-point devices, old legacy systems, and technological advancement due to rapid digitalization as the causes of data breaches and the vulnerability of digital health care systems to attacks and threats. This study also revealed that research in the areas of education, awareness, training, collaborative partnerships, blockchain, and machine learning for health care cybersecurity

is underrepresented. In addition, there was inconsistency in the publication of intervention studies. There is a gap in intervention studies published between 2012 and 2013, as shown in this SLR, as well as breaks in research publications between 2012 and 2022, as illustrated in Table 3 and Figure 4.

As shown in Table 1, of the 70 papers published between 2012 and 2022 and reviewed in this study, only 8 (11%) carried out research in the areas of human error–related perspectives where health care systems are vulnerable to attacks. This finding clearly shows that considerably more studies are required on human factors. We also identified from this review that network-connected end-point devices are the most vulnerable challenge that causes health information breaches. However, stakeholders have rolled out interventions in the areas of health policy, health care system support (network security), and training. The support and training target operational activities and health care delivery while investment in cybersecurity critical infrastructure is disregarded. Rapid technology advancement has resulted to an increasing risk of cyberattacks and threats because most manufactured connected medical devices were not built with security in mind. With the possible sociotechnical solutions in Table 4, we form conclusions about how to protect health care systems as a sociotechnical solution in relation to the gap in research on technology, human behavior, and processes.

Health care organizations must concede that efficient and effective cybersecurity cannot be addressed with a technological process only but must also evolve beyond technological operation to a sociotechnical process that calls for a comprehensive knowledge of the human elements.

The profound implication of our findings steps further from just the concept of security. It deems it necessary for a major change in the approach to health care security by shifting from a reactive measure of patching and mitigation toward an approach of proactiveness and integration of detailed mechanisms that depend on complex sociotechnical dynamics at play in the design and development processes across the health care systems.

Our review emphasized the importance of a mandatory collaboration and cross-disciplinary engagement among stakeholders in health care, technology policy, and academia. The inclusion of a team-based effort from stakeholders will foster an integrated solution that responds to the challenges of cybersecurity vulnerabilities in health care systems.

In addition, our findings also give prominence to the great significance of investment in health care systems, such as in cybersecurity technology, medical devices, networks, health care professionals, and cybersecurity professionals, in advancing health care organizations. Furthermore, investment is imperative in cybersecurity education and training programs that will provide health care professionals and organizations with the updated knowledge and skills to navigate the complexities of cybersecurity vulnerabilities constructively. Governments should provide additional financial incentives for health care organizations to facilitate cybersecurity sustainability in health care systems. Future research should explore the application of blockchain technology for safeguarding health care system data. Blockchain offers a secure decentralized architecture. Therefore, system developers should consider a human-centric design approach when integrating blockchain technology into health care systems.

By strengthening awareness culture, intelligence information sharing, and accountability in health care systems, health care organizations can equip their operations and workforce to become active front-runners in safeguarding patient data and health care critical infrastructure and assuring the confidentiality, availability, and integrity of health care systems. Consequently, our SLR implores for an exhaustive procedure regarding cybersecurity in health care that affirms and entwines the sociotechnical nature of the vulnerabilities and challenges. By merging a technical approach with human-centric strategies, health care organizations can protect health care systems from vulnerabilities and cyber threats and advance a culture of resilience, trust, and innovation in health care service delivery. The implications of this review present a sociotechnical solution for establishing more secure and resilient health care ecosystems. This paper provides health care organizations with a better understanding of and resilience to cyberattacks, threats, and vulnerabilities.

Acknowledgments

The author is grateful to the Finnish Cultural Foundation and University of Vaasa in Finland for their support in funding this research.

Conflicts of Interest

None declared.

Multimedia Appendix 1

PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) checklist guide.
[PDF File (Adobe PDF File), 118 KB-Multimedia Appendix 1]

Multimedia Appendix 2

Search strategy.
[DOCX File , 15 KB-Multimedia Appendix 2]

References

1. Cybersecurity in healthcare. Health Insurance Portability and Accountability Act. URL: https://www.himss.org/resources/cybersecurity-healthcare [accessed 2024-05-05]
2. 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. Intell National Secur. Apr 22, 2020;35(4):556-585. [FREE Full text] [doi: 10.1080/02684527.2020.1752459]
3. Frost. Medical Device and Network Security Coming to terms with the Internet of Medical Things (IoMT). -. 2024:2019. [FREE Full text]
4. Karambelas C. Healthcare care technology: ransomware risk and protection. Am Bankruptcy Inst J. May 2020;39(5):30.
5. Giansanti D. Cybersecurity and the digital-health: the challenge of this millennium. Healthcare (Basel). Jan 11, 2021;9(1):62. [FREE Full text] [doi: 10.3390/healthcare9010062] [Medline: 33440612]
6. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas. Jul 2018;113:48-52. [FREE Full text] [doi: 10.1016/j.maturitas.2018.04.008] [Medline: 29903648]
7. Walker T. Interoperability a must for hospitals, but it comes with risks. Managed Healthcare Executive. Dec 10, 2017. URL: https://www.managedhealthcareexecutive.com/view/interoperability-must-hospitals-it-comes-risks [accessed 2024-05-06]
8. Dameff CJ, Selzer JA, Fisher J, Killeen JP, Tully JL. Clinical cybersecurity training through novel high-fidelity simulations. J Emerg Med. Feb 2019;56(2):233-238. [FREE Full text] [doi: 10.1016/j.jemermed.2018.10.029] [Medline: 30553562]
9. Klonoff DC. Cybersecurity for connected diabetes devices. J Diabetes Sci Technol. Apr 16, 2015;9(5):1143-1147. [FREE Full text] [doi: 10.1177/1932296815583334] [Medline: 25883162]
10. Reshmi TR. Information security breaches due to ransomware attacks - a systematic literature review. Int J Inf Manag Data Insights. Nov 2021;1(2):100013. [FREE Full text] [doi: 10.1016/j.jjimei.2021.100013]
11. 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. Jan 11, 2019;19(1):10. [FREE Full text] [doi: 10.1186/s12911-018-0724-5] [Medline: 30634962]
12. Zarour M, Alenezi M, Ansari MT, Pandey AK, Ahmad M, Agrawal A, et al. Ensuring data integrity of healthcare information in the era of digital health. Healthc Technol Lett. Jun 2021;8(3):66-77. [FREE Full text] [doi: 10.1049/htl2.12008] [Medline: 34035927]
13. What are the penalties for HIPAA violations? The HIPAA Journal. URL: https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/ [accessed 2024-05-06]
14. Mcnulty M, Kettani H. On cybersecurity education for non-technical learners. In: Proceedings of the 3rd International Conference on Information and Computer Technologies (ICICT). 2020. Presented at: ICICT 2020; March 9-12, 2020; San Jose, CA. URL: https://doi.org/10.1109/ICICT50521.2020.00072 [doi: 10.1109/icict50521.2020.00072]
15. Ricci J, Breitinger F, Baggili I. Survey results on adults and cybersecurity education. Educ Inf Technol. Jul 11, 2018;24(1):231-249. [FREE Full text] [doi: 10.1007/s10639-018-9765-8]
16. Sweeney E. Healthcare data breaches haven't slowed down in 2017, and insiders are mostly to blame. Fierce Healthcare. Aug 3, 2017. URL: https://tinyurl.com/yn2m49y8 [accessed 2024-05-06]
17. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care. Feb 21, 2017;25(1):1-10. [FREE Full text] [doi: 10.3233/thc-161263]
18. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: review (for the non-cyber professional). Front Digit Health. 2022;4:862221. [FREE Full text] [doi: 10.3389/fdgth.2022.862221] [Medline: 36033634]
19. Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S. Health care and cybersecurity: bibliometric analysis of the literature. J Med Internet Res. Feb 15, 2019;21(2):e12644. [FREE Full text] [doi: 10.2196/12644] [Medline: 30767908]
20. Healthcare data breach statistics. The HIPAA Journal. URL: https://www.hipaajournal.com/healthcare-data-breach-statistics/#:~:text=2021%20was%20a%20bad%20year,stolen%2C%20or%20otherwise%20impermissibly%20disclosed [accessed 2024-05-06]
21. IBM report: cost of a data breach hits record high during pandemic. IBM. Jul 28, 2021. URL: https://tinyurl.com/euc26j9y [accessed 2024-05-06]
22. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors (Basel). Jul 28, 2021;21(15):5119. [FREE Full text] [doi: 10.3390/s21155119] [Medline: 34372354]
23. Heeks R. Health information systems: failure, success and improvisation. Int J Med Inform. Feb 2006;75(2):125-137. [FREE Full text] [doi: 10.1016/j.ijmedinf.2005.07.024] [Medline: 16112893]
24. Casola V, De Benedictis A, Rak M, Villano U. Security-by-design in multi-cloud applications: an optimization approach. Inf Sci. Jul 2018;454-455:344-362. [FREE Full text] [doi: 10.1016/j.ins.2018.04.081]
25. Secure-by-design: shifting the balance of cybersecurity risk: principles and approaches for secure by design software. Cybersecurity and Infrastructure Security Agency. Oct 25, 2023. URL: https://www.cisa.gov/resources-tools/resources/secure-by-design [accessed 2024-05-06]

26. Mumford E. The story of socio‐technical design: reflections on its successes, failures and potential. Inf Syst J. Sep 04, 2006;16(4):317-342. [FREE Full text] [doi: 10.1111/j.1365-2575.2006.00221.x]
27. Palvia SC, Sharma RS, Conrath DW. A socio-technical framework for quality assessment of computer information systems. Ind Manag Data Syst. 2001;101(5):237-251. [FREE Full text] [doi: 10.1108/02635570110394635]
28. Atkinson C, Eldabi T, Paul RJ, Pouloudi A. Investigating integrated socio-technical approaches to health informatics. In: Proceedings of the 34th Annual Hawaii International Conference on System Sciences. 2001. Presented at: HICSS 2001; January 6, 2001; Maui, HI. URL: https://doi.org/10.1109/HICSS.2001.926578 [doi: 10.1109/hicss.2001.926578]
29. Altman R. Informatics in the care of patients: ten notable challenges. West J Med. Feb 1997;166(2):118-122. [FREE Full text] [Medline: 9109328]
30. Coiera E. Four rules for the reinvention of health care. BMJ. May 15, 2004;328(7449):1197-1199. [FREE Full text] [doi: 10.1136/bmj.328.7449.1197] [Medline: 15142933]
31. Mohan DN, Gowda SS, Vikyath IS. Cyber security in health care. Int J Res Eng Sci Manag. 2020;3(1):551-553. [doi: 10.47607/ijresm]
32. Luna R, Rhine E, Myhra M, Sullivan R, Kruse CS. Cyber threats to health information systems: a systematic review. Technol Health Care. Jan 27, 2016;24(1):1-9. [FREE Full text] [doi: 10.3233/thc-151102]
33. Jalali MS, Russell B, Razak S, Gordon WJ. EARS to cyber incidents in health care. J Am Med Inform Assoc. Jan 01, 2019;26(1):81-90. [FREE Full text] [doi: 10.1093/jamia/ocy148] [Medline: 30517701]
34. Williams P, Woodward A. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices Evid Res. Jul 2015;8:305-316. [FREE Full text] [doi: 10.2147/mder.s50048]
35. Safavi S, Meer AM, Melanie EK, Shukur Z. Cyber vulnerabilities on smart healthcare, review and solutions. In: Proceedings of the Cyber Resilience Conference (CRC). 2018. Presented at: CR 2018; November 13-15, 2018; Putrajaya, Malaysia. URL: https://doi.org/10.1109/CR.2018.8626826 [doi: 10.1109/cr.2018.8626826]
36. He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. J Med Internet Res. Apr 20, 2021;23(4):e21747. [FREE Full text] [doi: 10.2196/21747] [Medline: 33764885]
37. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res. May 28, 2018;20(5):e10059. [FREE Full text] [doi: 10.2196/10059] [Medline: 29807882]
38. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. Mar 29, 2021;372:n71. [FREE Full text] [doi: 10.1136/bmj.n71] [Medline: 33782057]
39. Arndt RZ. For epic, interoperability comes from within. Modern Healthcare. Jan 29, 2018. URL: https://www.modernhealthcare.com/article/20180130/NEWS/180139993/for-epic-interoperability-comes-from-within [accessed 2024-05-06]
40. Incident detection, email attacks continue to cause headaches for companies. Twitter. URL: https://twitter.com/SandraProske/status/967893399599796224 [accessed 2024-05-06]
41. Mukherjee SY. Anthem's historic 2015 health records breach was likely ordered by a foreign government. Fortune. Jan 10, 2017. URL: https://fortune.com/2017/01/09/anthem-cyber-attack-foreign-government/ [accessed 2024-05-06]
42. 2017 cost of data breach study: United States. Ponemon Institute. Jun 13, 2017. URL: https://www.ponemon.org/news-updates/blog/security/2017-cost-of-data-breach-study-united-states.html [accessed 2024-05-06]
43. Cost of a data breach report 2021. IBM Security. URL: https://info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF [accessed 2024-05-06]
44. Scott M, Wingfield N. Hacking attack has security experts scrambling to contain fallout. New York Times. May 13, 2017. URL: https://tinyurl.com/4weatd6e [accessed 2024-05-06]
45. Gordon WJ, Wright A, Glynn RJ, Kadakia J, Mazzone C, Leinbach E, et al. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. J Am Med Inform Assoc. Jun 01, 2019;26(6):547-552. [FREE Full text] [doi: 10.1093/jamia/ocz005] [Medline: 30861069]
46. Bouveret A. Cyber risk for the financial sector: a framework for quantitative assessment. SSRN. Preprint posted online July 16, 2018. [FREE Full text] [doi: 10.2139/ssrn.3203026]
47. Top 10 health technology hazards for 2016. ECRI Institute. Nov 2015. URL: https://www.ecri.org/Resources/Whitepapers_and_reports/2016_Top_10_Hazards_Executive_Brief.pdf [accessed 2024-05-06]
48. Faruki P, Bharmal A, Laxmi V, Ganmoor V, Singh Gaur M, Conti M, et al. Android security: a survey of issues, malware penetration, and defenses. IEEE Commun Surv Tutorials. 2015;17(2):998-1022. [FREE Full text] [doi: 10.1109/comst.2014.2386139]
49. Filkins B. Health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon. SANS Institute. 2014. URL: https://asprtracie.hhs.gov/technical-resources/resource/3381/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-on-horizon [accessed 2024-05-06]
50. Fu K, Blum J. Controlling for cybersecurity risks of medical device software. Commun ACM. Oct 2013;56(10):35-37. [FREE Full text] [doi: 10.1145/2508701]
51. McHugh M. Medical device software and technology: the past, present and future. BEAI Spectrum, Biological and Clinical Engineers Association of Ireland. 2015. URL: https://arrow.tudublin.ie/scschcomart/38/ [accessed 2024-05-06]

52. Newman LH. Medical devices are the next security nightmare. WIRED. Mar 2, 2017. URL: https://www.wired.com/2017/03/medical-devices-next-security-nightmare/ [accessed 2024-05-06]
53. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health Secur. 2020;18(3):228-231. [FREE Full text] [doi: 10.1089/hs.2019.0123] [Medline: 32559153]
54. The state of ransomware in the US: report and statistics 2019. Emsisoft Malware Lab. Dec 12, 2019. URL: https://tinyurl.com/ykx5zjce [accessed 2024-05-06]
55. The state of ransomware in the US: report and statistics 2020. Emsisoft Malware Lab. Jan 18, 2021. URL: https://www.emsisoft.com/en/blog/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/ [accessed 2024-05-06]
56. Branley-Bell D, Coventry L, Sillence E, Magalini S, Mari P, Magkanaraki A, et al. Your hospital needs you: eliciting positive cybersecurity behaviours from healthcare staff. Ann Disaster Risk Sci. 2020;3(1). [FREE Full text] [doi: 10.51381/adrs.v3i1.51]
57. Information Commissioner's Office, National Cyber Security Centre, James M. New figures show large numbers of businesses and charities suffer at least one cyber attack in the past year. United Kingdom Government. Apr 25, 2018. URL: https://www.gov.uk/government/news/new-figures-show-large-numbers-of-businesses-and-charities-suffer-at-least-one-cyber-attack-in-the-past-year [accessed 2024-05-06]
58. IT security in the era when everything can be hacked. Kaspersky Lab. URL: https://www.unodc.org/documents/organized-crime/cybercrime/cybercrime-april-2018/RUSSIAN_FED.pdf [accessed 2024-05-06]
59. GDPR: getting ready for the new EU data protection regulation. PECB Insights. Apr 27, 2018. URL: https://insights.pecb.com/gdpr-compliance-getting-ready/ [accessed 2024-05-06]
60. Rahman NA, Sairi IH, Zizi NA, Khalid F. The importance of cybersecurity education in school. Int J Inf Educ Technol. 2020;10(5):378-382. [FREE Full text] [doi: 10.18178/ijiet.2020.10.5.1393]
61. Chowdhury N, Gkioulos V. Cyber security training for critical infrastructure protection: a literature review. Comput Sci Rev. May 2021;40:100361. [FREE Full text] [doi: 10.1016/j.cosrev.2021.100361]
62. Coventry L, Branley-Bell D, Sillence E, Magalini S, Mari P, Magkanaraki A, et al. Cyber-risk in healthcare: exploring facilitators and barriers to secure behaviour. In: Proceedings of the HCI for Cybersecurity, Privacy and Trust 2020. 2020. Presented at: HCI-CPT 2020; July 19-24, 2020; Copenhagen, Denmark. URL: https://tinyurl.com/v2dbyrsx [doi: 10.1007/978-3-030-50309-3_8]
63. Burns AJ, Johnson ME, Honeyman P. A brief chronology of medical device security. Commun ACM. Sep 22, 2016;59(10):66-72. [FREE Full text] [doi: 10.1145/2890488]
64. Chua JA. Cybersecurity in the healthcare industry - A collaborative approach. American Association for Physician Leadership. Jan 8, 2021. URL: https://www.physicianleaders.org/articles/cybersecurity-healthcare-industry-collaborative-approach [accessed 2024-05-06]
65. Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: new concern cyber security issues of critical cyber infrastructure. Appl Sci. May 17, 2021;11(10):4580. [FREE Full text] [doi: 10.3390/app11104580]
66. Francis R. Medical devices that could put you at security risk. IDG Communications. Apr 27, 2017. URL: https://www.csoonline.com/article/561347/medical-devices-that-could-put-you-at-security-risk.html [accessed 2024-05-06]
67. Handa A, Sharma A, Shukla SK. Machine learning in cybersecurity: a review. WIREs Data Min Knowl. Feb 17, 2019;9(4):e1306. [FREE Full text] [doi: 10.1002/widm.1306]
68. Lechner NH. Developing a compliant cybersecurity process for medical devices. In: Proceedings of the Central European Conference on Information and Intelligent Systems. 2018. Presented at: CECIIS 2018; September 19-21, 2018; Varaždin, Croatia. URL: https://www.proquest.com/openview/8a2a254a80f34ef64b55c71d5bac01d6/1?pq-origsite=gscholar&cbl=1986354
69. Lewis CJ. Cybersecurity in healthcare. Utica College. 2014. URL: https://tinyurl.com/3usz5jat [accessed 2024-05-16]
70. Lyon D. Making trade-offs for safe, effective, and secure patient care. J Diabetes Sci Technol. Mar 2017;11(2):213-215. [FREE Full text] [doi: 10.1177/1932296816676281] [Medline: 28264187]
71. Mohan A. Cyber security for personal medical devices internet of things. In: Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems. 2014. Presented at: DCOSS 2014; May 26-28, 2014; Marina Del Rey, CA. URL: https://doi.org/10.1109/DCOSS.2014.49 [doi: 10.1109/dcoss.2014.49]
72. Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutyifa V, et al. Cybersecurity for cardiac implantable electronic devices: what should you know? J Am Coll Cardiol. Mar 20, 2018;71(11):1284-1288. [FREE Full text] [doi: 10.1016/j.jacc.2018.01.023] [Medline: 29475627]
73. Perakslis E. Cybersecurity in health care. N Engl J Med. Jul 31, 2014;371(5):395-397. [FREE Full text] [doi: 10.1056/nejmp1404358]
74. Peterson A. Yes, terrorists could have hacked Dick Cheney's heart. The Washington Post. Oct 21, 2013. URL: https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/ [accessed 2024-05-06]
75. Sajedi H, Rahbar Yaghobi S. Information hiding methods for E-Healthcare. Smart Health. Mar 2020;15:100104. [FREE Full text] [doi: 10.1016/j.smhl.2019.100104]

76. Omotosho A, Adegbola O, Mikail OO, Emuoyibofarhe J. A secure electronic prescription system using steganography with encryption key implementation. Int J Comput Inform Technol. Sep 2014;03(5):980-986. [doi: 10.48550/arXiv.1502.01264]
77. Singh Rayat A, Singh I, Singh K. Review on security challenges of data communication in IoT devices. Int J Electron Eng. 2019;11(2):406-415. [FREE Full text]
78. Sittig DF, Singh H. Electronic health records and national patient-safety goals. N Engl J Med. Nov 08, 2012;367(19):1854-1860. [FREE Full text] [doi: 10.1056/nejmsb1205420]
79. Snell E. Healthcare data breach costs highest for 7th straight year. Health IT Security. 2017. URL: https://healthitsecurity.com/news/healthcare-data-breach-costs-highestfor-7th-straight-year [accessed 2024-05-06]
80. 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. Apr 02, 2020;44(5):98. [FREE Full text] [doi: 10.1007/s10916-019-1507-y] [Medline: 32239357]
81. Raina MacIntyre C, Engells TE, Scotch M, Heslop DJ, Gumel AB, Poste G, et al. Converging and emerging threats to health security. Environ Syst Decis. 2018;38(2):198-207. [FREE Full text] [doi: 10.1007/s10669-017-9667-0] [Medline: 32288980]
82. Filkins BL, Kim JY, Roberts B, Armstrong W, Miller MA, Hultner ML, et al. Privacy and security in the era of digital health: what should translational researchers know and do about it? Am J Transl Res. 2016;8(3):1560-1580. [FREE Full text] [Medline: 27186282]
83. Rodrigues JJ, de la Torre I, Fernández G, López-Coronado M. Analysis of the security and privacy requirements of cloud-based electronic health records systems. J Med Internet Res. Aug 21, 2013;15(8):e186. [FREE Full text] [doi: 10.2196/jmir.2494] [Medline: 23965254]
84. -. Verizon: 2019 data breach investigations report. Comput Fraud Secur. Jan 2019;2019(6). [doi: 10.1016/S1361-3723(19)30060-0]
85. 2022 cost of insider threats global report. Ponemon Institute. 2022. URL: https://protectera.com.au/wp-content/uploads/2022/03/The-Cost-of-Insider-Threats-2022-Global-Report.pdf [accessed 2024-05-06]
86. Wagner S. The medical data of hundreds of HUG patients accessible on the internet. Ictjournal. 2019. URL: https://www.ictjournal.ch/news/2019-10-04/les-donnees-medicales-dune-centaines-de-patients-des-hug-accessibles-sur-internet [accessed 2019-10-04]
87. Arapi K. The healthcare industry: evolving cyber threats and risks. Utica College. May 2018. URL: https://www.proquest.com/openview/6fb8d8f9984e83b682b5499fb1d36194/1?pq-origsite=gscholar&cbl=18750 [accessed 2024-05-06]
88. Perriello B. 'Medjack:' hackers threaten hospitals using medical devices as back doors. MassDevice. Jun 5, 2015. URL: https://www.massdevice.com/medjack-hackers-threaten-hospitals-using-medical-devices-as-back-doors/ [accessed 2024-05-06]
89. Meggitt S. MEDJACK attacks: the scariest part of the hospital. Tufts University. Dec 18, 2018. URL: https://www.cs.tufts.edu/comp/116/archive/fall2018/smeggitt.pdf [accessed 2024-05-06]
90. Rajamäki J, Pirinen R. Towards the cyber security paradigm of ehealth: resilience and design aspects. AIP Conf Proc. Jun 5, 2017;1836(1). [FREE Full text] [doi: 10.1063/1.4981969]
91. Murphy S. Is cybersecurity possible in healthcare? National Cybersecur Institute J. 2015;1(3):49. [FREE Full text]
92. Kioskli K, Fotis T, Mouratidis H. The landscape of cybersecurity vulnerabilities and challenges in healthcare: security standards and paradigm shift recommendations. In: Proceedings of the 16th International Conference on Availability, Reliability and Security. 2021. Presented at: ARES '21; August 17-20, 2021; Vienna, Austria. URL: https://doi.org/10.1145/3465481.3470033 [doi: 10.1145/3465481.3470033]
93. Tuttle I. Cyberdisaster: how the government compromised our security. National Review. Sep 9, 2016. URL: https://www.nationalreview.com/2016/09/opm-hack-house-oversight-committee-report/ [accessed 2024-05-08]
94. Loi M, Christen M, Kleine N, Weber K. Cybersecurity in health – disentangling value tensions. J Inform Commun Ethics Soc. May 13, 2019;17(2):229-245. [FREE Full text] [doi: 10.1108/jices-12-2018-0095]
95. Christen M, Gordijn B, Loi M. The ethics of cybersecurity. CrimRxiv. 2020. URL: https://www.crimrxiv.com/pub/s79bo1xu/release/1 [accessed 2024-05-06]
96. Coles-Kemp L, Williams PA. Changing places: the need to alter the start point for information security design. Electron J Health Inform. 2014;8(2). [FREE Full text]
97. Khaloufi H, Abouelmehdi K, Beni-hssane A, Saadi M. Security model for big healthcare data lifecycle. Procedia Comput Sci. 2018;141:294-301. [FREE Full text] [doi: 10.1016/j.procs.2018.10.199]
98. Holst C, Sukums F, Radovanovic D, Ngowi B, Noll J, Winkler AS. Sub-Saharan Africa—the new breeding ground for global digital health. Lancet Digit Health. Apr 2020;2(4):e160-e162. [FREE Full text] [doi: 10.1016/s2589-7500(20)30027-3]
99. Khando K, Gao S, Islam SM, Salman A. Enhancing employees information security awareness in private and public organisations: a systematic literature review. Comput Secur. Jul 2021;106:102267. [FREE Full text] [doi: 10.1016/j.cose.2021.102267]
100. Winton R. Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating. Los Angeles Times. Feb 18, 2016. URL: https://tinyurl.com/5yae788s [accessed 2024-05-06]

101. Dobuzinskis A, Finkle J. California hospital makes rare admission of hack, ransom payment. Reuters. Feb 20, 2016. URL: https://www.reuters.com/article/idUSKCN0VS05M/ [accessed 2024-05-06]
102. Bickers S, Dunlevy S, Minear T. Hackers are offering to sell the medicare details of Australians on the dark web, government confirms. News Corp Australia Network. Jul 4, 2017. URL: https://tinyurl.com/4ryf66v8 [accessed 2024-05-06]
103. Zorabedian J. How malware works: anatomy of drive-by download web attack. Sophos News. Mar 26, 2014. URL: https://news.sophos.com/en-us/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/ [accessed 2024-05-06]
104. Omotosho A, Asanga U, Fakorede A. Electronic prescription system for pediatricians. Eur Sci J. 2017;13(18):426. [FREE Full text] [doi: 10.19044/esj.2017.v13n18p426]
105. Chen B, Ren Z, Yu C, Hussain I, Liu J. Adversarial examples for CNN-based malware detectors. IEEE Access. 2019;7:54360-54371. [FREE Full text] [doi: 10.1109/access.2019.2913439]

Abbreviations

EHR: electronic health record
GDPR: General Data Protection Regulation
IoMT: Internet of Medical Things
PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses
RQ: research question
SLR: systematic literature review

Edited by A Mavragani; submitted 03.03.23; peer-reviewed by R Marshall, V Perez Jover; comments to author 27.07.23; revised version received 17.10.23; accepted 08.03.24; published 31.05.24

Please cite as:
Ewoh P, Vartiainen T
Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review
J Med Internet Res 2024;26:e46904
URL: https://www.jmir.org/2024/1/e46904
doi: 10.2196/46904
PMID:

JOURNAL OF MEDICAL INTERNET RESEARCH Ewoh et al

Review

Sociotechnical Cybersecurity Framework for Securing Health Care From Vulnerabilities and Cyberattacks: Scoping Review

Pius Ewoh[1], MBA; Tero Vartiainen[1], PhD; Timo Mantere[2], PhD

[1]School of Technology and Innovations, Information Systems Science, University of Vaasa, Vaasa, Finland

[2]School of Technology and Innovations, Automation Technology, University of Vaasa, Vaasa, Finland

Corresponding Author:
Pius Ewoh, MBA
School of Technology and Innovations
Information Systems Science
University of Vaasa
Wolffintie 32
Vaasa, 65200
Finland
Phone: 358 414888477
Email: pius.ewoh@uwasa.fi

Abstract

Background: The vulnerability of health care systems to cyberattacks and breaches of health information is on the rise worldwide. Considering the increasing rate of reported cyber incidents and the risks they pose to patient safety, privacy, and financial losses, there is a need to examine the way cybersecurity is conceptualized in health care organizations, taking into account technology, processes, and humans.

Objective: This study examined the dynamics of the factors of vulnerabilities and cyberattacks in the context of sociotechnical systems theory underlying the relationships among humans, technology, and processes. It developed a conceptual sociotechnical cybersecurity framework for preventing vulnerabilities and responding to cyberattacks and threats in health care systems.

Methods: A scoping review was conducted to search the extant literature in 3 databases—Web of Science, PubMed (MEDLINE), and Scopus. A total of 1375 papers from the period of 2012-2024 were retrieved, 76 of which, in the domain of health care and cybersecurity, were reviewed and analyzed. Original research and review papers were included. Only published English-language papers were included to focus on contemporary issues, challenges, and solutions. Relevant information from the included sources was charted and summarized. The study characteristics were extracted from the included papers, and the evidence was synthesized using thematic analysis.

Results: Of the 1375 papers identified, 76 (5.5%) met the inclusion criteria. The results showed that the factors of vulnerabilities to cyberattacks comprise 12 subfactors in health care systems. Concerning technology-related factors of vulnerabilities, most studies described the complex system design and usability (16/76, 21%) and integration of new technology (15/76, 20%) as challenges in health care systems. Concerning human-related factors, most studies described a shortage of skilled professionals and limited budgets as contributing to poor cybersecurity management. The study found that processes involved both technology and humans relative to the unit factors of vulnerabilities to cyberattacks. There was a sociotechnical interplay across the factors of vulnerabilities. The concept of sociotechnical cybersecurity offers a comprehensive and explicit perspective on the sociotechnical underpinning and joint optimization required to advance cybersecurity toward achieving sustainable health care systems.

Conclusions: The conceptual framework of sociotechnical cybersecurity provides a contemporary foundation and deep insight for identifying and preventing vulnerabilities and responding to cyberattacks in health care systems. The framework is important due to its suitability, applicability, and customizability for dynamic and complex health care systems. The study also provides compliance standards for applying the proposed conceptual framework to guide health care organizations in cybersecurity practices. The study of cybersecurity through the sociotechnical lens in the health care domain is limited. Further studies are needed on cybersecurity incident management. Health care organizations should leverage the strength of cybersecurity through the implementation of risk assessment and incident response plans.

(J Med Internet Res 2025;27:e75584) doi: 10.2196/75584

KEYWORDS

computer security; network security; digital health; health information; electronic health record system; cyber threats; ransomware; breaches

Introduction

Background

The digitalization of the health care system has introduced numerous positive effects and gains, such as easy access to health information and effective and efficient health care delivery processes and outcomes [1]. In the last 2 decades, health care digitalization has emerged as a topic of discussion among stakeholders in securing critical infrastructure. Understanding how health care professionals use digital technologies to provide high-quality care requires a stakeholder's viewpoint.

Technology integration is the implementation of electronic health records (EHRs), integration of Internet of Medical Things (IoMTs) devices, and broader IT infrastructure. The rapid integration of these technologies into health care systems created this pathway of improved access to medical services, enhanced patient outcomes, and streamlined workflows for health care providers and services in a borderless, continuous health care journey for transitional nations. Patient health care diagnostics reports and information can be accessed in real-time to enable managing medical history and response to emergency cases with the use of EHR systems. However, this has introduced significant vulnerabilities, making health care systems more susceptible to cyberattacks that could compromise sensitive patient data and disrupt health care services [1-3]. As these vulnerabilities are linked to their areas of occurrence, they can be categorized and described through the interplay of technology, humans, and processes. This enables the application of sociotechnical systems (STS) theory and knowledge management approaches to health care systems [4,5]. The National Institute of Standards and Technology (NIST) Cybersecurity Framework acknowledges that these vulnerabilities may arise from human factors, technology, and organizational processes [6]. Additionally, the research by Kaberuka and Johnson [7] on adapting the STAMP (Systems Theoretic Accident Model and Processes) for sociotechnical cybersecurity challenges in emerging nations acknowledges that human factors, organizational processes, and technology are of great concern. These vulnerabilities must be addressed for organizations to maintain resilience to cyberattacks and threats. NIST interagency and internal reports define these vulnerabilities as weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source [8,9].

The relationships among technology, humans, and organizational processes lead to vulnerabilities exploited by cybercriminals or state-sponsored attackers to gain access and control over critical health care infrastructure and sensitive data, thereby disrupting health services. These vulnerabilities can be considered a sociotechnical problem in a complex health care system [7,10-12]. This problem can be solved using a sociotechnical approach to tackling vulnerabilities in health care systems. According to the 2024 report of the World Economic Forum, the cost of damage incurred by all forms of cybercrime resulting from humans, technology, and organizational processes could reach US $10.5 trillion in 2025. Some of the main sociotechnical cybersecurity problems in health care systems include the following. First, in 2021, ransomware attacks were launched on the health care systems of Ireland, known as the Health Service Executive, disrupting the health care services of 54 public hospitals, and IT systems nationwide were shut down. As a result, more than 80% of the IT environment was encrypted by cybercriminals, and information was exposed at a great financial cost [13,14]. Second, the WannaCry ransomware attacks in 2017 infected over 200,000 computers worldwide and disrupted services due to vulnerabilities in computer operating systems [15-17]. Third, in 2017, Hollywood Presbyterian Medical Center was also attacked by ransomware that encrypted all health information. The medical center paid a ransom of US $17,000 to regain access to its data [18]. Fourth, in 2016, Lukaskrankenhaus, a public hospital in Germany, was attacked by ransomware initiated through phishing. Computer systems were forced by authorities to shut down [19].

Based on this knowledge gap identified, the following research questions (RQs) were asked: (1) What are the sociotechnical factors of vulnerabilities to cyberattacks that affect health care systems? (RQ 1) (2) What kind of framework is best suited for preventing vulnerabilities and responding to cyberattacks and threats in health care systems? (RQ 2). The objective of this study was to examine the dynamics of the factors of vulnerabilities to cyberattacks from a sociotechnical perspective and develop a conceptual framework for preventing vulnerabilities and responding to cyberattacks and threats in health care systems.

Rationale and Sociotechnical Perspective

Rationale

The motivation for this research emerged following the increasing number of cyberattacks in health care organizations. Preventing cyberattacks requires an understanding of the multidimensional complexities of health care system factors of vulnerabilities. However, few studies have been conducted in the field of cybersecurity in health care from a sociotechnical perspective. Garcia-Perez et al [20], Szczepaniuk and Szczepaniuk [21], and Vukotich [22] addressed cybersecurity challenges in health care systems from a technical perspective. Zimmermann and Renaud [23] and Nicho and McDermott [24] focused on addressing vulnerabilities in health care organizations using a social approach. This contributes to the literature by addressing the scholarly call for a sociotechnical cybersecurity framework in health care aimed at preventing vulnerabilities and responding to cyberattacks and threats [25-27]. Nicho and McDermott [24], Wani et al [28], and Sutton and Tompson [29] noted that a comprehensive cybersecurity framework that closes the sociotechnical gap within health care organizations' cyberspace is important. A study conducted by Malatji et al [17] found that "only four security frameworks, namely NIST,

ISO/IEC, COBIT, and IT-CMF partially fulfilled the security requirements of the social dimension of a sociotechnical system" [25].

Scholars have contributed to cybersecurity theory by developing various generic frameworks for different types of organizations [17,29-31]. This study proposed a conceptual sociotechnical cybersecurity framework for health care organizations to prevent vulnerabilities and respond to cyberattacks.

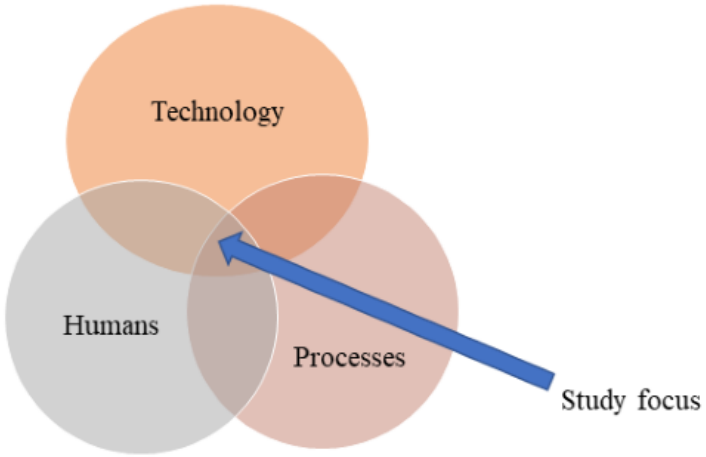
STSs Perspective

The STS theory examines the introduction of new technologies in organizations, their impact on humans, and the interactions between individuals of different skill sets, all within organized units to optimize the performance of social and technical systems [32,33]. According to Trist [33], an STS perspective in any organization comprises a set of integrated and interacting social and technical subsystems or constructs, such as people, infrastructure, technology, culture, goals, and processes. At their core, STSs conceptualize the design and performance of any organizational system that can only be optimized if there is an integration and interplay of the social and technical aspects, and they are deemed interdependent parts of a complex system.

The term STSs originated with Emery and Tris in 1960, as they observed that systems involve complex interactions among people, machines, and the environmental aspects of the organizational system [34]. The concept of STS theory was proposed by the Tavistock Institute as a method used to treat wounded soldiers and in constructions by Mumford [35], Emery [36], and Trist [37]. The underlying assumption of STSs advocates that systems design should be a process that considers both social and technical aspects that influence the functionality and usage of interconnected computer-based systems [38].

This study adopted an STS perspective on cybersecurity in the domain of health care that integrates technology, humans, and processes, subsystems, or constructs. In the context of cybersecurity in health care, the aforementioned constructs were established in the study conducted by Zimmermann and Renaud [23]. Figure 1 illustrates the 3 areas of STSs that were integrated in a holistic approach to prevent vulnerabilities and respond to cyberattacks in health care systems through an intervention framework [16,25,27].

Figure 1. Sociotechnical interplay.



Methods

Protocol and Registration

The review was performed based on the PRISMA-ScR (Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews) checklist by the JBI (Joanna Briggs Institute) [39,40]. This study aimed to examine the dynamics of the factors of vulnerabilities to cyberattacks and propose a conceptual framework for health care systems. During the planning stage of this scoping review, a protocol was created that reflected sources of information, search strategies, inclusion and exclusion criteria, source selection, and data charting processes. This scoping review protocol was not registered. The PRISMA-ScR checklist is presented in Multimedia Appendix 1.

Information Sources

Three scientific databases—Web of Science, PubMed (MEDLINE), and Scopus—were searched to retrieve relevant papers, including both original research and review papers.

Search

Search queries were customized to the syntax and indexing features of each database. Keyword searches targeted the key concepts of cyberattacks and health care for PubMed, Scopus, and Web of Science. The title and additional abstract search terms were used to identify relevant publications. Truncation was used to identify word variations of the key concepts in

different publications. The search terms were separated with the Boolean operators “AND” and “OR.”

PubMed (MEDLINE) incorporated a combination of Medical Subject Headings, including computer security, health care facilities, workforce, services, and delivery of health care. An example of the search strategy in one of the databases is shown in Textbox 1. The detailed search strategy used for the other databases is provided in Multimedia Appendix 2.

Textbox 1. Search strategy showing the search string for PubMed.

“Computer Security”[Mesh] OR Cyberattack*[tw] OR Cybercrime*[tw] OR “Cyber Crime”[tw] OR Cyberthreat*[tw] OR “Cyber Threat”[tw] OR “Cyber Crises”[tw] OR “Cyber Risk”[tw] OR “Cyber Incident”[tw] OR Cyber Operation[tw] OR Cyberspace[tw] OR “Cyber Infrastructure”[tw] OR “Data Breach”[tw] OR “Data Security”[tw] OR “Firewall”[tw] OR “Information Security”[tw] OR “Information Technology Security”[tw] OR “Information Systems Security”[tw] OR “Security Incident”[tw] OR “Network Security”[tw] OR Ransomware[tw] OR Malware[tw] OR Phishing[tw]) AND (“Health Care Facilities, Workforce, and Services”[Mesh] OR “Delivery of Health Care, Integrated”[Mesh] OR “Health Care”[tw] OR “Health Information”[tw] OR “Health Information Management”[tw] OR “Healthcare Systems”[tw] OR “Health Systems”[tw] OR “Health System Infrastructure”[tw] OR “Medical Devices”[tw] OR Medical Technolog*[tw] OR Health Technolog*[tw] OR Health Care Technolog*[tw].

Eligibility Criteria

The inclusion criteria for the papers were relevance to health care cybersecurity, coverage of cybersecurity issues, challenges, and solutions in health care systems. Only English-language papers published between 2012 and 2024 were included (Table 1).

Table 1. Inclusion and exclusion criteria.

Criterion	Inclusion	Exclusion
Language of papers	Papers in English	Non–English-language papers
Year of publication	Papers published between 2012 and 2024	Papers published outside the range of 2012-2024
Research topic focus	Cybersecurity and health care	The topic is different from the topic areas
Scope of work	Key elements and factors that contribute to or lead to breaches, cyberthreats, cyberattacks, and vulnerabilities, and the development of a sociotechnical intervention framework for health care system resilience	Topics outside the research scope of work
Publication type	Original research and review papers	Research in-progress papers, editorial papers, and theses

Selection of Sources of Evidence

The retrieved papers were exported to the citation tool Zotero (Digital Scholar), in which duplicates were identified and removed using the duplicate item function. To assess eligibility, the titles and abstracts of each paper were analyzed by 2 of the authors. In instances in which the eligibility criteria for the papers were not clear, all 3 authors checked the papers and perused them to assess their relevance.

Data Charting Process

Using a standard Microsoft Excel (Microsoft Corp) spreadsheet, data from the studies that met the eligibility criteria were extracted independently by one of the authors and assessed by the other 2 authors to ensure data quality and consistency. This was used to identify the key characteristics of each study and relevant information regarding cyberattacks in health care.

Data Items

The key data items extracted included author, year of publication, country of origin, study design, aims, and key findings. The extracted data items were checked by the second author. A list of the extracted characteristics for the included studies (N=76) is provided in Multimedia Appendix 3 [1,4,6,7,9,11,12,16-18,20-23,25-27,41-99].

Critical Appraisal Within Sources of Evidence

The quality of the source of evidence was checked by 2 authors using 3 different appraisal tools. Joanna Briggs Critical Appraisal Tools were used for qualitative research [100], the Mixed Methods Appraisal Tool [101] was used for mixed methods studies, and the Centre for Evidence-Based Medicine Critical Appraisal Checklist was used for cross-sectional studies [102] and the Scale for the Assessment of Narrative Review Articles Appraisal Tool for narrative review papers [103]. This was carried out to ensure that the sources of evidence were up-to-date, relevant, and reputable. For instances in which this was not clear, all 3 authors assessed the sources (Multimedia Appendix 4 [1,4,6,7,9,11,12,16-18,20-23,25-27,41-99,104]). However, the JBI Manual for Evidence Synthesis suggests that critical appraisal is not required for scoping review [40,105]. Multimedia Appendix 5 elucidates the different quality appraisal methods in detail. Studies were not excluded based on quality to capture as much literature as possible; however, low-quality studies were not used to draw conclusions.

Synthesis of Results

Thematic analysis was conducted manually following the 6-step approach described by Braun and Clarke [106]. The 6-step approach involves familiarization with data, generating initial code by using sticky notes, searching for themes, reviewing the themes, defining and naming the themes, and producing the

report. The analysis is hybrid in nature. The results were presented for the data extracted from the relevant papers in tabular form and descriptive formats (categorized into themes), which aligned with the objective and scope of the review.

Results

Overview

A total of 1375 papers were identified from the databases. Thereafter, 377 duplicate papers were removed, and 998 were screened. Subsequently, 213 full-text papers underwent screening. In the end, 76 papers were included in the review (Figure 2 illustrates the selection process).

The review of the extant literature confirmed the 3 factors of vulnerabilities to cyberattacks (technology, humans, and processes) from the lens of the STS theory in health care systems; they are presented in Tables 2-4. These factors were further categorized into twelve subfactors: (1) new technology integration, (2) complex system design and usability, (3) third-party application and plugin, (4) limited monitoring, (5) inadequate access control management, (6) insider threats, (7) shortage of skilled professionals and limited budget, (8) inefficient training, (9) security culture, (10) untimely incidence response and recovery plan, (11) inadequate policy and procedure, and (12) lack of regular audit and assessment. Subsequently, these 12 subfactors were outlined in descriptive formats.

Figure 2. PRISMA diagram for paper selection. PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses.

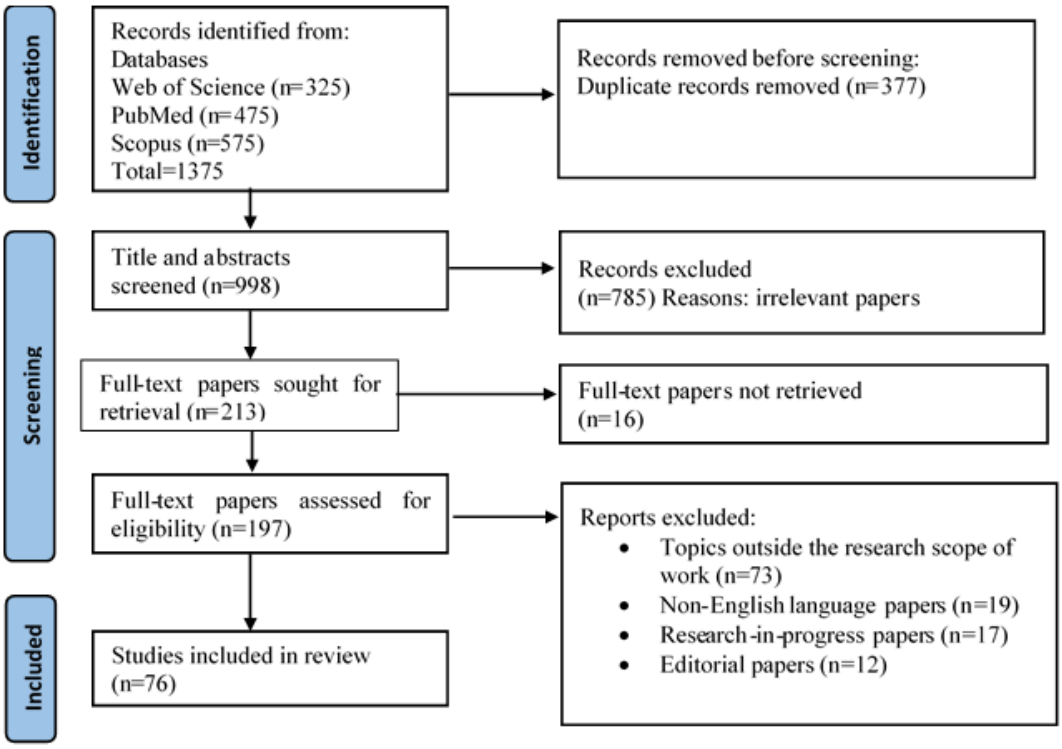


Table 2. Technology factors.

Technology	Studies, n (%)	References
New technology integration	15 (20)	
New technology integration into health care systems creates a new landscape for health care systems to be vulnerable to cyberattacks and threats.		[9,11,20,41-45]
Inappropriate technology integration creates loopholes and interoperability and compatibility challenges that lead to cyberattacks and threats.		[1,27,46]
Interconnected medical and end point devices, when exposed to the internet, create security risks that are possible points of access for cyberattackers to gain access to health care systems.		[16,23,42,47,48]
Complex system design and usability	16 (21)	
Complex system design tends not to be user-friendly; thus, its application in health care systems creates ambiguity in managing cloud-based big data and information, which results in exploitation by cybercriminals.		[12,47,49,50]
Design limitations on implanted medical sensor devices, such as assembly size and limited energy source, lead to connectivity and communication interruption for health care professionals in monitoring patients and data due to denial-of-service attacks. Such limitations also create encryption challenges.		[44,51]
Lack of a comprehensive or holistic framework for the security design in all layers of connected medical devices and software applications creates health information and privacy risks for internet-based device architecture and the operational environment.		[21,26,52,53]
Highly complex interconnected network systems increase the likelihood of vulnerabilities.		[9,23,27,54,55,99]
Third-party applications and plugins	7 (9)	
Software internet-based products from third-party applications leverage vulnerabilities in medical devices and authentication errors that can be exploited by hackers to steal sensitive data or manipulate health care system operations.		[42,51]
Most incidents of vulnerability and cyberattacks in health care systems stem from a wide range of sources, such as operating systems or cloud-based software architectures of third-party developers.		[56-58]
Third-party universal applications and devices, such as mobile apps and hardware integration in health care systems used for telemedicine applications, are not able to provide user anonymity when confronted with cyberattacks.		[59,60]
Health care plugin apps for mobile devices often face privacy and security issues due to developer deviation from compliance with regulatory standards.		[42,61]
Limited monitoring	11 (15)	
Inadequate capabilities for continuous monitoring of systems result in health information breaches and cyberattacks in health care systems.		[4,12,22,61,90]
Inconsistent monitoring affects compliance, health care cyber-critical infrastructure updates, and organizational processes. This invariably constrains organizations' preparedness to achieve the goals of security standards.		[52,65,83,91]
Complexities in monitoring processes in health care organizations are a gateway to data breaches, cyber threats, and cyberattacks.		[68,69]
Inadequate access control management	8 (11)	
Reactive health care systems that lack a strong access control system are prone to privilege escalation attacks.		[4,71,84,91]
In the course of a malware incident, attackers can modify access control systems to grant administrative privileges to exploit health care systems.		[46,84,92]
Breakdown in access control management resulting from an update, server disruption, or malicious intrusion pushes health care organizations to shut down operational processes in the event of a cyberattack to reduce harm.		[52,67,92]

Table 3. Human factors.

Humans	Studies, n (%)	References
Insider threats	7 (9)	
Insiders can introduce threats and vulnerabilities through inadvertent actions, such as inappropriate behavior, clicking phishing links, and falling victim to cyber threats.		[9,42,62]
Most of the breaches that occur in health care organizations originate with insiders stealing and leaking sensitive information to cybercriminals for money or political gain.		[9,11,52,63]
Negligence by internal IT teams in failing to terminate vendor accounts or agreements in intersupport systems of care could create an entry point for vulnerability to cyberattacks.		[52,61]
Inefficient training	9 (12)	
Health care cybersecurity training implementations are largely misdirected, with a focus on cybersecurity professionals and information and communication technology (ICT) departments only, while neglecting health care–based professionals.		[62,64,65]
Ineffective cybersecurity training helps cybercriminals gain access to a health care system's sensitive information through social engineering methods such as phishing, malware, and baiting.		[6,20,62,66,67]
Training that lacks blended skill development is ineffective in achieving a sustainable goal to mitigate cyber exploitation and ensure personal development for health care professionals.		[7,27,67]
Shortage of skilled professionals and limited budget	15 (20)	
Another reason for increasing cyber breaches of sensitive health information is the limited budget allocation for cybersecurity.		[1,4,43,47,52,68-70]
Health care organizations endure poor security management in containing attacks and cybercrime, and developing new strategies to counteract cyber threats and breaches due to a shortage of skilled professionals and limited budget.		[18,41,63,71]
The shortage of cybersecurity experts in health care organizations creates a vacuum for attacks and breaches, while also hindering the development of cybersecurity knowledge among employees.		[43,54,72,73]
Security culture	11 (15)	
Lack of security culture awareness among health care organization staff, coupled with inadequate training in behavior, interactions, and meaningful work practices within the work environment, constitutes a significant factor that may facilitate improper data handling practices and protection.		[74-76,96,97]
Novel viral infections and pandemics requiring rapid technological advancement in health care diagnostics invariably affect behavioral patterns at work and the daily cybersecurity activities of employees.		[77,78]
Poor management of organizational culture may affect employees' cybersecurity behaviors and attitudes toward technology use, thereby increasing the risk of cyberattacks.		[70,78-81]

Table 4. Process factors.

Processes	Studies, n (%)	Reference
Untimely incident response and recovery plan	12 (16)	
Ineffective operational communication systems create poor incident response and preparedness to respond to threats and cyberattacks.		[58,61,82-84]
Containing an attack and a breach in a health care system through postincident response takes approximately 100 days or more before a health information system is restored to normal, safe mode.		[85]
Cybersecurity strategies in health care systems are often reactive instead of proactive in cyber defense mechanisms, backup, and recovery.		[22,86,87,98]
There is limited research on cybersecurity response strategies, which is a great concern.		[87-89]
Inadequate policies and procedures	11 (15)	
Standard policy protocol for most health care organizations is inadequate to meet best practice measures in cybersecurity.		[42,44,92-94]
Some policies and procedures set out by regulatory bodies are cumbersome in laying down information security expectations and are complex to follow. For example, breaches below 500 are neglected and not taken into account.		[61,62]
Policies in line with secure behavioral awareness are inadequate for safeguarding health care systems from cyber breaches.		[43,80,90,95]
Lack of regular audits and assessments	10 (13)	
Most health care organizations do not perform regular or consistent security audits and risk assessments as required by regulations and best practices to visualize security risk levels.		[4,6,22,45]
Most health care organizations do not categorize their risks into external and internal risks or have an effective risk plan in place.		[4,52,84]
Conducting an assessment and audit of a complex sociotechnical system in cybersecurity fails to factor in technology, organizational environment, and humans as a whole.		[17,22,25,26,84,91]

Technology Factors

Integration of New Technology

Smart health care systems have successfully procured and integrated medical cyber-physical systems technologies with the Internet of Things to facilitate operations using virtual networks, applications, and devices, as well as to monitor diagnoses, manage treatment, and manage administrative processes in the delivery of health care services [11]. This new technology integration has helped to streamline health care for effective service delivery. The integration of these digital technologies has evolved as they create complex interconnected ecosystems, making it challenging to implement and maintain robust security measures across all components [16,27,41,44,45,47].

Inappropriate technology integration increases the vulnerability of health care organizations to cyberattacks and breaches when the complex STSs integration process and standards are not properly followed or managed [9,42,90]. Additionally, it poses a risk when data is exchanged between the cloud and electronic records, or when it travels within the health care delivery ecosystem. Some of the reasons for the risk are unsupported integration, inappropriate standard implementation [43,46], lack of secure development in the ideation stage [107], ineffective communication, and interoperability issues. These issues, in turn, can give cybercriminals unauthorized access to health information or data because of such vulnerabilities in technology [64]. Furthermore, it is necessary for health care system actors to know that the integration of medical devices and interconnectivity does not equate to interoperability; likewise, interoperability does not equate to the security of medical devices and data protection.

Complex System Design and Usability

Complex design and usability can lead to security vulnerabilities in health care information systems [9,104] by affecting data processing, confidentiality, availability, integrity, and design limitations. It creates friction for staff, which can lead to unhealthy security practices in monitoring the IoMT devices and compromising patient safety and privacy [44,50,51]. Additionally, complex and poor system design can make it easier for hackers to exploit vulnerabilities in medical devices and systems, resulting in cyber incidents such as phishing attacks or other social engineering tactics to trick users into giving up their login credentials or downloading and executing malicious software [47,85]. This can harm patients in an emergency and slow care delivery, which can be linked to biomedical nonmaleficence principles [108]. In managing complex health IT challenges, adopting a user-centered approach to health care service operations is pivotal for preventing vulnerabilities and cyberattacks in health care systems [12].

Complex designs and user interfaces of health care devices and applications make it difficult to secure the valuable information in health care systems. Poor design and usability can lead to human user errors, such as accidentally exposing sensitive patient information or mistakenly changing critical medical settings or configurations. The emerging usability literature has highlighted these sociotechnical shortcomings, which could lead to threats and medical errors in health care systems [68].

User satisfaction—whether for patients or health care professionals—at every stage of task performance is enhanced by a friendly design process that prioritizes usability [1,28], design, and data processing. This, in turn, facilitates the effective and efficient delivery of health care services.

Third-Party Applications and Plugins

The adoption of third-party applications and plugin software in modern-day smart health care systems can be used in many more ways than traditional standalone software in health care delivery. Third-party application software, in the form of software as a service, has evolved to make use of web-based, intelligent chatbots and large language models. The complexity of these technologies makes it difficult to control their service dynamics as they become vulnerable to cyberattacks [42,51,70,109]. In some cases, the vulnerability of cyber-critical systems that expose health information and patient privacy is not only an issue of the medical device, but also a software malfunction that could put organizations at risk and affect the quality of services [58,61,110].

Hackers can embed malicious software, such as ransomware, in application software or operating systems. Such malicious software can execute and replicate viruses in health care systems by acting like a legitimate third-party software program. It can then create a backdoor to gain access to sensitive information and organization files for launching cryptolocker attacks [56,111]. Additionally, cybercriminals use third-party software and application plugins to impersonate health care service providers, all the while having malicious motives as part of organized syndicates illegally collecting health data. Some medical applications hosted on mobile systems are illegitimate third-party apps, which are another source of privacy violations and data leakage [59,71,112,113].

Malware can easily be introduced to the medical network of systems when the IT team of the medical device software application makes an error during the development stage. It is estimated that 90% of incidents or breaches occur through exploiting vulnerabilities in a device system's software application program [114]. The use of implanted devices always has issues of software malfunction and update-related problems [1]. For instance, a 2013 analysis of mobile medical health fitness apps showed that over 40% of paid medical applications were completely lacking privacy policies, and 40% of the applications stored sensitive patient information, such as financial details, biodata, and addresses [60]. While only 50% of mobile apps encrypt the personal identifying information sent over the internet, 80% of these third-party applications store this personal identifying information on a local device without encryption, which is liable to be accessed [115]. Having control over third-party software applications and systems while also focusing on developing software from the same device manufacturer will help curb the risk of data breaches and protect sensitive health care–related information [42].

Researchers seem to relate cyber issues to medical devices, neglecting the fact that without operating systems and application software, medical devices would not execute other clinical functions and administrative services in delivering health care [57,58,83]. Regularly updating system software is necessary to improve security against new threats and viruses, since over 90% of breaches stem from programmable software applications or boot systems kernel development, which can be used for implanting viruses in computer systems.

Limited Monitoring

Limited monitoring of the health care systems' critical infrastructure increases the risk of delayed detection of threats and vulnerabilities, allowing them to propagate in the system and cause even greater damage [4,42,52]. Perimeter monitoring technology, such as antivirus and firewalls, also called detection technology, has been developed to recognize known variants of viruses and other threats. In the era of fast-paced technology advancement, ransomware coders are also advancing with detection technology by reprogramming malicious code so that it can remain undetected by the monitoring scanner [52]. Despite the advancement of technology, many health care organizations are still using traditional security monitoring procedures to protect sensitive information and health care systems. Continuous monitoring of health care systems in both real-time and offline modes is essential to enable detection and mitigation of threats [4,42,65].

Inadequate Access Control Management

New technology in health care systems requires role-based access control management for professionals and organizations in managing sensitive resources and operations. Many health care organizations become victims of health information breaches or cyberattacks due to inadequate access control management across different technology platforms and applications. This creates a weak access point for cybersecurity operational integration, which results in system flaws, compatibility issues, and interoperability challenges that facilitate access for cybercriminals to gain entry into the health care system network. Strong access control policies help foster effective access control and identity management [6,28,84]. Managing employee privileges and training them not to share passkeys can help prevent lapses in access authorization while ensuring role-based access control to strengthen identity and access management in health care systems [71].

Health care organizations must ensure that their network has strong control systems and structures for better identity management to avoid unauthorized access, breaches of sensitive information, and identity theft [52,67,91]. Weak cybersecurity control and identity management could stem from software applications, human factors, and organizational management processes as a result of outdated systems and technology [69,116-118].

Human Factors

Insider Threats

Insider threats have recently been seen as a growing challenge. Research has attributed these specific threats to the emergence of connected health care IT, which is one of the causes of data breaches or leakages of protected health information [42,119]. However, insider threats are linked to the human element of health care IT systems, wherein human error has been seen as one of the major sources of vulnerabilities in the critical cyber

infrastructure [19,67,96]. The root causes of insider threats include insecure behavior by employees and organizations' inadequate investment in employees' cybersecurity skills for social and technical know-how [80,81,120]. In contrast, during the era of nontechnical application of care delivery, insider threats were less visible to organizations when protected health information was filed through paper-based manual storage systems. The traditional breaches from insider threats were physical breaches, such as the theft of patients' valuable information, theft of files and computers, or missing paper health care records [9,11,52,63]. The missing data or breach in patient information was known only to the health care organizations, so the collection of new health records from patients would begin without the need to notify patients about General Data Protection Regulation or Health Insurance Portability and Accountability Act violations [95].

Research has also revealed that since the emergence of the interconnectivity of records, the level of insider threats and attacks has increased tremendously, as such interconnectivity provides multiple gateways for access in a remote location and setting [9,16,61]. Furthermore, the level of insider threats in this era of digital health processes will be more accountable with proper cybersecurity systems and monitoring compared to the paper-based process, where the insider goes unnoticed and underreported. Research has also revealed that, between 2019 and 2024, organizations reported that insider threats increased from 66% to 74% [119]. The literature has also revealed that insiders, rather than outsiders, contributed to about 70% of data fraud and breaches in an organization [86]. This is also attributed to a lack of employee cybersecurity ethics, management implementation of data integrity, and privacy of patient records as a culture of ethics in the workplace [108]. Authors have highlighted different issues of insider threats, digging deep into the risks and issues of insider threats and breaches in health care organizations [67].

Inefficient Training

Inefficient training of employees can have a significant negative impact on health care systems, most importantly when a health care professional lacks the knowledge and understanding of cybersecurity vulnerabilities and threat patterns of the health care system [1,52]. It is the duty of health care organizations to give proper training and awareness of cyber threats and attacks to their staff [64,65]; otherwise, employees may easily become vulnerable, resulting in data breaches of sensitive health information [70]. It is important to conduct training assessments for employees; otherwise, it will be difficult to ascertain the extent of the training required [62]. Phishing training, including gamification-based methods, is one approach to assessing employee knowledge. Training results can then be used to design a curriculum that is tailored to work processes, ensuring that employees acquire the training needed to enhance IT security awareness and readiness [42,67]. It is important that health care professionals who use critical hospital infrastructure are trained in comprehensive cybersecurity user applications, including sociotechnical techniques for dealing with health care cybersecurity vulnerabilities, threats, and risks [6,27].

Shortage of Skilled Professionals and Limited Budget

Cybersecurity breaches in health care increase daily due to a growing shortage of skilled professionals and limited budgets, posing a significant concern [69,70,73]. This concern is critical for health care organizations due to the large amounts of valuable sensitive data stored in the EHR system and cloud. This sensitive data includes medical records, insurance information, and financial data [16].

Many health care institutions lack the cybersecurity expertise required to defend their digital health care systems from cyberattacks [5,9]. However, while the demand for cybersecurity experts in health care is high, the supply is low. As a result, health care organizations may be subjected to complex assaults on critical infrastructure requiring specific knowledge [54,71]. For instance, cybercriminals take advantage of employees' low skill sets to exploit them [52]. This shortage of skills continues to leave health care organizations challenged in the changing environment of health care systems, which constrains the organizations from detecting and preventing cyberattacks in health care systems [54]. Furthermore, limited investment in cybersecurity systems and technology accelerates vulnerabilities, threats, and attacks in health care organizations [1,47,104] due to obsolete techniques that lag behind digital trust and security protection. In some cases, health care businesses have limited cybersecurity budgets, making it difficult to invest in the required technologies and resources for defending themselves against threat actors and vulnerabilities [4,43,68]. The shortage of skilled professionals and limited budgets can lead to major cybersecurity vulnerabilities in the health care system [52,69].

Security Culture

Security culture plays a crucial role in addressing cyber threats in health care organizations. To properly protect information assets, information security behavior is essential [79]. The norms, values, and attitudes of health care professionals contribute to the development and maintenance of a robust security culture in health care organizations that actively support security initiatives [121]. Thus, employees' behavior with regard to data privacy is important for the effectiveness of cybersecurity in the workplace environment [70]. Insecure behavior has been identified as one of the most significant factors contributing to vulnerabilities in cybersecurity [76]. Its 4 key components are lack of awareness and experience, unauthorized workflows, behavior prioritization, and environmental appropriateness [80,81].

In this digital health care era, the social influence of peers is a critical driver that influences health care professionals' motives regarding data privacy policy and security. Furthermore, attitude plays a mediating role in employees' motives regarding compliance with data privacy and policy [97]. Digitalization in health care organizations can be influenced by attitudes toward cybersecurity, subjective norms, and perception of control over security measures [9]. Insecure behaviors and attitudes of employees and patients regarding the use of technology increase vulnerabilities to cyberattacks.

Process Factors

Untimely Incident Response and Recovery Plan

Untimely incident responses and recovery plans in the event of health information breaches and cyberattacks in health care systems undermine public, stakeholder, and patient trust that health care organizations or hospitals can manage their sensitive health information [84,85,111]. A planned or coordinated response and recovery strategy determines the health care systems' ability to contain breaches or threats [70,88]. Effective response and recovery plans can mitigate the severity of cyberattacks in health care systems, reducing their impact and preventing future occurrences [71,82]. Despite this, many health care organizations ignore incident response and recovery plans as part of their cybersecurity strategy and measures for protecting health care systems [84,122].

The WannaCry cyberattack incident against the UK's National Health Service metamorphosed to infect larger systems of health care. This was due to the negligence and poor response strategies associated with the attack [87]. Although the National Health Service management was informed of the vulnerability of the Windows operating system, the IT team was slow to respond to updating the legacy system [52,69]. To mitigate both visualized and hidden cyberattacks in health care systems, the cybersecurity IT team must establish an effective response strategy that integrates evolving technological advancements with new approaches to advanced persistent threats [58,116].

In some cases in which health care organizations were attacked with ransomware, the organizations lost all health care data when they refused to pay a ransom to a cybercriminal. This was due to the lack of a contingency plan, backup, and recovery systems [42,61,85]. Health care organizations are expected to have backup and recovery plans that enable failover of health care data in the event of a cyberattack [12,83] to avoid disruption of services [82].

Inadequate Policies and Procedures

Many health care organizations still operate under traditional information security policies and procedures despite technological advancements and the increase in health care breaches and cyberattacks. Traditional information security policies and old-order operational procedures have become obsolete as technology has evolved [93]. Security policies and operational procedures form the foundation for health care systems' defense against cyber threats and vulnerabilities because they dictate how sensitive health information is protected, incidents are handled, and employees are trained on cybersecurity programs to ensure best practices [52,92,95]. Inadequate policies and procedures predispose health care systems to the risk of cyberattacks and threats [121]. Inadequate policies can stem from several factors, such as underestimation of cyber threats, lack of awareness to engage with cybersecurity issues, and underinvestment [85]. For example, Health Insurance Portability and Accountability Act regulations state that cybersecurity breaches affecting fewer than 500 people should not be reported or fined, which can create ambiguity and gaps in enforcement [61,62]. Additionally, this may encourage organizations with fewer than 500 patients to neglect the security and privacy of this group of patients. Such organizations might endure breaches without disclosing them to the necessary data protection and regulatory authority. The 2015 Anthem breach is a case study of one of the largest breaches, in which the personal information of over 78 million individuals was exposed as a result of inadequate encryption, weak access control policies, and human error [70].

As technology develops, some health care organizations fail to implement new policies that align with evolving technology and the compliance standards necessary to protect health care systems and ensure resilience in managing health information and the entire ecosystem [42,44,61,69,104].

Lack of Regular Audit and Assessment

Existing research has shown that many health care organizations conduct security audits and assessments once a year. Health care organizations that do not engage in regular and comprehensive cybersecurity audits and risk assessments often fail to identify cyberthreats and vulnerabilities in health care systems [4,91]. Furthermore, in the absence of regular security audits and assessments health care organizations may struggle to detect vulnerabilities, making it easier for cybercriminals to exploit the weaknesses in their systems [45]. For instance, the cause of the SolarWinds supply chain attack, in which the back door was created by a cybercriminal without detection, is a case in which sensitive information was harvested for more than a year before being detected only after the cybercriminals exposed the information in the public domain. A regular audit ensures the proper monitoring and evaluation of employee behaviors and security practices [84]. Additionally, with these measures, health care organizations can easily detect vulnerabilities and risk levels of third-party applications through comprehensive and regular audits of the health care systems [42,45,91].

Health care organizations that do not conduct monthly and quarterly audits and assessments will significantly increase their cybersecurity risk profile, which may lead to the possibility of continual breaches [42,71].

Taxonomy Factors of Vulnerabilities to Cyberattacks

Table 5 indicates the taxonomy-related factors of vulnerabilities to cyberattacks, unit-related factors of vulnerabilities to cyberattacks, types of cyberattacks, and their effects on health care organizations.

Table 5. Taxonomy factors of vulnerabilities to cyberattacks.

Factors of vulnerabilities to cyberattacks	Unit factors of vulnerabilities to cyberattacks	Types of cyberattacks	Effect on the health care organization	Reference
Technology				
New technology integration	EHRs[a], medical and network devices, and software	Ransomware, cryptojacking, and DOS[b]	Health information breaches, legal fines from regulators, operational disruptions, data loss, and reputation damage	[1,16,41,45,52,61,70]
Complex system design and usability	EHRs, medical and network devices, and software	Ransomware and DOS	Operation disruptions, cyber breaches, loss of trust, legal fines from regulators, financial loss, and reputation damage	[27,43,51,61]
Third-party application and plugin	EHRs, medical and network devices, and software	Phishing, DOS, and ransomware	Cyber breaches, health care security weakness, operational disruption, compromised safety, and data loss	[42,61,66,109]
Limited monitoring	EHRs, medical and network devices, and applications	DOS, worm infection, ransomware, and data exfiltration	Patient safety risk, service disruption, data breaches, data loss, compromise of Confidentiality, Integrity, and Availability, and operational handicap	[52]
Inadequate access control management	EHRs, medical and network devices, and applications	Ransomware, DOS, privilege escalation attack, and phishing	Patient safety risk, data breaches, identity theft, manipulation of data, and possible ransom payments	[16,42,62,66,92]
Humans				
Insider threats	Health care professionals and EHRs	Identity theft, espionage, and sabotage	Service disruption, loss of trust, sale of data, sensitive data breaches, and data loss	[16,25,42,52,61,70]
Inefficient training	Health care professionals	Phishing, worm infection, and ransomware	Financial loss, fine imposition, huge cost implication, data loss, incorrect diagnosis, and error treatment	[27,43,46,70]
Shortage of skilled professionals and limited budget	Health care professionals	Ransomware, viruses, phishing, and DOS	Patient safety risk, decreased secure care quality, inadequate compliance, insecure health care services, budget reallocation, and data breaches	[27,46,52,61,63,72]
Security culture	Health care professionals	Ransomware, virus, phishing, DOS, DDOS[c]	Insecure behavior, reputation damage, loss of trust, identity theft, security negligence, data breaches, and poor service delivery	[70,77,80,81,97]
Processes				
Poor incident response and recovery plan	Health information, medical devices, applications, health care professionals, and patients	Ransomware, crypto jacking, DNS[d] spoofing, and DOS	Health information breaches, identity theft, legal suits, health care service disruption, ransom payments, loss of data, hard-to-recover data, and financial loss	[43,82,85,98,123]
Inadequate policy and procedure	Health information, medical devices, applications, health care professionals, and patients	Ransomware, worm infection, phishing, and DOS	Service disruption, possible patient harm, compromised sensitive data, regulatory fines, violation of privacy, financial loss, poor security strategies, and data breaches	[43,61,62,92,95]
Lack of regular audit and assessment	Health information, medical devices, applications, health care professionals, and patients	Man-in-the-middle attack, crypto jacking, and worm infection	Reputation damage, possible patient harm, service disruption, privacy violation, unauthorized access freedom, breaches of sensitive information, and data loss	[42,52]

[a]EHR: electronic health record.

[b]DOS: denial of service.

[c]DDOS: distributed denial of service.

[d]DNS: domain name system.

Discussion

Summary of the Findings

This study examined the dynamics of the factors of vulnerability to cyberattacks in the 3 core areas of the STSs theory of technology, humans, and processes in health care systems through a scoping review of 76 papers.

This study found that the integration of new technology can be challenging in protecting health care systems from cyberattacks in the absence of an appropriate intervention. The findings also showed that complexities in system design present adaptability challenges for health care professionals; thus, cyberspace is prone to a high-risk incidence of threats. Furthermore, third-party software limits security in smart health care, which has various impacts on health organizations.

The findings revealed that internal threats existing in health care systems are not linked only to health care professionals but also to IT teams. Additionally, inefficient cybersecurity training exposes health care organizations to vulnerabilities and cyberattacks. The findings also showed that inadequate investment in human capital and limited finances contribute to poor cybersecurity management. This study further found that the decline in security culture is based on cultural deviation and radical technological change in health care organizations, which is deeply rooted in the behaviors and attitudes of employees.

The present study found that most health care organizations are unprepared and do not have a proactive incident response and recovery plan in place in the event of a cyberattack [85]. The communication gap, untimely postincident response, cybersecurity strategies, and limited research on cybersecurity responses contribute immensely to cyber threats and cyberattacks. Furthermore, limitations in continuous monitoring include inadequate capabilities, inconsistent monitoring, and complex monitoring processes that increase cyber insecurity in health care organizations. The findings also indicate that cybersecurity policies and procedures can be complex and inadequate in shaping the security of health care cyberspace. Additionally, cybersecurity auditing and assessment can be inconsistent, fail to classify risks as internal or external, and include nonholistic perspectives of the STS. The study further found that weak access control management and breakdowns facilitate the exploitation of sensitive data in health care systems.

The findings showed that despite the similar unit factors of vulnerabilities to cyberattacks for the subfactor of technology and the occurrence of various types of cyberattacks, the effect on health care organizations remains the same. Additionally, despite the similar unit factors of vulnerabilities to cyberattacks for the subfactor of humans, the types of cyberattacks that occurred differed to some extent; however, the effect on health care organizations was somewhat varied. Furthermore, despite the similar unit factors of vulnerabilities to cyberattacks for the subfactors of processes, the types of cyberattacks that occurred were similar to a great extent; consequently, the effects on health care organizations were also similar to a great extent. In general, this study found that processes involve both technology and humans relative to the unit factors of vulnerabilities to cyberattacks. This confirms the sociotechnical interplay among the factors of vulnerabilities in health care systems [17].

Sociotechnical Cybersecurity Framework

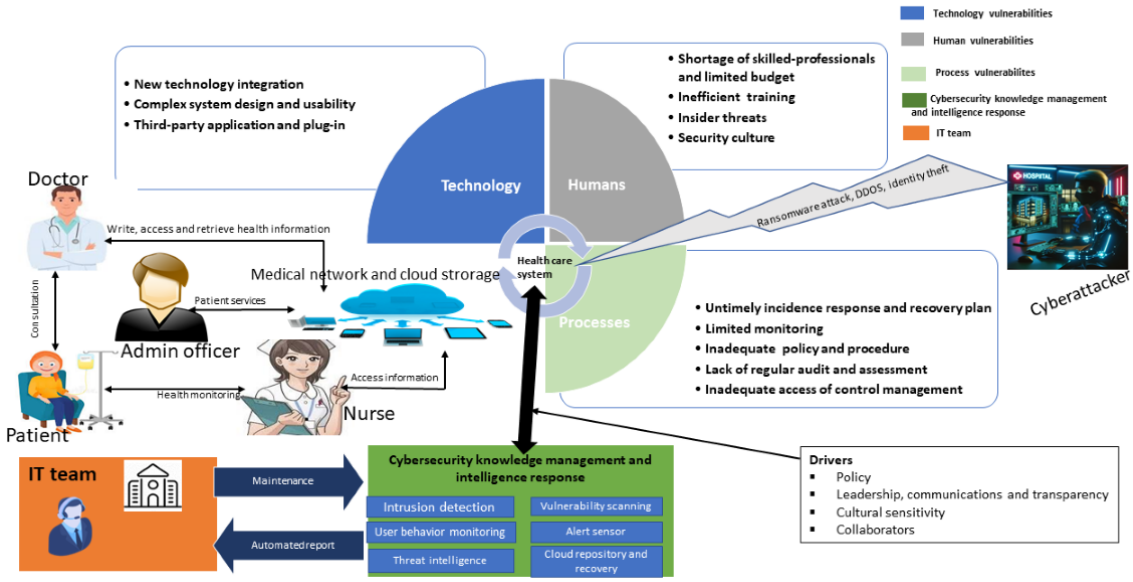
Overview

The three core constructs of STSs that can protect health care systems from vulnerabilities to cyberattacks and breaches are technology, humans, and processes [23,25]. In the context of this study, the three constructs of STSs are referred to as the factors of vulnerabilities, which are the areas in which vulnerabilities occur.

This study proposed a conceptual sociotechnical cybersecurity framework for health care systems that entails the factors of vulnerabilities, IT team, cyberattackers, and cybersecurity knowledge management and intelligence response (CKMIR). The framework incorporates features such as intrusion detection and response, user behavior monitoring, threat intelligence, vulnerability scanning, alert sensors, cloud-based repositories, and recovery mechanisms as a comprehensive approach in responding to the vulnerabilities, cyberattacks, and threats in health care systems; this framework is presented in Figure 3.

The components of the sociotechnical cybersecurity framework are explained in the following sections.

Figure 3. Conceptual sociotechnical cybersecurity framework. DDOS: distributed denial of service; IT: information technology.



Factors of Vulnerabilities

The factors of vulnerabilities involve humans, technology, and processes, which are interwoven in the sociotechnical cybersecurity framework [5,54,87].

IT Team

The IT team is one of the human elements in the loop that provides technical support, maintenance, and remediation for the health care system. The IT team includes software engineers, system developers, cybersecurity experts, compliance officers, IT support staff, and network engineers. They are responsible for the day-to-day health of IT operations to ensure smooth and secure health care service delivery.

Health Care Professionals

Health care professionals include doctors, nurses, administrative staff, etc. The doctors consult with the patients online and onsite, access their medical history from the cloud through the EHR system, and prescribe medication, while the nurses monitor patients' health, provide care, and access patients' medical information through the medical network. Health care administrative staff are responsible for administrative and clinical tasks, such as scheduling staff and appointments for patients to ensure the practice runs smoothly.

Cyberattackers

The cyberattacker is a cybercriminal who exploits the health care system using sophisticated techniques to launch attacks on health care–critical infrastructure. They launch attacks through denial of service, ransomware, and identity theft of patient health information. The stolen information is sold on the dark web for financial gain.

About CKMIR

The CKMIR intrusion detection feature systematically analyzes network traffic, human behavior, technology, and processes in real time to optimally detect and isolate known and unknown cyber threats and attacks in health care systems to enable remediation.

The CKMIR user behavior monitoring feature identifies and analyzes the patterns of human behavior and interactions within health care systems, such as login times, access patterns, file transfers, and application usage, as well as internal and external threats, to determine unauthorized access and compromised accounts.

The CKMIR threat intelligence feature collects, analyzes, and interprets raw data on the intent, opportunity, and capability of malicious actors and shares structured information with the IT team through actionable intelligence.

The CKMIR vulnerability scanning feature scans, detects, identifies, and classifies technology, human, and process factors of vulnerabilities in health care systems and provides countermeasures for cyber threats.

The CKMIR alert sensor senses isolated cyber threats and attacks and sends alerts to the IT team in real time.

The CKMIR cloud repository and recovery feature store and back up encrypted data, critical system files, and security event records to recover data in the event of a cyberattack.

Drivers

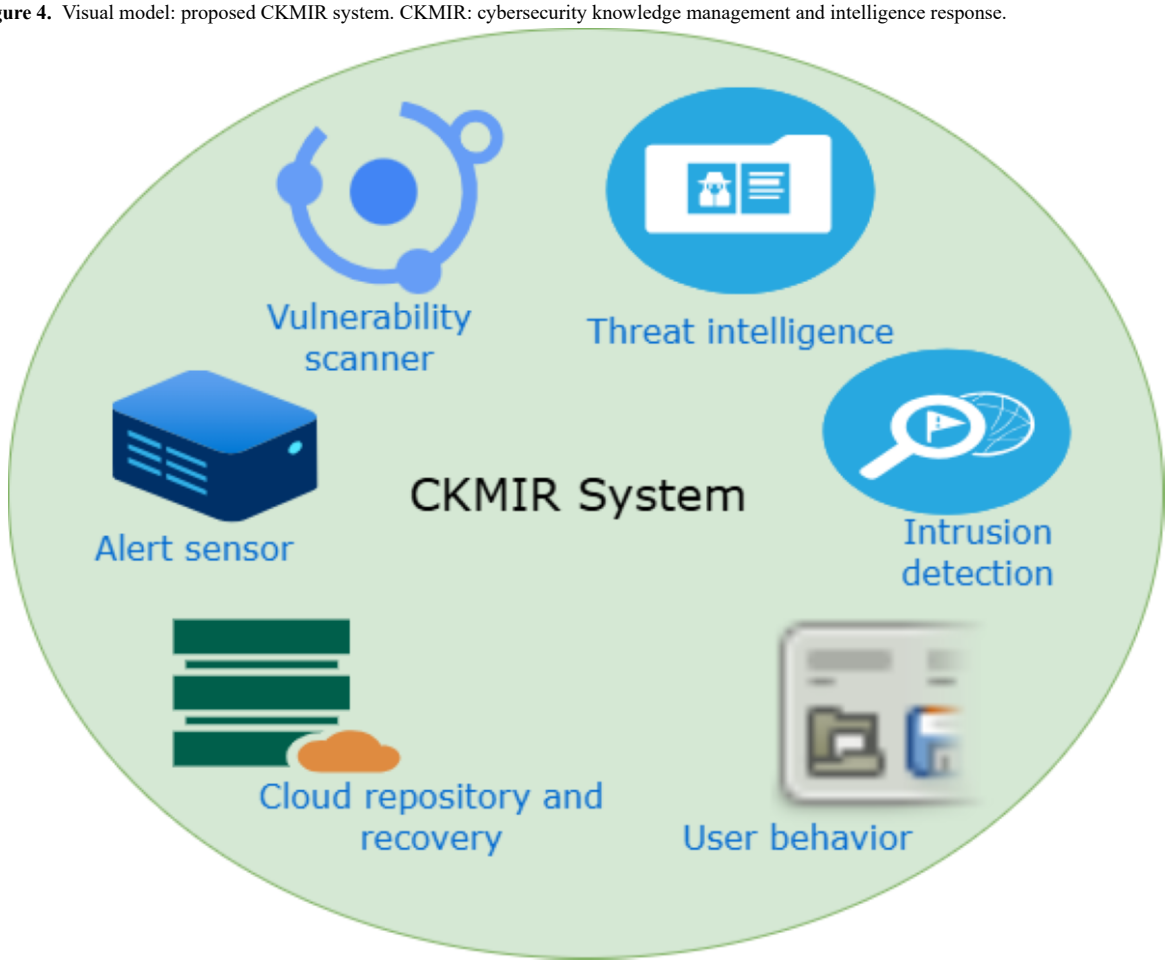
The drivers are the factors that determine the transition of cybersecurity in health care organizations. They play critical roles in shaping sustainable cybersecurity in health care systems. These drivers include policy, leadership, communications and transparency, cultural sensitivity, and collaborators.

In this conceptual framework, CKMIR plays a significant role in automated defense regarding vulnerabilities and intelligent response in the event of a cyber threat or attack.

The framework provides a contemporary foundation and pathway for identifying and preventing vulnerabilities and responding to cyberattacks and threats in health care systems. This conceptual framework is important for identifying, capturing, organizing, storing, and sharing real-time data and actionable intelligence and preventing vulnerabilities to cyberattacks in health care systems. The conceptual framework functions holistically from a sociotechnical perspective of cybersecurity in health care systems. The proposed framework plays a critical role in system interplay for detecting, classifying, and preventing vulnerabilities and providing real-time incident response and automated report generation to ensure that the IT team is informed of the current security status, ongoing incidents, and actions taken.

In Figure 3, an up-down bidirectional arrow indicates the relationship between CKMIR and health care systems. This up-down bidirectional relationship shows that CKMIR prevents vulnerabilities, provides real-time incident response, stores data, and remediates it in the event of threat intrusion and cyberattack, while the health care systems transmit data to CKMIR. Furthermore, opposing 2-way arrows show a relationship between CKMIR and the IT team. This 2-way relationship indicates that CKMIR transmits automated reports while the IT team accesses CKMIR to perform maintenance, remediation, and decision-making. In essence, this framework offers a comprehensive and well-defined approach to the sociotechnical underpinning and joint optimization of cybersecurity's progress in achieving sustainable health care systems. The visual model of the proposed CKMIR system is shown in Figure 4.

Figure 4. Visual model: proposed CKMIR system. CKMIR: cybersecurity knowledge management and intelligence response.



Practical Implementation Steps for the Conceptual Framework

The practical implementation steps for the validation of the proposed conceptual sociotechnical cybersecurity framework are shown in Multimedia Appendix 6. The implementation steps involve the classification of the vulnerability's areas of occurrence (technology, humans, and processes), defining goals, mapping stakeholders, orientation, risk assessment, validation, and feedback. The guide indicates an interplay within the vulnerability's areas of occurrence (technology, humans, and processes). It also shows that there is a joint optimization between the vulnerabilities' areas of occurrence and the CKMIR system to identify and prevent vulnerabilities and respond to

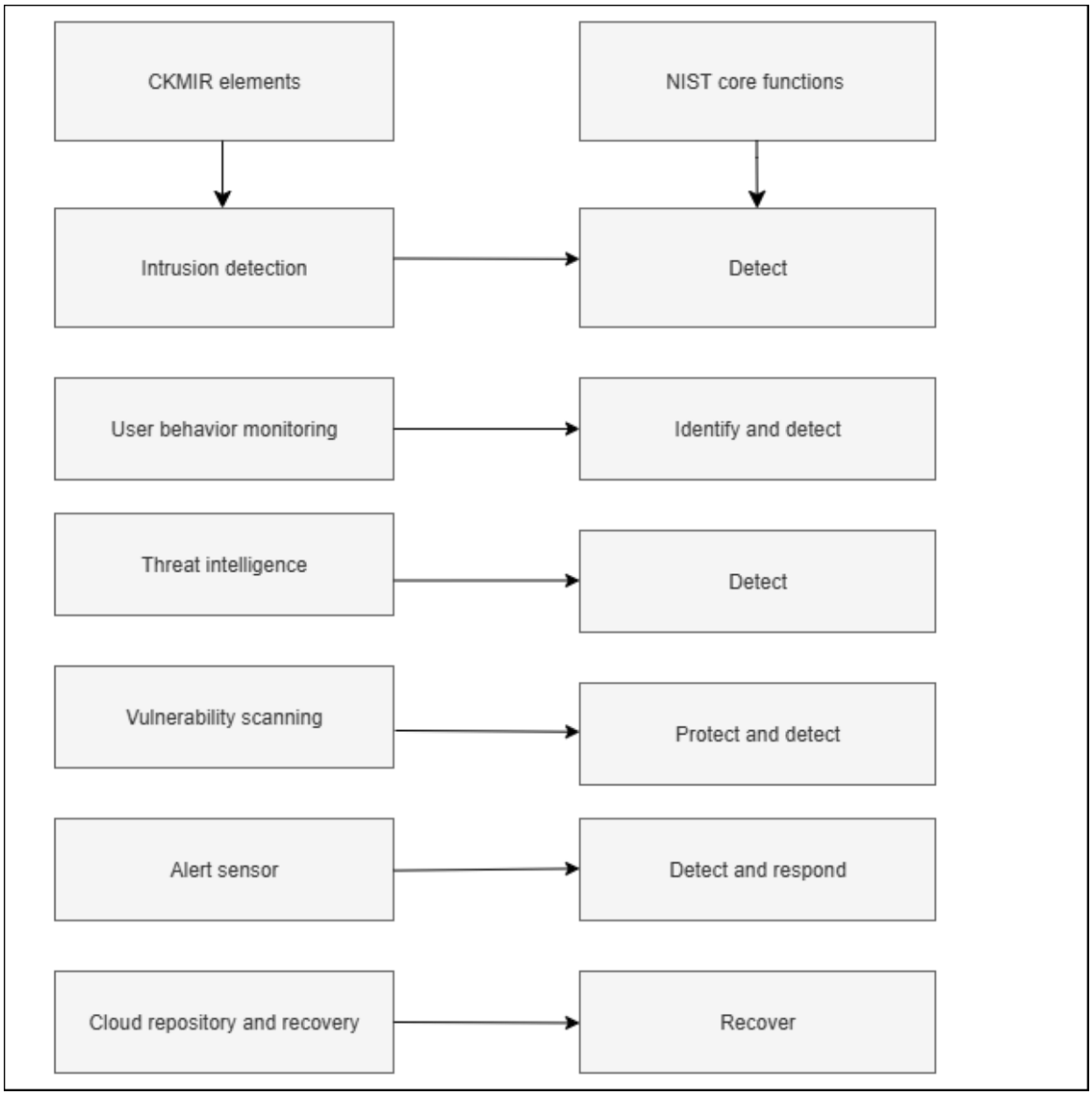
cyberattacks. The implementation of the proposed sociotechnical cybersecurity framework for health care systems (hospitals) in a real-world scenario is aimed at achieving optimal cybersecurity resilience.

Linking the CKMIR System to the NIST Model

The CKMIR elements align with the core functions of the NIST model in Figure 5. The core functions of the NIST model involve identifying, protecting, detecting, responding, and recovering [124]. The CKMIR elements involve intrusion detection, vulnerability scanning, user behavior monitoring, alert sensors, threat intelligence, and cloud repository and recovery.

The unique value proposition of the CKMIR model is the configuration, dynamic integration, and its mode of operation, such as real-time incident response optimization. Specifically, its unique value proposition is the provision of threat intelligence, human behavior analytics, and cross-component integration in the health care system. The CKMIR model applies to the health care system in its capacity to solve complex health care problems in the vulnerable areas of occurrence emanating from IoMT devices, cloud, EHRs, health care professionals, and patients. The model-specific sociotechnical contributions encompass the optimal identification and mitigation of vulnerabilities arising from technology, humans, and processes.

Figure 5. CKMIR element alignment with the NIST model. CKMIR: cybersecurity knowledge management and intelligence response; NIST: National Institute of Standards and Technology.



Compliance Standards for Applying the Proposed Framework

Compliance standards are necessary for the application of the conceptual sociotechnical cybersecurity framework to guide health care organizations in their cybersecurity practices. It will also facilitate the process of cybersecurity risk assessment for health care professionals. The compliance standard is detailed in Multimedia Appendix 7 [12,22,25,42,44,45,52,53,61,63,70-72,75,76,80,81,87,95,99,125].

Practical Implications

Considering the increase in cyberattacks, breaches, and overdependence on modern technology for health care diagnosis and treatment, it is important for health care organizations and stakeholders to examine how technology can be implemented. In particular, policies should mandate secure development for technology integration and third-party applications through adoption and control measures within health care system audit assessments and compliance procurement plans. Health care organizations should leverage the strength of cybersecurity through the implementation of risk assessment and incident response plans that complement current and emerging threats and cyberattacks. Health care organizations should adopt compliance standards for applying the sociotechnical framework as a guide to maintaining cybersecurity hygiene in health care systems (Multimedia Appendix 7). Health care institutions should ensure that the implementation of a medical device security lifecycle is integrated into Confidentiality, Integrity, and Availability practices as quality control measures [21]. Health care organizations should implement network segregation of sensitive areas for greater protection, easy usability, and secure workarounds. Additionally, regular network assessment is required to monitor traffic and network behavior, and to trigger alerts regarding abnormalities [50]. The design of network systems should be simplified and while training professionals to develop secure health care systems. Further, health care management should recruit more skilled professionals, offer training to employees, and increase budgeting for cybersecurity to ensure the delivery of uninterrupted health care services. Health care organizations must implement strong access control systems and policies that ensure the use of strong password systems, multifactor authentication, and strong privileges that grant access to health care critical infrastructure only to authorized employees.

The adoption of the sociotechnical cybersecurity framework by health care organizations will accelerate and optimize cybersecurity progression and support IT teams and operational processes in sustaining the health care cyber space.

Comparison With the Previous Literature

The findings of the scoping review are in line with the existing evidence that obsolete infrastructure, limited budget, complex policies and procedures, ineffective training, and a shortage of cybersecurity experts are barriers to cybersecurity in health care systems [1,68,72]. Additionally, Al-Qarni [92] affirms our findings that health care organizations must have an evolving policy that aligns with emerging technological trends and cyber threats, along with a continuous upgrade and backup plan.

Various schools of thought advocate addressing cybersecurity vulnerabilities in health care systems through a sociotechnical approach, rather than relying solely on technical or social perspectives. Invariably, studies support holistic and joint optimization approaches [11,17,126,127].

The concept of applying a sociotechnical perspective to cybersecurity in the health care domain has received little attention over the years, and the notion of a sociotechnical perspective on cybersecurity in health care is still evolving. Nevertheless, for cybersecurity in health care, a myriad of perspectives, such as a social perspective [24], a cybersecurity perspective [10,20], a sociotechnical perspective [12], the NIST perspective [45], an organizational perspective [104], and a knowledge management perspective [5] have been applied. In this study, cybersecurity challenges and issues were addressed in health care organizations from an outstanding approach of the sociotechnical viewpoint by developing the sociotechnical cybersecurity framework; this is a novel instance of the theoretical contributions (Figure 3).

In the quest for solutions, scholars have developed various frameworks that contribute to the theory of cybersecurity in health care. Rehman et al [55] proposed a framework for a secure health monitoring system in health care 5.0 and used blockchain technology and an intrusion detection system to detect any malicious activity in health care networks. Wazid et al [53] proposed a framework for generalized secure healthcare 5.0 to provide solutions for the challenges in health care systems. Furthermore, Jalali et al [88] proposed the Eight Aggregated Response Strategies (EARSs) framework for cybersecurity incidents. In this context, the CKMIR model differs from the secure health monitoring model [55] in the configuration of its elements. Further, the CKMIR model differs from the secure healthcare 5.0 model [53] in its capability to respond to numerous simultaneous cyberattacks. Additionally, our proposed model optimized cybersecurity response capabilities compared to the EARS model [88]. The incident reporting and vulnerability analysis are automated and embedded within our model, unlike in the EARS model. Generally, the CKMIR model differs from existing models in its components' compatibility, design, and joint optimization of the technology, humans, and processes in preventing vulnerabilities and responding to cyberattacks.

This study contributes to existing cybersecurity theory in several ways, taking an entirely different approach. One way is through the thematic classification of technology, human, and process-related factors of vulnerabilities to cyberattacks in health care systems in their descriptive format (Tables 2-4). It highlights the 3 constructs of sociotechnical-related factors of vulnerabilities to cyberattacks relative to their subfactors in health care systems. The second contribution is an in-depth analytical synthesis of the taxonomy factors of vulnerabilities to cyberattacks. It highlights such factors relative to their subfactors in health care systems (Table 5). The main contribution is the development of the conceptual sociotechnical cybersecurity framework for health care systems (Figure 3). The framework identifies and prevents vulnerabilities and responds to threats and cyberattacks. The proposed framework provides the foundation for understanding the connection and

integration of the factors of vulnerabilities (technology, humans, and processes) to cyberattacks and threats from a sociotechnical perspective in health care systems. It presents a comprehensive approach that is important for fostering and supporting the current understanding of cybersecurity from a sociotechnical lens in health care systems.

Limitations

This study included only papers published in English. Gray literature was not examined. Reports, research-in-progress papers, editorial papers, and inaccessible papers were also excluded. Furthermore, papers outside the study's context were excluded. Cybersecurity in health care papers from a sociotechnical perspective were rarely available.

Conclusions

The sociotechnical perspective of cybersecurity is a critical prerequisite and foundation for resolving vulnerabilities and preventing cyberattacks, breaches, and threats in a complex health care system. This study used a scoping review to examine the dynamics of the factors of vulnerabilities to cyberattacks and develop the sociotechnical cybersecurity framework for preventing vulnerabilities and responding to threats and cyberattacks in health care systems. Furthermore, this study also presents the compliance standards for the application of the conceptual framework to guide health care organizations' cybersecurity practices. This study examined the landscape of cybersecurity vulnerabilities and confirmed that an interplay exists among the 3 sociotechnical themes of technology, humans, and processes.

Despite the growing benefits of technology, this study observed that the increasing number of breaches and cyberattacks is linked to the unpreparedness of health care organizations, a lack of compliance, communication issues, irregular adverse assessments, and a lack of timely response to cybersecurity incidents and proper monitoring. It should be noted that online and offline backup and recovery plans are important for mitigating incidents. Health care organizations that embed a culture of inclusiveness and training with the necessary skills can eliminate insider threats and cyberattacks in health care systems. To address the vulnerabilities related to complexities in system design, health care organizations must ensure that priority is given to cybersecurity and user-centered designs for processes and the technological integration, application, and implementation of critical health care infrastructure as a sociotechnical approach [27,54]. This includes implementing security design and multifactor authentication instructions, secure text display, cryptographic instructions, tokenization, and alert triggers to providers and legitimate users to control system security operations. This implementation can affect usability and complex design from the patients' and providers' points of view to track intrusions, detect abnormalities, and prevent unlawful access to health information.

The proposed conceptual sociotechnical cybersecurity framework provides a comprehensive and explicit overview of the sociotechnical foundations of vulnerabilities (technology, human factors, and processes) in health care systems.

In spite of the existing generic cybersecurity frameworks from a sociotechnical perspective to tackle issues of vulnerabilities and cyberattacks in organizations, the framework is important for its suitability, applicability, and customization to a dynamic and complex health care system.

In addition to further research to empirically validate the proposed framework for accuracy, feasibility, and effectiveness in health care organizations, there is also a need to investigate the adoption of blockchain technology for accelerating incident response processes in health care systems.

Acknowledgments

The author is grateful to the Finnish Cultural Foundation for its support in funding this research.

Authors' Contributions

PE was responsible for this study's design, quality appraisal, screening, data extraction, synthesis of results, and paper preparation. TV contributed by providing inputs and advice on protocols, data extraction, and eligibility criteria, as well as screening papers, abstracts, and full texts. Additionally, TV played a significant role in shaping this paper by offering critical feedback on the draft for continuous improvement. TM provided guidance, data collection, and comments on the revised paper.

Conflicts of Interest

None declared.

Multimedia Appendix 1

PRISMA-ScR checklist.
[PDF File (Adobe PDF File), 101 KB-Multimedia Appendix 1]

Multimedia Appendix 2

Detailed search strategy.
[DOCX File , 15 KB-Multimedia Appendix 2]

Multimedia Appendix 3

Characteristics of the included studies.
[DOCX File , 51 KB-Multimedia Appendix 3]

Multimedia Appendix 4

Critical appraisal.
[DOCX File , 35 KB-Multimedia Appendix 4]

Multimedia Appendix 5

Quality appraisal grouped by study method.
[DOCX File , 17 KB-Multimedia Appendix 5]

Multimedia Appendix 6

Practical implementation steps for the conceptual framework.
[DOCX File , 165 KB-Multimedia Appendix 6]

Multimedia Appendix 7

The compliance standards to guide the conceptual framework.
[DOCX File , 19 KB-Multimedia Appendix 7]

References

1. Kioskli K, Fotis T, Mouratidis H. The landscape of cybersecurity vulnerabilities and challenges in healthcare: security standards and paradigm shift recommendations. 2021. Presented at: ARES '21: Proceedings of the 16th International Conference on Availability, Reliability and Security; August 17-20, 2021:1-9; Vienna, Austria. [doi: 10.1145/3465481.3470033]
2. Slayton R. Governing uncertainty or uncertain governance? Information security and the challenge of cutting ties. Sci, Tech, Hum Values. 2020;46(1):81-111. [doi: 10.1177/0162243919901159]
3. Wurm J, Jin Y, Liu Y, Hu S, Heffner K, Rahman F, et al. Introduction to cyber-physical system security: a cross-layer perspective. IEEE Trans Multi-Scale Comput Syst. 2017;3(3):215-227. [doi: 10.1109/tmscs.2016.2569446]
4. Dias FM, Martens ML, Monken SFDP, Silva LFD, Santibanez-Gonzalez EDR. Risk management focusing on the best practices of data security systems for healthcare. Int J Innovation. 2021;9(1):45-78. [doi: 10.5585/iji.v9i1.18246]
5. Wang S, Wang H. A sociotechnical systems analysis of knowledge management for cybersecurity. Int J Sociotechnol Knowl Dev. 2021;13(3):77-94. [doi: 10.4018/ijskd.2021070105]
6. Kaberuka J, Johnson C. Case studies in the socio-technical analysis of cybersecurity incidents: comparing attacks on the UK NHS and irish healthcare systems. 2022. Presented at: Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media; June 20–21, 2022:357-387; Wales. [doi: 10.1007/978-981-19-6414-5_21]
7. Kaberuka J, Johnson C. Adapting STPA-sec for socio-technical cyber security challenges in emerging nations: a case study in risk management for Rwandan health care. 2020. Presented at: International Conference on Cyber Security and Protection of Digital Services (Cyber Security); 2020 June 15-19; Dublin, Ireland. [doi: 10.1109/cybersecurity49315.2020.9138863]
8. Kissel R. Glossary of key information security terms glossary of key information security terms. The National Institute of Standards and Technology. 2013. URL: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf [accessed 2025-09-13]
9. Zhan Y, Ahmad SF, Irshad M, Al-Razgan M, Awwad EM, Ali YA, et al. Investigating the role of cybersecurity's perceived threats in the adoption of health information systems. Heliyon. 2024;10(1):e22947. [FREE Full text] [doi: 10.1016/j.heliyon.2023.e22947] [Medline: 38148811]
10. Anastasopoulou K, Mari P, Magkanaraki A, Spanakis E, Merialdo M, Sakkalis V. Public and private healthcare organisations: a socio-technical model for identifying cybersecurity aspects. 2020. Presented at: ICEGOV '20: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance; September 23-25, 2020:168-175; Athens, Greece. [doi: 10.1145/3428502.3428525]
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. Intell Natl Security. 2020;35(4):556-585. [doi: 10.1080/02684527.2020.1752459]
12. Sittig D, Singh H. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Appl Clin Inform. 2016;7(2):624-632. [FREE Full text] [doi: 10.4338/ACI-2016-04-SOA-0064] [Medline: 27437066]
13. Abdi A, Bennouri H, Keane A. 2024. Presented at: 13th Mediterranean Conference on Embedded Computing (MECO); June 11-14, 2024:1-8; Budva, Montenegro. [doi: 10.1109/meco62516.2024.10577790]

14. Health sector cybersecurity: 2021 retrospective and 2022 look ahead. Health and Human Services. URL: https://www.hhs.gov/sites/default/files/2021-retrospective-and-2022-look-ahead-tlpwhite.pdf [accessed 2025-09-13]
15. Lasky S. WannaCry ransomware worm attacks the world. SecurityInfoWatch.com. 2017. URL: https://www.securityinfowatch.com/cybersecurity/information-security/article/12334948/wannacry-ransomware-worm-attacks-the-world [accessed 2025-09-13]
16. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas. 2018;113:48-52. [FREE Full text] [doi: 10.1016/j.maturitas.2018.04.008] [Medline: 29903648]
17. Malatji M, Von Solms S, Marnewick A. Socio-technical systems cybersecurity framework. ICS. 2019;27(2):233-272. [doi: 10.1108/ics-03-2018-0031]
18. Argaw ST, Bempong N, 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(1):10. [FREE Full text] [doi: 10.1186/s12911-018-0724-5] [Medline: 30634962]
19. Argaw ST, Troncoso-Pastoriza JR, Lacey D, Florin M, 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(1):146. [FREE Full text] [doi: 10.1186/s12911-020-01161-7] [Medline: 32620167]
20. Garcia-Perez A, Cegarra-Navarro JG, Sallos MP, Martinez-Caro E, Chinnaswamy A. Resilience in healthcare systems: cyber security and digital transformation. Technovation. 2023;121:102583. [doi: 10.1016/j.technovation.2022.102583]
21. Szczepaniuk H, Szczepaniuk EK. Cryptographic evidence-based cybersecurity for smart healthcare systems. Inf Sci. 2023;649:119633. [doi: 10.1016/j.ins.2023.119633]
22. Vukotich G. Healthcare and cybersecurity: taking a zero trust approach. Health Serv Insights. 2023;16:11786329231187826. [FREE Full text] [doi: 10.1177/11786329231187826] [Medline: 37485022]
23. Zimmermann V, Renaud K. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. Int J Hum-Comput Stud. 2019;131:169-187. [doi: 10.1016/j.ijhcs.2019.05.005]
24. Nicho M, McDermott C. Dimensions of 'Socio' vulnerabilities of advanced persistent threats. IEEE; 2019. Presented at: International Conference on Software, Telecommunications and Computer Networks (SoftCOM); September 19-21, 2019:1-5; Split, Croatia. [doi: 10.23919/softcom.2019.8903788]
25. Malatji M, Marnewick A, von Solms S. Validation of a socio-technical management process for optimising cybersecurity practices. Comput Secur. 2020;95:101846. [doi: 10.1016/j.cose.2020.101846]
26. Svandova K, Smutny Z. Internet of medical things security frameworks for risk assessment and management: a scoping review. J Multidiscip Healthc. 2024;17:2281-2301. [FREE Full text] [doi: 10.2147/JMDH.S459987] [Medline: 38765613]
27. Ewoh P, Vartiainen T. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. J Med Internet Res. 2024;26:e46904. [FREE Full text] [doi: 10.2196/46904] [Medline: 38820579]
28. Wani TA, Mendoza A, Gray K. A sociotechnical approach to bring-your-own-device security in hospitals: development and pilot testing of a maturity model using mixed methods action research. JMIR Hum Factors. 2025;12:e71912. [FREE Full text] [doi: 10.2196/71912] [Medline: 40802372]
29. Sutton A, Tompson L. Towards a cybersecurity culture-behaviour framework: a rapid evidence review. Comput Secur. 2025;148:104110. [doi: 10.1016/j.cose.2024.104110]
30. Mozzaquatro BA, Agostinho C, Goncalves D, Martins J, Jardim-Goncalves R. An ontology-based cybersecurity framework for the internet of things. Sensors (Basel). 2018;18(9):3053. [FREE Full text] [doi: 10.3390/s18093053] [Medline: 30213085]
31. Mtsweni J, Gcaza N, Thaba M. A unified cybersecurity framework for complex environments. 2018. Presented at: SAICSIT '18: Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists; September 26-28, 2018:1-9; Port Elizabeth South Africa. [doi: 10.1145/3278681.3278682]
32. Davis MC, Challenger R, Jayewardene DN, Clegg CW. Advancing socio-technical systems thinking: a call for bravery. Appl Ergon. 2014;45(2, Part A):171-180. [FREE Full text] [doi: 10.1016/j.apergo.2013.02.009] [Medline: 23664481]
33. Trist EL. Towards A Social Ecology: Contextual Appreciation of the Future in the Present. London; New York. Plenum Press; 1973.
34. Appelbaum SH. Socio‐technical systems theory: an intervention strategy for organizational development. Manage Decis. 1997;35(6):452-463. [doi: 10.1108/00251749710173823]
35. Mumford E. The story of socio‐technical design: reflections on its successes, failures and potential. Inf Syst J. 2006;16(4):317-342. [doi: 10.1111/j.1365-2575.2006.00221.x]
36. Emery F. Sociotechnical foundations for a new social order? Hum Relat. 1982;35(12):1095-1122. [doi: 10.1177/001872678203501203]
37. Trist E. The evolution of socio-technical systems. Conf Organ Des Perform. 1981. URL: https://sistemas-humano-computacionais.wdfiles.com/local--files/capitulo%3Aredes-socio-tecnicas/Evolution_of_socio_technical_systems.pdf [accessed 2025-09-28]
38. Baxter G, Sommerville I. Socio-technical systems: from design methods to systems engineering. Interact Comput. 2011;23(1):4-17. [doi: 10.1016/j.intcom.2010.07.003]
39. Arksey H, O'Malley L. Scoping studies: towards a methodological framework. Int J Soc Res Methodol. 2005;8(1):19-32. [doi: 10.1080/1364557032000119616]

40. Tricco AC, Lillie E, Zarin W, O'Brien KK, Colquhoun H, Levac D, et al. PRISMA Extension for Scoping Reviews (PRISMA-ScR): checklist and explanation. Ann Intern Med. 2018;169(7):467-473. [FREE Full text] [doi: 10.7326/M18-0850] [Medline: 30178033]
41. Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare challenges in the era of cybersecurity. Health Secur. 2020;18(3):228-231. [doi: 10.1089/hs.2019.0123] [Medline: 32559153]
42. Arafa A, Sheerah H, Alsalamah S. Emerging digital technologies in healthcare with a spotlight on cybersecurity: a narrative review. information. 2023;14(12):640. [doi: 10.3390/info14120640]
43. He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. J Med Internet Res. 2021;23(4):e21747. [FREE Full text] [doi: 10.2196/21747] [Medline: 33764885]
44. Alhammad A, Yusof MM, Jambari DI. A review of cyber threats to medical devices integration with electronic medical records. 2022. Presented at: International Conference on Cyber Resilience (ICCR); October 06-07, 2022; Dubai, United Arab Emirates. [doi: 10.1109/iccr56254.2022.9995984]
45. Kandasamy K, Srinivas S, Achuthan K, Rangan VP. Digital healthcare - cyberattacks in Asian organizations: an analysis of vulnerabilities, risks, NIST perspectives, and recommendations. IEEE Access. 2022;10:12345-12364. [doi: 10.1109/access.2022.3145372]
46. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care. 2017;25(1):1-10. [FREE Full text] [doi: 10.3233/THC-161263] [Medline: 27689562]
47. Pool J, Akhlaghpour S, Fatehi F, Burton-Jones A. A systematic analysis of failures in protecting personal health data: a scoping review. Int J Inf Manage. 2024;74:102719. [doi: 10.1016/j.ijinfomgt.2023.102719]
48. Cartwright AJ. The elephant in the room: cybersecurity in healthcare. J Clin Monit Comput. 2023;37(5):1123-1132. [FREE Full text] [doi: 10.1007/s10877-023-01013-5] [Medline: 37088852]
49. Calyam P, Kejriwal M, Rao P, Cheng J, Wang W, Bai L. Towards a domain-agnostic knowledge graph-as-a-service infrastructure for active cyber defense with intelligent agents. 2023. Presented at: IEEE Applied Imagery Pattern Recognition Workshop (AIPR); September 27-29, 2023; St. Louis, MO. [doi: 10.1109/aipr60534.2023.10440708]
50. Messinis S, Temenos N, Protonotarios NE, Rallis I, Kalogeras D, Doulamis N. Enhancing internet of medical things security with artificial intelligence: a comprehensive review. Comput Biol Med. 2024;170:108036. [FREE Full text] [doi: 10.1016/j.compbiomed.2024.108036] [Medline: 38295478]
51. Lopatina K, Dokuchaev V, Maklachkova VV. Data risks identification in healthcare sensor networks. 2021. Presented at: International Conference on Engineering Management of Communication and Technology (EMCTECH); October 20-22, 2021; Vienna, Austria. [doi: 10.1109/emctech53459.2021.9619178]
52. Filipec O, Plášil D. The cybersecurity of healthcare the case of the Benešov hospital hit by Ryuk ransomware, and lessons learned. OaS. 2021;21(1):27-52. [doi: 10.3849/1802-7199.21.2021.01.027-052]
53. Wazid M, Das AK, Mohd N, Park Y. Healthcare 5.0 security framework: applications, issues and future research directions. IEEE Access. 2022;10:129429-129442. [doi: 10.1109/access.2022.3228505]
54. Ogunniye G, Hana A, Watson J. PETRAS: a socio-technical framework for internet of things research and development. Front Internet Things. 2024;3:1336564. [FREE Full text] [doi: 10.3389/friot.2024.1336564]
55. Rehman A, Abbas S, Khan M, Ghazal T, Adnan K, Mosavi A. A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. Comput Biol Med. 2022;150:106019. [doi: 10.31219/osf.io/gvkqc]
56. Semancik J, Wells A. Techniques to maximize O-level cyber security protection. 2023. Presented at: IEEE AUTOTESTCON; August 28-31, 2023; National Harbor, MD. [doi: 10.1109/autotestcon47464.2023.10296266]
57. Giansanti D. Cybersecurity and the digital-health: the challenge of this millennium. Healthcare (Basel). 2021;9(1):62. [FREE Full text] [doi: 10.3390/healthcare9010062] [Medline: 33440612]
58. Lee I. Analyzing web descriptions of cybersecurity breaches in the healthcare provider sector: a content analytics research method. Comput Secur. 2023;129:103185. [doi: 10.1016/j.cose.2023.103185]
59. Arora S, Yttri J, Nilse W. Privacy and security in mobile health (mHealth) research. Alcohol Res. 2014;36(1):143-152. [FREE Full text] [Medline: 26259009]
60. Wang Z, Huo Z, Shi W. A dynamic identity based authentication scheme using chaotic maps for telecare medicine information systems. J Med Syst. 2015;39(1):158. [doi: 10.1007/s10916-014-0158-2] [Medline: 25486894]
61. Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: insights from the U.S. healthcare industry. Bus Horiz. 2019;62(4):539-548. [doi: 10.1016/j.bushor.2019.03.010]
62. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps review for the non-cyber professional. Front Digit Health. 2022;4:862221. [FREE Full text] [doi: 10.3389/fdgth.2022.862221]
63. Janith K, Iddagoda R, Gunawardena C, Sankalpa K, Abeywardena K, Yapa K. SentinelPlus: a cost-effective cyber security solution for healthcare organizations. In.; 2021. Presented at: ICAC 2021 - 3rd International Conference on Advancements in Computing, Proceedings; December 09-11, 2021:359-364; Colombo, Sri Lanka. [doi: 10.1109/icac54203.2021.9670892]
64. Dameff CJ, Selzer JA, Fisher J, Killeen JP, Tully JL. Clinical cybersecurity training through novel high-fidelity simulations. J Emerg Med. 2019;56(2):233-238. [doi: 10.1016/j.jemermed.2018.10.029] [Medline: 30553562]

65. Feeley A, Lee M, Crowley M, Feeley I, Roopnarinesingh R, Geraghty S, et al. Under viral attack: an orthopaedic response to challenges faced by regional referral centres during a national cyber-attack. Surgeon. 2022;20(5):334-338. [doi: 10.1016/j.surge.2021.09.007] [Medline: 34782238]
66. Beaman C, Barkworth A, Akande TD, Hakak S, Khan MK. Ransomware: recent advances, analysis, challenges and future research directions. Comput Secur. 2021;111:102490. [FREE Full text] [doi: 10.1016/j.cose.2021.102490] [Medline: 34602684]
67. Hijji M, Alam G. A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. IEEE Access. 2021;9:7152-7169. [FREE Full text] [doi: 10.1109/ACCESS.2020.3048839] [Medline: 34786300]
68. Fernando J, Dawson L. The natural hospital environment: a socio-technical-material perspective. Int J Med Inform. 2014;83(2):140-158. [doi: 10.1016/j.ijmedinf.2013.10.008] [Medline: 24286731]
69. Pranggono B, Arabo A. COVID-19 pandemic cybersecurity issues. Internet Technol Lett. 2021;4(2):e247. [doi: 10.1002/itl2.247]
70. Wilner AS, Luce H, Ouellet E, Williams O, Costa N. From public health to cyber hygiene: cybersecurity and Canada's healthcare sector. Int J. 2022;76(4):522-543. [doi: 10.1177/00207020211067946]
71. DeFord D. Sustainable digital health demands cybersecurity transformation. Front Health Serv Manage. 2022;38(3):31-38. [doi: 10.1097/HAP.0000000000000137] [Medline: 35191859]
72. Hines E, Trivedi S, Hoang-Tran C, Mocharnuk J, Pfaff M. Perspectives on cybersecurity and plastic surgery: a survey of plastic surgeons and scoping review of the literature. Aesthet Surg J. 2023;43(11):1376-1383. [doi: 10.1093/asj/sjad122] [Medline: 37186025]
73. Gordon W, Wright A, Glynn R, Kadakia J, Mazzone C, Leinbach E, et al. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. J Am Med Inf Assoc. 2019;26(6):547-552. [FREE Full text] [doi: 10.1093/jamia/ocz005] [Medline: 30861069]
74. Ireland CA, Ireland JL, Jones NS, Chu S, Lewis M. Predicting security incidents in high secure male psychiatric care. Int J Law Psychiatry. 2019;64:40-52. [doi: 10.1016/j.ijlp.2019.01.004] [Medline: 31122639]
75. Sekandi JN, Murray K, Berryman C, Davis-Olwell P, Hurst C, Kakaire R, et al. Ethical, legal, and sociocultural issues in the use of mobile technologies and call detail records data for public health in the East African region: scoping review. Interact J Med Res. 2022;11(1):e35062. [FREE Full text] [doi: 10.2196/35062] [Medline: 35533323]
76. Yeng PK, Szekeres A, Yang B, Snekkenes EA. Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: systematic mapping study. JMIR Hum Factors. 2021;8(2):e17604. [FREE Full text] [doi: 10.2196/17604] [Medline: 34106077]
77. Alfawzan N, Christen M, Spitale G, Biller-Andorno N. Privacy, data sharing, and data security policies of women's mHealth apps: scoping review and content analysis. JMIR mHealth uHealth. 2022;10(5):e33735. [FREE Full text] [doi: 10.2196/33735] [Medline: 35522465]
78. Monteith S, Bauer M, Alda M, Geddes J, Whybrow PC, Glenn T. Increasing cybercrime since the pandemic: concerns for psychiatry. Curr Psychiatry Rep. 2021;23(4):18. [FREE Full text] [doi: 10.1007/s11920-021-01228-w] [Medline: 33660091]
79. Sari PK, Handayani PW, Hidayanto AN, Yazid S, Aji RF. Information security behavior in health information systems: a review of research trends and antecedent factors. Healthcare (Basel). 2022;10(12):2531. [FREE Full text] [doi: 10.3390/healthcare10122531] [Medline: 36554055]
80. Coventry L, Branley-Bell D, Sillence E, Magalini S, Mari P, Magkanaraki A. Cyber-risk in healthcare: exploring facilitators and barriers to secure behavior. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2020. URL: https://scispace.com/pdf/cyber-risk-in-healthcare-exploring-facilitators-and-barriers-1kmegfd0ff.pdf [accessed 2025-09-28]
81. Branley-Bell D, Coventry L, Sillence E, Magalini S, Mari P, Magkanaraki A, et al. Your hospital needs you: eliciting positive cybersecurity behaviours from healthcare staff. Ann Disaster Risk Sci. 2020;3(1). [doi: 10.51381/adrs.v3i1.51]
82. Abbou B, Kessel B, Natan MB, Gabbay-Benziv R, Dahan Shriki D, Ophir A, et al. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Front Digit Health. 2024;6:1321485. [FREE Full text] [doi: 10.3389/fdgth.2024.1321485] [Medline: 38433989]
83. Harrison AS, Sullivan P, Kubli A, Wilson KM, Taylor A, DeGregorio N, et al. How to respond to a ransomware attack? One radiation oncology department's response to a cyber-attack on their record and verify system. Pract Radiat Oncol. 2022;12(2):170-174. [doi: 10.1016/j.prro.2021.09.011] [Medline: 34644601]
84. Mohammed Z. Data breach recovery areas: an exploration of organization's recovery strategies for surviving data breaches. OCJ. 2022;2(1):41-59. [doi: 10.1108/ocj-05-2021-0014]
85. Keogh RJ, Harvey H, Brady C, Hassett E, Costelloe SJ, O'Sullivan MJ, et al. Dealing with digital paralysis: surviving a cyberattack in a national cancer center. J Cancer Policy. 2024;39:100466. [doi: 10.1016/j.jcpo.2023.100466] [Medline: 38176467]
86. 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(5):98. [doi: 10.1007/s10916-019-1507-y] [Medline: 32239357]

87. He Y, Maglaras L, Aliyu A, Luo C. Healthcare security incident response strategy - a proactive incident response (IR) procedure. Secur Commun Networks. 2022;2022(1):2775249. [doi: 10.1155/2022/2775249]
88. Jalali M, Russell B, Razak S, Gordon W. EARS to cyber incidents in health care. J Am Med Inf Assoc. 2019;26(1):81-90. [FREE Full text] [doi: 10.1093/jamia/ocy148] [Medline: 30517701]
89. Lohrke FT, Frownfelter-Lohrke C. Cybersecurity research from a management perspective: a systematic literature review and future research agenda. J Gen Manage. 2023. [doi: 10.1177/03063070231200512]
90. McEvoy TR, Kowalski SJ. Deriving cyber security risks from human and organizational factors – a socio-technical approach. CSIMQ. 2019;(18):47-64. [doi: 10.7250/csimq.2019-18.03]
91. Tin D, Hata R, Granholm F, Ciottone RG, Staynings R, Ciottone GR. Cyberthreats: a primer for healthcare professionals. Am J Emerg Med. 2023;68:179-185. [doi: 10.1016/j.ajem.2023.04.001] [Medline: 37061434]
92. Al-Qarni EA. Cybersecurity in healthcare: a review of recent attacks and mitigation strategies [internet]. Int J Adv Comput Sci Appl. 2023;14(5):135-140. [FREE Full text] [doi: 10.14569/IJACSA.2023.0140513]
93. Patel B, Makaryus AN. The implications of cardiac device cybersecurity responsibilities and challenges faced by policymakers, manufacturers, and patients. Expert Rev Pharmacoecon Outcomes Res. 2024;24(6):743-747. [doi: 10.1080/14737167.2024.2361076] [Medline: 38808954]
94. Parmeggiani D, Moccia G, Torelli F, Miele F, Luongo P, Sperlongano P. The adoption of a cybersecurity framework in a healthcare, surgical and oncological environment: Synergy-net a Campania FESR-POR (European Fund of Regional Development-Regional Operative Program) research project. Onkologia i Radioterapia. 2024;18(7):1-7.
95. Grande D, Luna Marti X, Feuerstein-Simon R, Merchant RM, Asch DA, Lewson A, et al. Health policy and privacy challenges associated with digital technology. JAMA Netw Open. 2020;3(7):e208285. [FREE Full text] [doi: 10.1001/jamanetworkopen.2020.8285] [Medline: 32644138]
96. Khando K, Gao S, Islam SM, Salman A. Enhancing employees information security awareness in private and public organisations: a systematic literature review. Comput Secur. 2021;106:102267. [doi: 10.1016/j.cose.2021.102267]
97. Alhassani ND, Windle R, Konstantinidis ST. A scoping review of the drivers and barriers influencing healthcare professionals' behavioral intentions to comply with electronic health record data privacy policy. Health Informatics J. 2024;30(4):14604582241296398. [FREE Full text] [doi: 10.1177/14604582241296398] [Medline: 39435737]
98. Sullivan N, Tully J, Dameff C, Opara C, Snead M, Selzer J. A national survey of hospital cyber attack emergency operation preparedness. Disaster Med Public Health Prep. 2023;17:e363. [doi: 10.1017/dmp.2022.283] [Medline: 36945857]
99. Giansanti D, Monoscalco L. The cyber-risk in cardiology: towards an investigation on the self-perception among the cardiologists. mHealth. 2021;7:1-5. [FREE Full text] [doi: 10.21037/mhealth.2020.01.08] [Medline: 33898597]
100. Lockwood, Munn Z, Porritt K. Qualitative research synthesis: methodological guidance for systematic reviewers utilizing meta-aggregation. Int J Evid Based Healthc. 2015;13(3):179-187. [doi: 10.1097/XEB.0000000000000062] [Medline: 26262565]
101. Hong QN, Fàbregues S, Bartlett G, Boardman F, Cargo M, Dagenais P, et al. The mixed methods appraisal tool (MMAT) version 2018 for information professionals and researchers. EFI. 2018;34(4):285-291. [doi: 10.3233/efi-180221]
102. Critical appraisal checklist for cross-sectional study. Center for Evidence Based Management. 2014. URL: https://cebma.org/assets/Uploads/Critical-Appraisal-Questions-for-a-Cross-Sectional-Study-July-2014-1-v2.pdf [accessed 2025-09-16]
103. Baethge, Goldbeck-Wood S, Mertens S. SANRA-a scale for the quality assessment of narrative review articles. Res Integr Peer Rev. 2019;4:5. [FREE Full text] [doi: 10.1186/s41073-019-0064-8] [Medline: 30962953]
104. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res. 2018;20(5):e10059. [FREE Full text] [doi: 10.2196/10059] [Medline: 29807882]
105. Peters M, Godfrey C, McInerney P, Munn Z, Tricco A, Khalil H. Chapter 11: scoping reviews. JBI manual for evidence synthesis. 2020. URL: https://jbi-global-wiki.refined.site/space/MANUAL/355863557/Previous+versions?attachment=/download/attachments/355863557/JBI_Reviewers_Manual_2020June.pdf&type=application/pdf&filename=JBI_Reviewers_Manual_2020June.pdf#page=406 [accessed 2025-09-28]
106. Braun V, Clarke V. Using thematic analysis in psychology. Qual Res Psychol. 2008;3(2):77-101. [doi: 10.1191/1478088706qp063oa]
107. Fernández Maimó L, Huertas Celdrán A, Perales Gómez ÁL, García Clemente FJ, Weimer J, Lee I. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors (Basel). 2019;19(5):1114. [FREE Full text] [doi: 10.3390/s19051114] [Medline: 30841592]
108. Loi M, Christen M, Kleine N, Weber K. Cybersecurity in health – disentangling value tensions. JICES. 2019;17(2):229-245. [doi: 10.1108/jices-12-2018-0095]
109. Iqbal MJ, Aurangzeb S, Aleem M, Srivastava G, Lin JC. RThreatDroid: a ransomware detection approach to secure IoT based healthcare systems. IEEE Trans Netw Sci Eng. 2023;10(5):2574-2583. [doi: 10.1109/tnse.2022.3188597]
110. Ghanbari H, Vartiainen T, Siponen M. Omission of quality software development practices. ACM Comput Surv. 2018;51(2):1-27. [doi: 10.1145/3177746]
111. Ghafir I, Prenosil V, Hammoudeh M, Baker T, Jabbar S, Khalid S, et al. BotDet: a system for real time botnet command and control traffic detection. IEEE Access. 2018;6:38947-38958. [doi: 10.1109/access.2018.2846740]

112. Loughlin S, Fu K, Gee T, Gieras I, Hoyme K, Rajagopalan SR, et al. A roundtable discussion: safeguarding information and resources against emerging cybersecurity threats. Biomed Instrum Technol. 2014;48(s1):8-17. [doi: 10.2345/0899-8205-48.s1.8] [Medline: 24848144]
113. Yang J, Li J, Niu Y. A hybrid solution for privacy preserving medical data sharing in the cloud environment. Future Gener Comput Syst. 2015;43-44:74-86. [doi: 10.1016/j.future.2014.06.004]
114. Zorabedian J. How Malware Works: Anatomy of Drive-By Download Web Attack. Boston.; 2014. URL: https://news.sophos.com/en-us/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/ [accessed 2025-09-16]
115. Ackerman L. Mobile health and fitness applications and information privacy. Protection Foundation. Privacy Rights Clearinghouse. 2013. URL: https://privacyrights.org/ [accessed 2025-09-16]
116. Jalali MS, Razak S, Gordon W, Perakslis E, Madnick S. Health care and cybersecurity: bibliometric analysis of the literature. J Med Internet Res. 2019;21(2):e12644. [FREE Full text] [doi: 10.2196/12644] [Medline: 30767908]
117. Williams P, Woodward A. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices (Auckl). 2015;8:305-316. [FREE Full text] [doi: 10.2147/MDER.S50048] [Medline: 26229513]
118. Borky J, Bradley T. Protecting information with cybersecurity. In: Effective Model-Based Systems Engineering. Cham. Springer International Publishing; 2019.
119. Insider threat report 2024. Cybersecurity Insider. 2024. URL: https://www.cybersecurity-insiders.com/2024-insider-threat-report/ [accessed 2025-09-16]
120. Pollini A, Callari TC, Tedeschi A, Ruscio D, Save L, Chiarugi F, et al. Leveraging human factors in cybersecurity: an integrated methodological approach. Cogn Technol Work. 2022;24(2):371-390. [FREE Full text] [doi: 10.1007/s10111-021-00683-y] [Medline: 34149309]
121. Wani TA, Mendoza A, Gray K. BYOD security behaviour and preferences among hospital clinicians - a qualitative study. Int J Med Inform. 2024;192:105606. [FREE Full text] [doi: 10.1016/j.ijmedinf.2024.105606] [Medline: 39226635]
122. Jalali MS, Siegel M, Madnick S. Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment. J Strategic Inf Syst. 2019;28(1):66-82. [doi: 10.1016/j.jsis.2018.09.003]
123. Pham T, Loo T, Malhotra A, Longhurst C, Hylton D, Dameff C, et al. Ransomware cyberattack associated with cardiac arrest incidence and outcomes at untargeted, adjacent hospitals. Crit Care Explor. 2024;6(4):e1079. [FREE Full text] [doi: 10.1097/CCE.0000000000001079] [Medline: 38605720]
124. Cybersecurity framework 2.0. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [accessed 2025-09-16]
125. Badidi E, Lamaazi H. Toward a secure healthcare ecosystem: a convergence of edge analytics, blockchain, and federated learning. 2024. Presented at: 20th International Conference on the Design of Reliable Communication Networks (DRCN); 2024 May 06-09; Montreal, QC, Canada. [doi: 10.1109/drcn60692.2024.10539174]
126. Carayon P, Hancock P, Leveson N, Noy I, Sznelwar L, van Hootegem G. Advancing a sociotechnical systems approach to workplace safety--developing the conceptual framework. Ergonomics. 2015;58(4):548-564. [FREE Full text] [doi: 10.1080/00140139.2015.1015623] [Medline: 25831959]
127. Perrotin P, Belloir N, Sadou S, Hairion D, Beugnard A. Using the architecture of socio-technical system to analyse its vulnerability. 2022. Presented at: 17th Annual System of Systems Engineering Conference (SOSE); June 07-11, 2022; Rochester, NY. [doi: 10.1109/sose55472.2022.9812648]

Abbreviations

CKMIR: cybersecurity knowledge management and intelligence response
EARS: Eight Aggregated Response Strategy
EHR: electronic health record
IoMT: Internet of Medical Things
JBI: Joanna Briggs Institute
NIST: National Institute of Standards and Technology
PRISMA-ScR: Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews
RQ: research question
STAMP: systems theoretic accident model and processes
STS: sociotechnical system

Edited by J Sarvestan; submitted 07.Apr.2025; peer-reviewed by M Krishnapatnam, TA Wani; comments to author 16.Apr.2025; revised version received 11.Jun.2025; accepted 08.Aug.2025; published 15.Oct.2025

Please cite as:
Ewoh P, Vartiainen T, Mantere T
Sociotechnical Cybersecurity Framework for Securing Health Care From Vulnerabilities and Cyberattacks: Scoping Review
J Med Internet Res 2025;27:e75584
URL: https://www.jmir.org/2025/1/e75584
doi: 10.2196/75584
PMID: 40838797

APPENDIX S2

Figure S2 Sociotechnical cybersecurity framework implementation steps

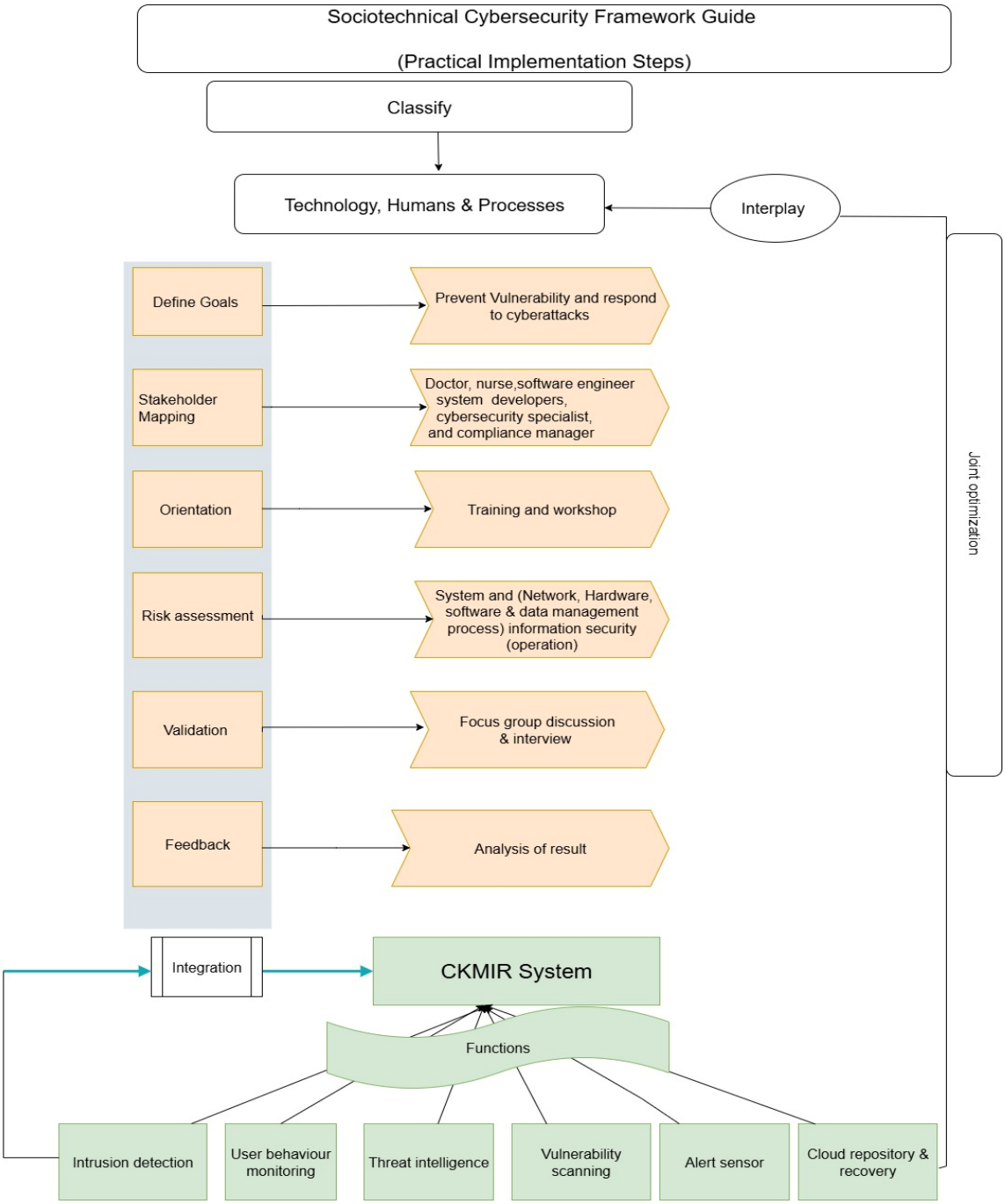


Table S1. The compliance standards to guide the conceptual framework

Factors of vulnerability	Health care organization action plan	Compliance in the health care organization	Responsible role	Reference
Technology				
Lack of regular audit and assessment	Regular cybersecurity assessment audits	The health care organization should conduct a monthly and quarterly audit, vulnerability scanning, and assessment to ensure all vulnerabilities are identified Develop an auditing plan and template	IT team, health care management, compliance officer	[47]
New technology integration	Secure design and technology integration support	Assess security risks before the adoption and integration of new technology Implement security control for IoT devices and applications across health care systems. Integrate secure design features in the early stages of development and during new technology integration Provide self-support and secure guidance	Health care management, procurement manager, original equipment manufacturer (O EM) technology integration expert, compliance officer, IT team	[23,46] [119]
Third-party applications and plugins	Implement third-party application management control	Implement access control and monitor privileges of third-party vendor applications and plugins as they interact with the health care information systems Health care organizations should implement control applications to monitor and manage third-party technologies, software, applications, and plugins	Procurement manager, OEM, integration expert, compliance officer, IT team, health care management	[44]

Factors of vulnerability	Health care organization action plan	Compliance in the health care organization	Responsible role	Reference
Complex system design and usability	User-centered design	Adopt user-friendly design without compromising security Promote the adoption of threat modeling in the design approach by incorporating security first into the design plan to meet all legal and regulatory requirements for data privacy and security	System developer, system integrator, health care management, compliance officer, IT team	[119]
Limited monitoring	Real-time monitoring and alerts	Health care management should engage in continuous monitoring of critical cyber infrastructure, alerting, and automatically counteracting any abnormalities in the network and systems Continuous updates of health care system devices and applications, policies, and training for emerging threats and trends in health care system	IT team, compliance officer, security operation center (SOC), health care management, human resource team	[13,66] [54,64]
Inadequate access control management	Identity and access control systems	Health care organization should implement strong identity and access control in health information systems to enable audit trail and footprint activities	IT team, human resources team, health management, compliance officer	[55]
Human factors				
Shortage of skilled professionals and limited budget	Research and development, talent acquisition, increase budget	Health care organizations should partner with educational institutes on research, knowledge transfer, training, and hiring cybersecurity graduates to reduce shortfalls and explore innovative cybersecurity practices and technologies	Human resource team, IT team, health care management, educational institution	[74,75]

Factors of vulnerability	Health care organization action plan	Compliance in the health care organization	Responsible role	Reference
		Increase budget for cybersecurity management.		
Inefficient training	Initiate cybersecurity educational training and awareness programs	Management should ensure to provide regular cybersecurity training for all health care staff Health care management should provide gamification and phishing simulation training tests for employees to check their level of awareness and reinforce cybersecurity awareness training	Human resource team, compliance officer, health care management	[64,73,120]
Insider threats	Monitoring and behavior analytics	Health care management should implement an organizational cybersecurity culture of inclusiveness, behavioral planning, equal opportunity, and deterrence for all employees Management should implement cybersecurity access and privileges to restrict employees from unauthorized information Implement multifactor authentication if data must be accessed in the health care organization Healthcare should implement clear policies on acceptable use, access control, data handling, and the consequences of violations	Human resource team, compliance officer, IT team, health care management legal policy team, security operation center (SOC)	[73]

Factors of vulnerability	Health care organization action plan	Compliance in the health care organization	Responsible role	Reference
Security culture	Initiate cybersecurity culture and behavioral measures	Health care management and human resources team should conduct behavioral tests to ensure that all employees maintain cyber hygiene	Human resource team, ethics committees, organizational development team, compliance officer, legal policy team, SOC	[78,84]
	Initiate psychological and cultural measures	Control over data encryption policy is critical		[79]
		Healthcare organizations should develop guidelines for management to foster a culture of trust, ethical guidance, and transparency for all employees		
		Organizational development team should provide a support channel to reduce grievances and manage inappropriate behavior that may lead to insecurity in the workplace		[83]
Processes				
Inadequate policy and procedure	Collaborative partnership and information sharing policy	Health care organization should partner with cybersecurity experts for support in technology and operational processes to combat challenges Establish platforms for threat intelligence sharing. Raise awareness of evolving cybersecurity threats and trends for all stakeholders	Human resource team, health care management, compliance officer, support team, IT team, knowledge management consultants	[26,54,74,98] [73]

Factors of vulnerability	Health care organization action plan	Compliance in the health care organization	Responsible role	Reference
		Regular policy reviews and updating cybersecurity policies should be consistent with regulatory requirements and emerging threats		
Untimely incident response and recovery plan	Incident response plan	Develop a contingency and cyber breach incident response and recovery plan in the health care organization Introduce online and offline cloud-based repositories for restoration of health information in the event of a security incident or ransomware attack in the health care system The operational manager should develop and establish a communication plan and quick protocol to respond to incidents in the case of cyberthreats and breaches of health information	IT team, compliance officer, SOC, health care management, human resources, computer emergency response team (CERT)	[54,64,73,90]

Cybersecurity in healthcare: A Checklist Model for security and privacy

Author Pius Ewoh [1]
[1]Affiliation School of Technology and Innovation, University of Vaasa, Vaasa, Finland

*Corresponding author: pius.ewoh@uwasa.fi

Abstract

Electronic Health Record systems (EHRs) are widely adopted due to their ability to provide accurate and comprehensive healthcare management across large healthcare networks. The rise of the internet has facilitated health data exchange, allowing EHRs data sharing through fog and cloud computing. However, digitalization has also led to unauthorized access, cyberattacks, data breaches, and violations of health data in various remote locations, compromising the privacy, safety, and security of sensitive patient information, as a result managerial and operational challenges related to privacy and security, such as breaches of patient data due to operational security lapses, quest for interoperable healthcare and ill intention by cybercriminals and intruders have intensified. This has raised concerns about the reliability of EHRs, despite the benefits of electronic health record (EHR) innovation, limited efforts have been made to address these issues. This article reviews existing literature to enhance our understanding of the managerial and operational challenges associated with the use and implementation of EHRs. In this study, we introduce an assessment checklist and management model specifically designed to address privacy, data security, and operational concerns within EHRs. This is a recommended approach for improving information security and privacy in electronic healthcare services.

Keywords: *Electronic health records, health information exchange, breaches, operational issues, interoperability, data privacy and security.*

1. Introduction

Electronic Health Record systems (EHRs) comprise medical records containing patient health information (PHI) generated by healthcare professionals, including medical doctors, nurses, and administrative health record staff. These records are managed by healthcare providers, maintained by health care systems administrators, and shared among physicians, patients, and health management offices both internally and externally [1].The integration of EHRs and the secure exchange of health information are essential for enhancing healthcare delivery [2]. An illustrative example is the OmaKanta electronic healthcare framework in Finland, which permits clinical experts or physicians to access a patient's computerized data, contingent upon the patient's permission or informed consent, to provide care or services during health crises and information requests [3,4]. Both clinicians

and non-clinicians may utilize this information to renew and manage authoritative capabilities and medical care services [5]. EHRs present new operational challenges for professionals that were not encountered during the era of paper-based clinical records. Traditionally, medical records were documented on paper, stored in folders, and kept in filing cabinets and drawers labelled as medical notes, with only a single copy produced during collection, pre-processing, and storage [6]. However, the widespread adoption of EHRs has been transformative for the healthcare industry, streamlining patient data management, accessibility, analysis, improving clinical decision-making, and enhancing the overall quality of healthcare delivery processes.

In this digital era, medical applications and devices are interconnected with cloud computing network services for healthcare information processing, exchange, diagnosis, and storage through the Internet of Medical Things (IoMT). IoMT is a network of connected medical devices that transfer data through the cloud [7,8]. Healthcare systems are supported by networks of these medical devices and centralized systems integrated through a network of servers and storage systems hosted locally to exchange health information and support healthcare delivery. These centralized systems are susceptible to single points of failure, data silos, unequal data standards, and inefficiencies in health information exchange [2].The transition from paper to electronic health records has rendered patient health information more accessible and effective, yet potentially vulnerable to cyberattacks [9].These deficiencies impact the interoperability of healthcare services, continuity of care, and medical errors, while also increasing the cost of healthcare delivery and compromising patient care safety. In the context of Industry 4.0 and the evolving Industry 5.0, healthcare systems will increasingly depend on electronic healthcare data-driven systems for decision-making; however, there is a pressing need for a robust, secure, and interoperable healthcare system. As a result, data security and privacy have become critical to advancing the security of sensitive health information and patient healthcare delivery and services.

One of the primary concerns in the healthcare sector is the escalating incidence of breaches involving patient health data [10,11], unauthorized disclosures, and the repurposing of such data beyond clinical contexts. These challenges not only raise significant operational and ethical concerns [12], but also actively undermine foundational principles such as informed consent, patient trust, and the assurance of privacy and confidentiality in healthcare systems [13,14]. In applications such as EHRs and healthcare information systems, the implementation of effective, efficient, reliable, and robust security measures is crucial. These measures are essential to protect healthcare ecosystems from cyberattacks, including system manipulation, denial of service, identity spoofing, and unauthorized access with privilege escalation, as well as to safeguard health information security and privacy. The rationale for this study is grounded in the European Union (EU) guidelines and scholarly literature, which call for prioritizing interoperability, data availability, cybersecurity, and

informatics infrastructure. This study employs a multi-factor approach to investigate and develop secure electronic health standards and data exchange in healthcare delivery, addressing regulatory issues through multiple methods and sociotechnical interactions in health information technologies to enhance the security and privacy of clinicians and patients in the design of healthcare technology, data sharing, and interoperability to meet international standards [15]. Consequently, these challenges have led to the proposal of a comprehensive framework [16]. There is a pressing need for further research on privacy and security regulations in healthcare [14], and innovative solutions are required to preserve privacy and protect patient data from unauthorized disclosure, access, breaches, and cyberattacks in electronic health record systems and cloud-based data exchange environments [5,17]. To address these challenges more effectively, this study conducted a review to explore and identify the causes of these information security challenges faced by healthcare systems and proposed solutions.

Research Question 1: What operational practices in health care data exchange contribute to the breach of security and privacy in EHRs?

Research Question 2: How can we ensure proper data security and privacy?

The objective of this study is to identify and address security and privacy concerns within electronic health record systems, considering them as critical assets for data at rest, in use, and during exchanges within the healthcare network.

Related literature

Health information protection requires a holistic approach to protect data at rest, in transit, and during exchanges to prevent breaches. EHRs facilitate exchange and must be designed with privacy and security features to prevent data breaches [18]. Habibzadeh et al., [19] Conducted a survey on cyber-physical systems in smart cities, focusing on cyberattack challenges to data privacy and security. This study proposed bifocal lenses to mitigate vulnerabilities in smart healthcare systems and identified Attribute-Based Encryption (ABE), blockchain, authentication, and authorization as solutions. However, it noted a limitation in the integration needed among policymakers, government entities, and citizens to secure the infrastructure. This limitation reflects a broader socio-technical challenge, where the lack of coordinated efforts, standardized policies, and mutual understanding among key stakeholders weakens the effectiveness of even the most advanced security technologies and hinders the creation of a truly robust and interoperable secure system. Without consistent regulatory frameworks, clear communication channels, and public trust, the deployment of these solutions may face resistance or inefficiency. Therefore, addressing this integration gap is essential to ensure that smart healthcare systems are not only technically secure but also socially and institutionally supported.

Xiang & Cai,[20] reviewed privacy protection and secondary use of health data, proposing a reduced risk of medical record re-identification through minimal data sharing using federated learning models. However, this approach limits interoperability where data exists in isolation. Anya et al., [21] highlighted issues of cross-boundary data-sharing that hinder clinical decision support, owing to privacy and security challenges, emphasizing cybersecurity design needs. The authors proposed an awareness model for cross-boundary clinical decision support, with their study advocating patient-centred frameworks to secure health information.

Costa Lima et al.,[5] proposed a security approach for electronic health (e-health) information using semantic web technology for secure data exchange. However, they acknowledged that semantic web technologies are still evolving and require improvement, indicating that security and privacy may not be guaranteed. This necessitates a combination of different solutions to achieve minimum reliability through new privacy solutions. Zhu et al.,[22] proposed a big-data-analytics-based cybersecurity framework that involves the application of multiple attributes, privacy through classification, and session-dependent encryption and decryption using machine learning and privacy decisions. This approach is related to the machine learning strategy for cloud-based medical record sharing proposed by [20], in which the exchange of information and security remains challenging owing to the presence of heterogeneous users and adversaries, as noted by [23].

Al-Issa et al.,[24] emphasized the need for cloud security in healthcare diagnosis. Their survey identified centralized cloud technology as a security vulnerability hindering adoption. They noted that the Confidentiality, Integrity, and Availability (CIA) approach lacks comprehensive protection and advocated advanced security mechanisms for e-health clouds. However, these studies mainly summarized existing literature, proposing partial solutions to the problem and emphasizing the need for a secure data exchange.

Thantilage et al.[17], Conducted a study on healthcare data security and privacy for data warehouse architectures and proposed a perspective focusing on data warehousing for secure storage in health environments, and acknowledged the need for more complex data security and privacy procedures. Also,[14] studies provide understanding on digitalisation of healthcare and revealed that electronic healthcare technology has brought about advancement in clinical support and monitoring diagnosis with precision. However, acknowledged a great concern on security and privacy while highlighting the need for privacy and security regulation for healthcare. In addition,[25] on the same topic proposed and analysed core constructs that contribute to the required transformative, adaptive, and absorptive capacities for health systems' digital transformation resilience and recommended a need for robustness in the understanding of operational knowledge of cybersecurity in healthcare digital resilience and sustainability. Gupta et al.[2]Analysis of security and privacy issues of information management of big data in B2B for data sharing, highlighted that data exchange via the Internet of Things (IoTs) is vulnerable to

cyberattacks. Numerous studies have explored issues related to privacy, information disclosure, and breaches in e-health technology, as well as the security of health information in the digital era [2,14,17,25,26]. However, there is a notable lack of research focusing on the privacy and security of patient data sharing and information exchanges within electronic healthcare records in interconnected healthcare networks and systems [2,9], as well as the integration of cybersecurity in operations and regulations [14,25]. In response to this gap, the present study aims to identify these operational concerns that have led to health information breaches in electronic health record systems and address information security and privacy within healthcare systems.

2. Materials and Methods

This study aimed to thoroughly review the literature on cybersecurity issues, with a particular focus on privacy and security breaches in e-health record systems. This study seeks to generate insights, propose solutions for healthcare organizations, and develop a checklist model to manage privacy, security levels, and compliance during health information exchange. This model is intended to enhance the security and facilitate interoperability in healthcare service operations. Although security and privacy have been widely discussed in various journals, this study specifically targets the healthcare sector. An integrative review approach was employed, as it reviews, critiques, and synthesizes representative literature on a topic in an integrated way to generate new frameworks and perspectives [27]. The integrative review method is systematically structured to reconceptualize the existing literature and provide research directions [28,29]. This study employed [30] PRISMA framework for article selection and screening (Figure 1), followed by integrated review steps.

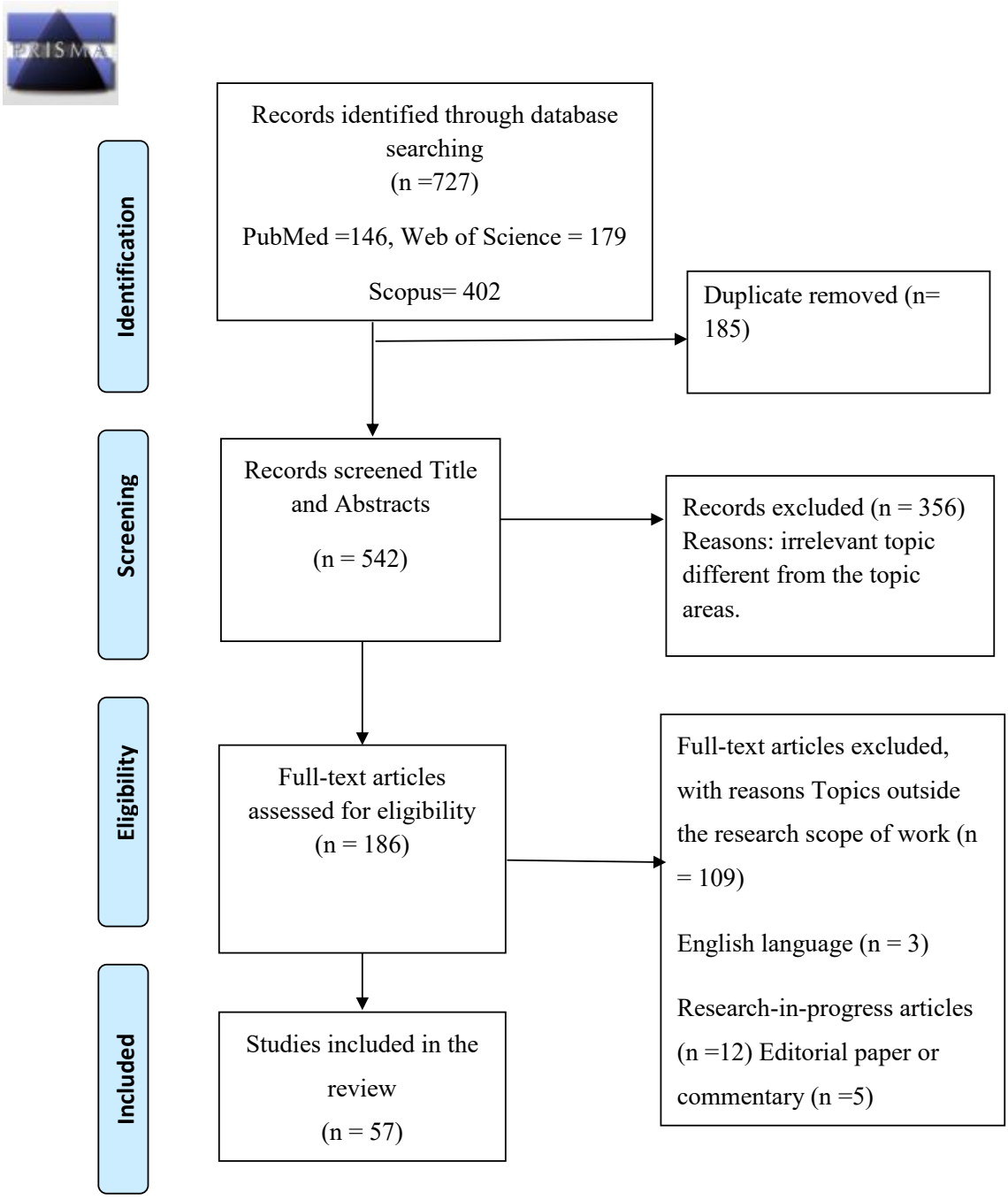


Figure 1 PRISMA Flow diagram of selection of articles

It is essential to comprehend the importance of health information and the consequences of its compromise or unauthorized access due to cybercriminal activities, as well as the

penalties imposed by regulatory authorities when such sensitive data is exposed in public cyberspace. This study seeks to identify the operational issues that have led to breaches of privacy and security of sensitive information within EHRs. The research began by identifying articles focused on cybersecurity, particularly concerning privacy and security in the healthcare sector, through searches of three databases: Scopus, Web of Science, and PubMed.

The search strategy was built around four major concept groups derived from the review objectives: EHRs, cybersecurity and data privacy, data exchange/interoperability, organizational, and operational practices. Search queries were customized to the syntax and indexing features of each database. For example, Medical Subject Headings (MeSH) search strategies were used to retrieve articles between 2012 – 2024 from PubMed, are as follows: ((“Electronic Health Records”[MeSH] OR EHR[Title/Abstract] OR “Electronic Medical Records”[Title/Abstract]) AND(“Cybersecurity”[Title/Abstract] OR “Data Security”[Title/Abstract] OR “Information Security”[Title/Abstract] OR “Data Privacy” [Title/Abstract] OR "Confidentiality[MeSH]) AND (“Data Sharing”[Title/Abstract] OR “Health Information Exchange”[MeSH] OR “Interoperability” [Title/Abstract]) AND (“Workflow”[MeSH] OR “Risk Management”[MeSH] OR Management [Title/Abstract] OR Process*[Title/Abstract] OR Administrat*[Title/Abstract])) . See multimedia appendix 1 for detail search strategy.

A total of 146 articles were retrieved from PubMed, the Web of Science (179), and Scopus (402), with a total of 727 articles. A total of 185 duplicate articles were removed, resulting in 542 screened articles. The protocols used for the inclusion and exclusion are listed in (Table 1).

Table 1. Inclusion and Exclusion Criteria

Inclusion criteria	Exclusion criteria
Peer review articles or research papers.	News, editorials, posters, commentary, and conference articles were excluded.
Studies should be written in the English language	Studies written in a language other than English.
Full-text article	Non-full-text article.
Studies related to cybersecurity and information security, privacy, and operations in healthcare domain	Irrelevant articles different from the topic areas and scope of work.
Studies between 2012- 2024	Articles outside the number of years specified.

The initial screening process assessed 542 articles based on their titles and abstracts, resulting in the exclusion of 356 articles that were deemed irrelevant to the study's focus or domain. Consequently, 186 articles were selected for a comprehensive full-text review. Of these, 129 were excluded because they fell outside the scope of the study, were not in English, or were research-in-progress papers, editorials, or commentaries. Ultimately, 57 studies were included in this review. An overview of the included studies is provided in Multimedia Appendix 2. In line with our objective of addressing privacy and security concerns in EHRs, this study adopted the categorization approach of Paul et al. (2023).

Additionally, the author utilized the Technology-Organization-Environment (TOE) framework of [31] to categorize the 57 articles selected for analysis. This framework was adapted to encompass three construct themes reflecting the processes, vulnerabilities, and interventions related to EHR cybersecurity and data exchange challenges. These themes were delineated as follows: technology, which includes infrastructure, security tools, and interoperability challenges; organization, which covers risk management, workflows, and internal policy gaps; and the environment, which addresses legal frameworks, regulatory standards, and the external threat landscape. This framework is recognized as a reliable method frequently employed in cybersecurity and technology-related research decisions [32,33]. The aim was to identify the security and privacy concerns that contribute to vulnerabilities, breaches, or disclosures within EHRs. Consequently, a model was developed as a solution for healthcare organizations.

The study themes were developed through qualitative content analysis using a hybrid approach and categorized according to the TOE framework. The article's data were systematically charted and analyzed based on their findings regarding the privacy and security operational challenges of EHRs, with justifications detailed in Tables 2 and 3.

3. Results

The result is presented to align with the research questions 1 in 4.1 and question 2 in 4.2, respectively.

The literature review outlined three main thematic constructs within the TOE model: technological operational dimension, organizational operational dimension, and environmental operational dimension, and categorized with operational practices contributing to data breaches, particularly in the context of EHRs. These operational practices include inadequate data security management, compliance with legal and regulatory standards, insecure health data sharing, insecure health data practices, privacy and confidentiality, and lack of proper informed patient consent.

Table 2 TOE-Based categorization of operational practices contributing to EHR security and privacy breaches

Healthcare Operational Practices	TOE Dimension	Justification	Reference
Inadequate data security management	Technological operational factors	Reflects flaws in technical safeguards such as encryption, access control, and infrastructure management	[2,13,19–21,25,34–39]
Compliance with legal and regulatory standards	Environmental operational factors	It involves external mandates like HIPAA, GDPR, or national data protection laws	[12,14,16,20,22,24,37,40–54]
Insecure health data sharing	Technological operational factors	This involves technical mechanisms of interoperability and secure data exchange	[2,9,13,20,21,26,34–36,41,43,46,52,55–62]
Privacy and confidentiality	Organization operational factors	This control is often shaped by internal policy, procedures, and staff practices for data handling	[5,12–14,19,21,22,24,42,44,50,54,56,61,63–69]
Lack of proper informed patient consent	Environmental operational factors	The focus is tied to ethical or legal expectations and national or international patient rights frameworks.	[21,24,25,38,39,49,60,64,70,71]

Inadequate data security management

Inadequate data security management, particularly in the encryption of patient records, can present significant operational challenges, resulting in security lapses and privacy breaches[19,36,72]. Electronic Health Record (EHRs) systems should be designed with secure access channels, support interoperability, and accommodate large-scale storage to meet accessibility and storage demands for data indexing, and secure exchange [20,35,73]. Given the increasing number of devices generating data without proper data security management, sensitive information could be transmitted inadvertently to unauthorised parties, managing data from an integrated perspective considering its volume, variety, and velocity. The concept of 3V framework can assist in addressing big data management challenges, particularly in smart healthcare environments where data is massive, diverse,

and rapidly generated[13,34,37,74] . Ensuring best practices in patient data protection and the quality of data harnessed, registered, processed, and stored in EHRs is crucial [39,75,76]. This approach will help overcome management and operational difficulties related to system limitations in data entry forms and quality from the perspective of systems users [25,77]. Understanding the relationship between data quality management and patient consent sharing is essential for collaborative data use, while obtaining patient consent during data exchange operations is mandatory [21]. Effective data quality management optimizes patient treatment throughout their healthcare journey [38], otherwise, these issues may lead to patients withholding sensitive data.

Inadequate data security management, including missing information, unauthorized access to patient information, and inappropriate health record management practices are major factors that contribute to managerial, operational challenges and uncertainties regarding health information privacy and security breaches [2,16,35,36]. Therefore, ensuring security, privacy, data integrity, management, and accuracy is crucial for maintaining trust in healthcare [22,38,55]. Training staff, transferring knowledge, and sensitizing patients can help in resolving operational challenges and ensure that the data quality remains consistent.

Compliance with legal and regulatory standards

Insufficient compliance with legal standards in healthcare information exchange poses a significant operational challenge, leading to breaches of EHRs [49]. Despite implementing the General Data Protection Regulation (GDPR) in the EU and establishing the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act in the United States to protect patient information, many healthcare organizations struggle to follow the guidelines for safeguarding health information and patient privacy [50,51,53]. Healthcare businesses must comply with regulations regarding patient privacy and security [54,78].
Some organizations develop compliance strategies for regulatory inspections only to revert to non-compliant practices by not implementing them in real-time [37]. Limited resources, lack of awareness, and inadequate organizational culture for managing cybersecurity leave many systems vulnerable to cyberattack [12,43,47]. Medium-sized and small organizations face challenges owing to limited resources, hindering their ability to protect sensitive healthcare information. It is essential to have a comprehensive cybersecurity framework to help organizations maintain regulatory compliance [45,51,53].
Although these laws and consequences of health information breaches have led many organizations to bankruptcy due to imposed fines [44], legal bodies and legislation require amendments to share breach burden between healthcare and technology developers and to reframe legislation to align with technological trends [14,20,24,48,79]. Continuous motivating policies that incentivize system developers and support healthcare providers in

sharing risks will foster creativity in addressing the security challenges related to patient health information [41]. Recognizing compliance is essential because non-compliance can undermine privacy and security for data-sharing systems with partners within electronic healthcare ecosystems [42,80]. Legal frameworks require healthcare organizations to safeguard internal data exchanges and manage external data sharing, an area in which many organizations are deficient [9,25,46]. Health institutions' inadequate compliance contributes to operational vulnerabilities. Organizations that fail to adhere to regulatory standards risk compromising patient privacy and critical information assets.

Insecure health data sharing

Insecure sharing or exchange of health data and inadequate protection within EHRs pose significant risks to patient security and privacy [9,13,46,55]. Developing methods for sharing EHR data in smart healthcare systems is essential for improving secure healthcare delivery in integrated care [35,56,64,81]. Data sharing within healthcare systems offers advantages in a precision-based service delivery and intensive care management [61]. Patients have the right to control their personal data dissemination [21]. Also, inadequate protection before exchanging sensitive health information could violate their right, privacy, and such failures can lead to financial losses, reputational damage, loss of trust, and physical harm [2,26,36,46,52,82].

Data security represents a significant challenge in healthcare systems, and health records sharing has gained attention in the health industry and research communities. Without patient or provider consent to sharing agreements, enhancing connected care becomes difficult [21,24,57,62]. Sensitive health information can be compromised by healthcare professionals, hackers, and cybercriminals in EHRs when healthcare does not have an effective and secure data sharing mechanism in place [20,22,41,58,59]. Patient data ownership and autonomy must be respected [60,83]. Trust and stigmatization remain key issues to address [43]. Security infrastructure and data encryption mechanisms for E-health records are necessary, while cloud-assisted health record sharing with cryptographic encryption will enhance security and protect information exchange in a connected healthcare [11,34,35,67]. Healthcare managers are also required to give the patients full control of their shared data and be informed of sharing instances.

Healthcare organizations can adopt data-sharing procedures that promote privacy, security, and regulatory compliance [21,22,59,84]. By doing so, organizations can enhance trust, privacy, and responsibility while leveraging shared data for societal good. This involves establishing responsible data sharing and protection strategies to address challenges associated with EHR systems.

Privacy and confidentiality.

Privacy and confidentiality are paramount in the context of EHRs because of the sensitive nature of personal health information [50]. A significant portion of managerial and operational challenges originates from the actions of personnel with authorized access to EHR systems, such as healthcare practitioners or dissatisfied employees within healthcare organizations. Numerous privacy breaches and security issues related to health information are attributed to insiders who either deliberately or inadvertently misuse patient data, such as accessing records without legitimate justification, or disseminating patient information without consent [21,44,54,64,85]. The intricate and multifaceted nature of the internet, combined with access to health data and the ongoing exchange of information through EHR systems and cloud-based big data processing, presents management risks concerning privacy and security [13,14,63,65,66]. In the absence of adequate security measures or encryption, the confidentiality of patient health data cannot be guaranteed over the internet, potentially resulting in the unauthorized use, access, and disclosure of sensitive information, thereby raising security concerns [5,42,61,68,86,87]. It is imperative to implement necessary precautions [88]. To address managerial and operational challenges, privacy can be embedded within the operational culture of healthcare organizations, ensuring confidentiality from technological, organizational, and patient perspectives [12,24,56,69], while respecting patient rights to privacy and confidentiality. This approach fostered trust and ensured effective communication [89]. Healthcare providers must uphold patient privacy while adhering to National Institute of Standards and Technology (NIST) and Open World wide Application Security Project (OWASP) frameworks for a secure electronic health information exchange [73]. Furthermore, the secure design and implementation of EHRs, including appropriate pseudonymization and encryption, are crucial for managing operational and managerial challenges in their use and implementation.

Lack of proper informed patient consent

Ensuring security requires understanding informed patient consent and endorsements. Ethical considerations regarding patient permission and involvement in EHRs impact patient autonomy, privacy, informed consent, and trust in healthcare [24,60,90]. When sharing health data, patients must be informed of implications for their health status and willingness to permit healthcare information or third parties to access their data for medical treatment and health-related purposes [21,39,87]. If health organizations use patient health data for commercial purposes without informing patients and addressing ethical concerns, this may lead to privacy violations, practices contrary to standards, and legal actions against healthcare organizations. The literature has also highlighted two consent models: general consent, with and without specific refusal. The general consent model provides patients

with the highest level of privacy protection [49]. Patients should have the option to opt in or out and be informed that their personal information will be shared [21]. Patients must be notified unless provider obligations are required.

According to the Health Records and Information Privacy Act 2002 (HIRPA), in New South Wales (NSW), Australia, health data must not be disclosed to anyone other than those who need it for essential purposes [64]. Healthcare organizations must not infringe upon patients' autonomy over their health information and must protect sensitive patient information to build trust and maintain reputation [71,91]. There is a need for patients, users, organizations, and technology providers to collaborate to establish secure, cooperative EHRs with workflow integration for clinicians and non-clinicians, and alert systems providing feedback to prevent challenges associated with EHR implementation of consent management systems and regulatory guidelines [24,25,70]. This approach will enable patients and staff to engage in the creative process and help organizations overcome operational challenges. As previously mentioned, consent should include both opt-in and opt-out options, ensuring that patients are thoroughly informed before any data sharing occurs. By effectively integrating patients into managerial and operational frameworks through training, workshops, and sensitization initiatives, healthcare management teams can maintain patient awareness and engagement, thereby ensuring patients are fully informed and privacy is maintained optimally [25,92].

Development of the check-list model

This study explored ways to ensure robust data security and privacy by developing a comprehensive privacy and security checklist model. This model, grounded in the operational risks identified in this review, was organized using the TOE framework. The checklist aims to serve as a practical tool for healthcare organizations, enabling them to safeguard EHRs across various operational domains within healthcare systems. The developed model reflects the study's focus on addressing security and privacy concerns for health information in use, at rest, and during exchanges within healthcare networks.

Table 3 Privacy and security checklist categorization using TOE Framework lenses

Privacy and security checklist assessment areas	**Areas of Policy implementation and action plans**	**TOE Classification domain**
Data Exchange	Encryption, Access Control	Technological

Healthcare Providers	Audits, Training	Organizational
Cloud	Data Residency, Compliance	Environmental/Technological
Data Sharing	Data Governance, Consent Management	Organizational/Environmental

Proposed Checklist Model

This study propose a holistic checklist model to protect patient health information (PHI), and exchange within the medical network. The model is next introduced.

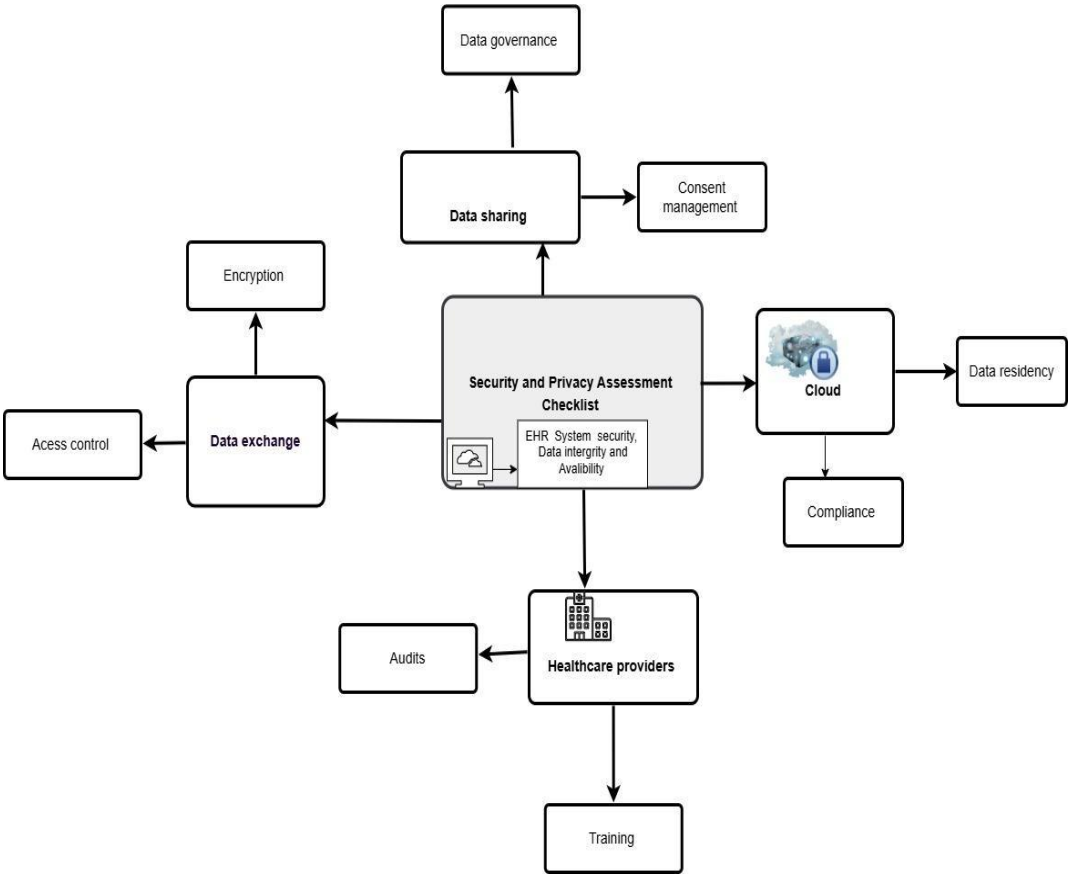


Figure 2. Security and Privacy Checklist model

The EHRs security and privacy Assessment checklist model is organized into four Parent themes, each of which is linked to a specific sub-theme as follows:
Data Exchange: The data exchange channel is crucial for sharing healthcare information, particularly in the current era of digitalization, where sensitive data are at risk of exposure [9,34]. The potential risks associated with data transmission can be mitigated through the implementation of encryption and access control measures, thereby preventing data breaches, exposure during operations, or cyberattacks [67]. Employing robust encryption standards, such as ISO/IEC 27001:2022, can ensure that data remains protected at every stage of data exchange.

Additionally, the use of role-based access control (RBAC) is critical for restricting data access to authorized users only, thereby enhancing sensitive data security both during transit and at rest [5,93]. In cloud-based environments, where EHRs are commonly stored, RBAC can be integrated with encryption key management systems to ensure that only users with predefined roles (e.g., physicians, nurses, administrative staff, and patients) can access or decrypt sensitive health data. Crucially, the patient role is uniquely defined for each individual, allowing patients full access to only their medical records while preventing access to others' data. This ensures that patient autonomy and privacy are preserved without compromising security. This role-specific access aligns with the principle of least privilege and supports the enforcement of patient consent preferences, allowing healthcare organizations to define which roles are permitted to access particular types of information. By embedding patient consent into access control policies, RBAC helps ensure that personal health data is accessed only when necessary and with appropriate authorization, thereby fostering transparency, upholding confidentiality, and building trust between patients and healthcare providers.

Data sharing: To facilitate the seamless exchange of health information, it is imperative to implement robust data-sharing policies. Often, the privacy of health information is compromised when the compliance standards of a receiving organization do not align with the security and privacy protocols of the originating entity [51]. This misalignment can render patient information vulnerable, particularly if the recipient's legacy systems serve as potential points for data exchange [58]. It is essential to uphold data-sharing policies and rights by establishing appropriate consent and permission. An effective data governance framework [9,37,47], coupled with a robust consent management mechanism, is crucial for ensuring accountability and transparency in the secure dissemination of healthcare data [49].

Healthcare Providers: Healthcare organizations or providers should prioritize the involvement of internal stakeholders, such as employees, in their security and privacy policies through audit assessments, and training, as this can effectively ensure the protection of health information and mitigate concerns about breaches or violations [94]. Regular internal security audits and ongoing staff training are instrumental in enhancing

the resilience of electronic health information protection and reducing the risk of both internal and external breaches [25,46,95] and cyberattacks through employee porousity and technical deficiency.

Cloud: Healthcare organizations managing health information storage must consider operational requirements, regional laws, and data residency standards. Compliance measures are essential not only to protect health information in the cloud during cyberattacks but also to meet legal and regulatory obligations. Insufficient compliance with regional policies can result in privacy violations, security breaches, and legal consequences. Regulatory frameworks vary by region—for example, the United States enforces HIPAA to safeguard patient data, while the European Union relies on GDPR to ensure strict data privacy and consent standards. Organizations operating across borders must account for these differences to maintain compliance and protect patient trust. Organizations with outdated systems, weak/poor backup infrastructure, and/or inadequate security protocols are especially vulnerable to data breaches and operational disruptions [45,69]. Organizations that are aware of legal jurisdiction over data storage are more empowered to ensure security and privacy accountability. Cloud storage policies can be tailored by incorporating data sovereignty and cross-border considerations when assessing different locations. Understanding regulations, selecting providers with strong regional compliance, and implementing governance policies can address residency, access, and security concerns regarding cloud-based health information sharing [40]. These processes enable organizations to maintain compliance and establish security controls, ensuring reliability without breaches or privacy violations.

4. Discussion

Summary of Key Findings

This systematic integrated literature review adopted the PRISMA method to screen and analyze a total of 57 articles and categorized themes using the TOE dimensions framework. The study addresses two research questions by identifying operational practices that contribute to cyberthreats and data breaches in EHRs and proposing strategies to ensure effective data security and privacy through a developed checklist model.

The result of the analysis revealed five thematic operational concerns contributing significantly to the breaches in healthcare data exchange. These themes were categorized under technological, organizational, and environmental factors derived from the TOE framework as follows:

- Inadequate data security management: numerous reflecting technological and organisational inadequacies, and indicates failures in implementation of robust security controls, such as weak authentication mechanisms, outdated security

protocols, insufficient encryption standards [5,69], and lack of an effective incident response plan.

- Compliance with legal and regulatory standards: The highest number of the articles revealed frequent lapses in adhering to the regulatory standards, such as the HIPAA, GDPR, further increasing vulnerability to breaches and compromising patient data. This highlights the primary organizational and environmental factors that contribute to the operational breach concern in healthcare systems. This shows that non-compliance standards are the most significant factors of healthcare organisation operational practices that contributes to the breaches[2].
- Insecure health data sharing: Technological and organizational limitations were observed as a key factor regarding insecure data transfer practices, which include: inadequate encryption during data sharing, use of unsecured exchange channels, and lack of clear access control mechanisms [83]. The study revealed lack of secure data exchange, whose shows the second largest operational practices of healthcare breaches and as collaborated to the finds in literature [9,41].
- Privacy and confidentiality: the study revealed that privacy violations concerns arise from inadequate organizational policies and improper technological safeguards as a great concern [5]. Also, the study revealed that many healthcare entities struggle to balance accessibility with privacy while frequently leaving sensitive patient information exposed [46]. Also, the study reveals that inadequate privacy and confidentiality is second most significant practices that contributed to the operational practices that led to health information breaches.
- Lack of proper informed patient consent: The study also found that some organizations neglect to communicate data handling processes clearly and most often fail to obtain explicit informed consent from patients when sharing patient data, undermining their autonomy and legal compliance. The result also revealed that informed consent as the least reported in the reviewed studies. However, this study observed that lack of proper informed consent is an internal or insider secrecy that maynot be shared or discussed or measured since alert or notifications is not designed in EHRs when patient data is shared unlawfully or lawfully to a third party even when the consent approval is signed during data pre-processing.

Furthermore, based on the analysis and result as highlighted that operational challenges that healthcare organization encounter with the use of electronic health record during operations and health information exchanged revealed that healthcare organization lacks proper data security and privacy practices in managing sensitive data due to complexity architectures [17], big data, and management. Our findings also revealed that health information breaches and disclosures occurred during data sharing and exchange between providers outside the hospital network [9]. Our findings also highlighted IoTs as a result

of digitalization that data sharing over the internet makes the privacy of health information vulnerable and prone to disclosure if proper security for data transport is not in place. Furthermore, the findings also underscore the need for a secure design approach. It can also be noted that most healthcare organizations are not compliant to data security regulations [14]. The author also observed that compliance is a big issue, because many organizations only comply when the regulatory authority is conducting audits. Healthcare organizations also require training in utilizing healthcare data and management [63].

Additionally, this study also highlights that patient confidence and willingness to share confidential and sensitive health information largely depend on the level of trust in the privacy and confidentiality of EHRs and data exchange models. When patients perceive that their data is handled with care, respect, and transparency, they are more likely to engage with digital health systems and disclose critical information essential for informed clinical decision-making, ultimately contributing to a more effective and responsive healthcare system. Conversely, any perceived lack of control or protection can undermine trust and hinder the effectiveness of data-driven healthcare delivery.

Contributions to literature

This review contributes to existing literature through categorising the operational practices impacting EHR security and privacy within the robust structure of the TOE framework. The study explicitly links each thematic issue to technological, organisational, and environmental contexts and also deepens understanding by offering clarity regarding the interconnected nature of security and privacy challenges.

This study developed a privacy and security checklist model for healthcare. The model consists of four themes and sub-themes: Data Exchange, data sharing, cloud, and healthcare providers, and discusses how the challenges of security and privacy can be addressed. The model contributes to the development of a secure healthcare in the form of a guide for management. In addition, this study contributes to the literature by educating and raising awareness from four perspectives linking technology developers, healthcare organizations, regulatory bodies, and patients, since the literature studies conducted in the field of managerial, operational, and ethical challenges linked to privacy and security are limited [15]. The model will aid in resolving operational and managerial challenges that may arise in the use and implementation of health records in healthcare delivery and services.

Recommendations for practice

The identified thematic concerns underscore the critical need for security and privacy of sensitive data and the EHRs technology and recommend for healthcare organizations to strengthen their security practices, improve regulatory compliance, improve patient consent procedures, and implement stringent privacy and data sharing protocols. This study also recommends regular cybersecurity audits, staff training on compliance [63], patient

consent, strong data encryption standards, and rigorous security management practices. Also, implementation of an Information security culture (ISC) plays a prominent role in the protection of healthcare data[12] . This study recommend that health care organisation should resolve interoperability concerns of EHRs and cross-border legislation and policy formulation and collaborate with insurance organisation to manage a risk in other to insure their critical assets in the case of cyberattacks and breaches.

The proposed operational guide assessment checklist model for privacy and security will help healthcare organizations, policymakers, and system developers to rethink operational challenges that may arise during use and when implementing EHRs. This conceptual model will enable healthcare organizations to have an assessment checklist and operational guidelines to ensure that all requirements regarding the privacy and security of EHRs systems in health care organizations are stringently met before adoption and implementation to manage health information in the EHRs. Furthermore, the proposed checklist model in (Figure 2) will help guide healthcare managers to ensure health information security, privacy, and confidentiality. In addition, when sharing health information, the checklist will ensure obtaining data owner consent, thus ensuring healthcare systems operate within ethical frameworks and that health information is exchanged securely.

Recommendations for future research

Managing security and privacy operational challenges of electronic health records systems require further research related to privacy, security and ethical guide in planning, development, and organization of new computerized break-throughs in therapeutic administrations [96]. This study recommends that further study should focus on empirical validation of the privacy and security checklist model in healthcare setting. In addition, research should also explore the effectiveness of emerging technologies in the areas of blockchain and artificial intelligence for the mitigation of identified operational risks.

Limitations

There are several limitations to this review. One is the limited number of databases searched, and grey literature was not examined. Also, this literature review focuses primarily on English-language articles, which may have inadvertently excluded valuable insights or articles from non-English.

5. Conclusion

This study presents an overview of the operational challenges surrounding the use and implementation of electronic health record (EHRs) systems in healthcare to curb issues regarding privacy and security, and discusses ways to resolve them. Operational practices

significantly influence the security and privacy of EHRs. In solving these identified operational concerns through proactive management, rigorous compliance with regulations, secure data sharing protocols, informed patient consent practices, and staff/employee trainings is essential to secure health information from breaches. The proposed privacy and security checklist model offer practical guidance to health care organizations aiming to mitigate risks and improve EHR security and privacy. This model also aims to bridge the gaps associated with health information breaches and exchange in medical network through the robust risk assessment measure. It serves as a comprehensive guide for ensuring data privacy and security in accordance with regulatory laws and policy standards for healthcare organizations.

Acknowledgments

The author will like to thank the Finnish Cultural foundation for supporting this research work

Funding

This study receives funding from Finnish Cultural foundation Grant No:

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability

Multimedia Appendix 1. Detailed search strategy
Multimedia Appendix 2. Overview of Included studies

References

1. Entzeridou E, Markopoulou E, Mollaki V. Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. *Int J Med Inform* 2018;**110**:98–107.

2. Gupta BB, Gaurav A, Kumar Panigrahi P. Analysis of security and privacy issues of information management of big data in B2B based healthcare systems. *J Bus Res* 2023;**162**, DOI: 10.1016/j.jbusres.2023.113859.

3. Coiera E, Clarke R. e-Consent: The Design and Implementation of Consumer Consent Mechanisms in an Electronic Environment. *Journal of the American Medical Informatics Association* 2004;**11**, DOI: 10.1197/jamia.M1480.

4. Jormanainen V. Large-scale implementation and adoption of the Finnish national Kanta services in 2010–2017: a prospective, longitudinal, indicator-based study. *Finnish Journal of eHealth and eWelfare* 2018;**10**:381–95.

5. Costa Lima V, Alves D, Andrade Bernardi F *et al.* Security approaches for electronic health data handling through the Semantic Web: A scoping review. *Semant Web* 2023;**14**, DOI: 10.3233/SW-223088.

6. Govindarajan UH, Singh DK, Gohel HA. Forecasting cyber security threats landscape and associated technical trends in telehealth using Bidirectional Encoder Representations from Transformers (BERT). *Comput Secur* 2023;**133**, DOI: 10.1016/j.cose.2023.103404.

7. Ahmed SF, Alam MS Bin, Afrin S *et al.* Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Information Fusion* 2024;**102**, DOI: 10.1016/j.inffus.2023.102060.

8. Wang L, Ali Y, Nazir S *et al.* ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods. *IEEE Access* 2020;**8**, DOI: 10.1109/ACCESS.2020.3017221.

9. Choi SJ, Chen M, Tan X. Assessing the impact of health information exchange on hospital data breach risk. *Int J Med Inform* 2023;**177**, DOI: 10.1016/j.ijmedinf.2023.105149.

10. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas* 2018;**113**, DOI: 10.1016/j.maturitas.2018.04.008.

11. Zack GJ. Strategies for Reducing Adverse Medical Events from Implanted Medical Devices. *ProQuest Dissertations and Theses* 2020.

12. Mikuletič S, Vrhovec S, Skela-Savič B *et al.* Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Comput Secur* 2024;**136**, DOI: 10.1016/j.cose.2023.103489.

13. Abouelmehdi K, Beni-Hssane A, Khaloufi H *et al.* Big data security and privacy in healthcare: A Review ScienceDirect Big data security and privacy in healthcare: A Review. *Procedia Comput Sci* 2017;**113**.

14. Paul M, Maglaras L, Ferrag MA *et al.* Digitization of healthcare sector: A study on privacy and security concerns. *ICT Express* 2023;**9**, DOI: 10.1016/j.icte.2023.02.007.

15. Kaplan B. REVISITING HEALTH INFORMATION TECHNOLOGY ETHICAL, LEGAL, and SOCIAL ISSUES and EVALUATION: TELEHEALTH/TELEMEDICINE and COVID-19. *Int J Med Inform* 2020;**143**:104239.

16. Casola V, Castiglione A, Choo KKR *et al.* Healthcare-Related Data in the Cloud: Challenges and Opportunities. *IEEE Cloud Computing* 2016;**3**, DOI: 10.1109/MCC.2016.139.

17. Thantilage RD, Le-Khac NA, Kechadi MT. Healthcare data security and privacy in Data Warehouse architectures. *Inform Med Unlocked* 2023;**39**, DOI: 10.1016/j.imu.2023.101270.

18. Supriya S, Padaki S. Data Security and Privacy Challenges in Adopting Solutions for IOT. *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, IThings-GreenCom-CPSCom-Smart Data 2016*. 2017.

19. Habibzadeh H, Nussbaum BH, Anjomshoa F *et al.* A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustain Cities Soc* 2019;**50**, DOI: 10.1016/j.scs.2019.101660.

20. Xiang D, Cai W. Privacy Protection and Secondary Use of Health Data: Strategies and Methods. *Biomed Res Int* 2021;**2021**, DOI: 10.1155/2021/6967166.

21. Anya O, Tawfik H, Alani MM *et al.* Cybersecurity design considerations for cross-boundary clinical decision support. *J Reliab Intell Environ* 2019;**5**, DOI: 10.1007/s40860-019-00076-z.

22. Zhu S, Saravanan V, Muthu BA. Achieving data security and privacy across healthcare applications using cyber security mechanisms. *Electronic Library* 2020;**38**, DOI: 10.1108/EL-07-2020-0219.

23. Alguliyev RM, Aliguliyev RM, Sukhostat L V. Efficient algorithm for big data clustering on single machine. *CAAI Trans Intell Technol* 2020;**5**, DOI: 10.1049/trit.2019.0048.

24. Al-Issa Y, Ottom MA, Tamrawi A. EHealth Cloud Security Challenges: A Survey. *J Healthc Eng* 2019;**2019**, DOI: 10.1155/2019/7516035.

25. Garcia-Perez A, Cegarra-Navarro JG, Sallos MP *et al.* Resilience in healthcare systems: Cyber security and digital transformation. *Technovation* 2023;**121**, DOI: 10.1016/j.technovation.2022.102583.

26. Chukwu E, Garg L. A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. *IEEE Access* 2020;**8**, DOI: 10.1109/ACCESS.2020.2969881.

27. Torraco RJ. Writing integrative literature reviews: Using the past and present to explore the future. *Human resource development review* 2016;**15**:404–28.

28. Hardy C, Maguire S, Power M *et al.* Organizing risk: Organization and management theory for the risk society. *Academy of management annals* 2020;**14**:1032–66.

29. Hopia H, Latvala E, Liimatainen L. Reviewing the methodology of an integrative review. *Scand J Caring Sci* 2016;**30**:662–9.

30. Moher D, Liberati A, Tetzlaff J *et al.* Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *J Clin Epidemiol* 2009;**62**:1006–12.

31. Depietro R, Wiarda E, Fleischer M. The context for change: Organization, technology and environment. *The processes of technological innovation* 1990;**199**:151–75.

32. Jia Q, Guo Y, Barnes SJ. Enterprise 2.0 post-adoption: Extending the information system continuance model based on the technology-Organization-environment framework. *Comput Human Behav* 2017;**67**:95–105.

33. Wallace S, Green KY, Johnson C *et al.* An extended TOE framework for cybersecurity-adoption decisions. *Communications of the Association for Information Systems* 2020;**47**:51.

34. Abouzakhar NS, Jones A, Angelopoulou O. Internet of things security: A review of risks and threats to healthcare sector. *2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2017, 373–8.

35. Esposito C, De Santis A, Tortora G *et al.* Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing* 2018;**5**, DOI: 10.1109/MCC.2018.011791712.

36. He Y, Zamani E, Yevseyeva I *et al.* Artificial intelligence–based ethical hacking for health information systems: simulation study. *J Med Internet Res* 2023;**25**:e41748.

37. Patil HK, Seshadri R. Big data security and privacy issues in healthcare. *Proceedings - 2014 IEEE International Congress on Big Data, BigData Congress 2014*. 2014.

38. Sahi MA, Abbas H, Saleem K *et al.* Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions. *IEEE Access* 2017;**6**, DOI: 10.1109/ACCESS.2017.2767561.

39. Sonkamble RG, Bongale AM, Phansalkar S *et al.* A secure interoperable method for electronic health records exchange on cross platform blockchain network. *MethodsX* 2024;**13**:103002.

40. Azeez NA, der Vyver C Van. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. *Egyptian Informatics Journal* 2019;**20**, DOI: 10.1016/j.eij.2018.12.001.

41. Cerchione R, Centobelli P, Riccio E *et al.* Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation* 2023;**120**:102480.

42. Chang J. Privacy and security concerns in online health services. *Appl Econ Lett* 2018;**25**:1351–4.

43. Kataria S, Ravindran V. Electronic Health Records: A Critical Appraisal of Strengths and Limitations. *Journal of the Royal College of Physicians of Edinburgh* 2020;**50**:262–8.

44. Kloss LL, Brodnik MS, Rinehart-Thompson LA. Access and disclosure of personal health information: a challenging privacy landscape in 2016-2018. *Yearb Med Inform* 2018;**27**:60–6.

45. Kruse CS, Smith B, Vanderlinden H *et al.* Security Techniques for the Electronic Health Records. *J Med Syst* 2017;**41**, DOI: 10.1007/s10916-017-0778-4.

46. Luna R, Rhine E, Myhra M *et al.* Cyber threats to health information systems: A systematic review. *Technology and Health Care* 2016;**24**, DOI: 10.3233/THC-151102.

47. Kruse CS, Frederick B, Jacobson T *et al.* Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care* 2017;**25**, DOI: 10.3233/THC-161263.

48. Lenert L, McSwain BY. Balancing health privacy, health information exchange, and research in the context of the COVID-19 pandemic. *Journal of the American Medical Informatics Association* 2020;**27**:963–6.

49. Munung NS, Staunton C, Mazibuko O *et al.* Data protection legislation in Africa and pathways for enhancing compliance in big data health research. *Health Res Policy Syst* 2024;**22**:145.

50. Puppala M, He T, Yu X *et al.* Data security and privacy management in healthcare applications and clinical data warehouse environment. *3rd IEEE EMBS International Conference on Biomedical and Health Informatics, BHI 2016*. 2016.

51. Shahid J, Ahmad R, Kiani AK *et al.* Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences (Switzerland)* 2022;**12**, DOI: 10.3390/app12041927.

52. Shi S, He D, Li L *et al.* Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Comput Secur* 2020;**97**:101966.

53. Shrivastava U, Song J, Han BT *et al.* Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation. *Int J Med Inform* 2021;**148**:104401.

54. Sivan R, Zukarnain ZA. Security and privacy in cloud-based e-health system. *Symmetry (Basel)* 2021;**13**:742.

55. Hathaliya JJ, Tanwar S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput Commun* 2020;**153**:311–35.

56. Holen-Rabbersvik E, Thygesen E, Eikebrokk TR *et al.* Barriers to exchanging healthcare information in inter-municipal healthcare services: a qualitative case study. *BMC Med Inform Decis Mak* 2018;**18**:1–14.

57. Hylock RH, Zeng X. A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study. *J Med Internet Res* 2019;**21**:e13592.

58. Jayabalan J, Jeyanthi N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *J Parallel Distrib Comput* 2022;**164**, DOI: 10.1016/j.jpdc.2022.03.009.

59. Kantarcioglu M, Ferrari E. Research Challenges at the Intersection of Big Data, Security and Privacy. *Front Big Data* 2019;**2**, DOI: 10.3389/fdata.2019.00001.

60. Khan S, Saravanan V, N GC *et al.* Privacy Protection of Healthcare Data over Social Networks Using Machine Learning Algorithms. Koundal D (ed.). *Comput Intell Neurosci* 2022;**2022**:9985933.

61. Koutzampasopoulou Xanthidou O, Xanthidis D, Manolas C *et al.* Security and privacy consideration for the deployment of electronic health records: a qualitative study covering Greece and Oman. *Information Security Journal: A Global Perspective* 2023;**32**:266–82.

62. Zaidan BB, Haiqi A, Zaidan AA *et al.* A security framework for nationwide health information exchange based on telehealth strategy. *J Med Syst* 2015;**39**:1–19.

63. Arain MA, Tarraf R, Ahmad A. Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *J Multidiscip Healthc* 2019:73–81.

64. Bertino E. Data security and privacy: Concepts, approaches, and research directions. *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAc)*. Vol 1. IEEE, 2016, 400–7.

65. Joshi N, Kadhiwala B. Big data security and privacy issues-A survey. *2017 Innovations in Power and Advanced Computing Technologies, i-PACT 2017*. Vol 2017-January. 2017.

66. Sharma P, Namasudra S, Gonzalez Crespo R *et al.* EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Inf Sci (N Y)* 2023;**629**, DOI: 10.1016/j.ins.2023.01.148.

67. Soni M, Barot Y, Gomathi S. A review on privacy-preserving data preprocessing. *Journal of Cybersecurity and Information Management* 2020:16.

68. Wu Z, Xuan S, Xie J *et al.* How to ensure the confidentiality of electronic medical records on the cloud: A technical perspective. *Comput Biol Med* 2022;**147**:105726.

69. Yaqoob I, Salah K, Jayaraman R *et al.* Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Comput Appl* 2022:1–16.

70. Svandova K, Smutny Z. Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review. *J Multidiscip Healthc* 2024;**17**:2281–301.

71. Zhang A, Bacchus A, Lin X. Consent-based access control for secure and privacy-preserving health information exchange. *Security and Communication Networks* 2016;**9**:3496–508.

72. Fernández-Alemán JL, Señor IC, Lozoya P ángel O *et al.* Security and privacy in electronic health records: A systematic literature review. *J Biomed Inform* 2013;**46**:541–62.

73. Spanakis EG, Sfakianakis S, Bonomi S *et al.* Emerging and Established Trends to Support Secure Health Information Exchange. *Front Digit Health* 2021;**3**, DOI: 10.3389/fdgth.2021.636082.

74. Lee I. Big data: Dimensions, evolution, impacts, and challenges. *Bus Horiz* 2017;**60**, DOI: 10.1016/j.bushor.2017.01.004.

75. Dias FM, Martens ML, Monken SF de P *et al.* Risk management focusing on the best practices of data security systems for healthcare. *International Journal of Innovation* 2021;**9**, DOI: 10.5585/iji.v9i1.18246.

76. Eichler HG, Bloechl-Daum B, Broich K *et al.* Data Rich, Information Poor: Can We Use Electronic Health Records to Create a Learning Healthcare System for Pharmaceuticals? *Clin Pharmacol Ther* 2019;**105**, DOI: 10.1002/cpt.1226.

77. Kim E, Rubinstein SM, Nead KT *et al.* The Evolving Use of Electronic Health Records (EHR) for Research. *Semin Radiat Oncol* 2019;**29**:354–61.

78. Health human services. *HIPAA Administrative Simplification* ., 2013.

79. Stoeger K, Schmidhuber M. The use of data from electronic health records in times of a pandemic—a legal and ethical assessment. *J Law Biosci* 2020;**7**:lsaa041.

80. Azarm-Daigle M, Kuziemsky C, Peyton L. A review of cross organizational healthcare data sharing. *Procedia Comput Sci* 2015;**63**:425–32.

81. Rai BK. PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. *Health Serv Outcomes Res Methodol* 2023;**23**, DOI: 10.1007/s10742-022-00279-7.

82. Tao H, Bhuiyan MZA, Rahman MA *et al.* Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems* 2019;**98**, DOI: 10.1016/j.future.2019.03.042.

83. Rezaeibagha F, Win KT, Susilo W. A systematic literature review on security and privacy of electronic health record systems: technical perspectives. *Health Information Management Journal* 2015;**44**:23–38.

84. Watson K, Payne DM. Ethical practice in sharing and mining medical data. *Journal of Information, Communication and Ethics in Society* 2021;**19**:1–19.

85. Chuma KG, Ngoepe M. Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective* 2022;**31**:179–95.

86. Jayabalan M, O'Daniel T. Access control and privilege management in electronic health record: a systematic literature review. *J Med Syst* 2016;**40**:261.

87. Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal* 2021;**22**, DOI: 10.1016/j.eij.2020.07.003.

88. Riordan F, Papoutsi C, Reed JE *et al.* Patient and public attitudes towards informed consent models and levels of awareness of Electronic Health Records in the UK. *Int J Med Inform* 2015;**84**, DOI: 10.1016/j.ijmedinf.2015.01.008.

89. Sulmasy LS, López AM, Horwitch CA. Ethical Implications of the Electronic Health Record: In the Service of the Patient. *J Gen Intern Med* 2017;**32**, DOI: 10.1007/s11606-017-4030-1.

90. Afzal S, Arshad A. Ethical issues among healthcare workers using electronic medical records: A systematic review. *Computer Methods and Programs in Biomedicine Update* 2021;**1**:100030.

91. Mathai N, Shiratudin MF, Sohel F. Electronic Health Record Management: Expectations, Issues, and Challenges. *J Health Med Inform* 2017;**08**, DOI: 10.4172/2157-7420.1000265.

92. Mazur LM, Mosaly PR, Moore C *et al.* Association of the Usability of Electronic Health Records With Cognitive Workload and Performance Levels Among Physicians. *JAMA Netw Open* 2019;**2**, DOI: 10.1001/jamanetworkopen.2019.1709.

93. Radanliev P, De Roure D. Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2). *Health Technol (Berl)* 2022;**12**:923–9.

94. Ben-Assuli O. Electronic health records, adoption, quality of care, legal and privacy issues and their implementation in emergency departments. *Health Policy (New York)* 2015;**119**, DOI: 10.1016/j.healthpol.2014.11.014.

95. Alshammari A. A novel security framework to mitigate and avoid unexpected security threats in saudi arabia. *Engineering, Technology & Applied Science Research* 2023;**13**:11445–50.

96. Christen M, Gordijn B,, Loi M. *The Ethics of Cybersecurity*. Springer Nature, 2020.

Appendix 1: Detailed search strategy for the databases

The concept for search is as follow:

- Search 1: EHR AND Cybersecurity
- Search 2: EHR AND Data Sharing/ Health Information Exchange
- Search 3: EHR AND Workflow/Risk Mgmt

PUBMED

("Electronic Health Records"[MeSH] OR EHR[Title/Abstract] OR "Electronic Medical Records"[Title/Abstract])

AND

("Cybersecurity"[Title/Abstract] OR "Data Security"[Title/Abstract] OR "Information Security"[Title/Abstract] OR "Data Privacy"[Title/Abstract] OR "Confidentiality"[MeSH])

AND

("Data Sharing"[Title/Abstract] OR "Health Information Exchange"[MeSH] OR "Interoperability"[Title/Abstract])

AND

("Workflow"[MeSH] OR "Risk Management"[MeSH] OR Management[Title/Abstract] OR Process*[Title/Abstract] OR Administrat*[Title/Abstract])

Scopus Search Strategy

TITLE-ABS-KEY ("electronic health record*" OR EHR OR "electronic medical record*") AND (

"cybersecurity" OR "data security" OR "information security" OR "data privacy" OR

"confidentiality") AND ("data sharing" OR "health information exchange" OR interoperability)

AND (workflow OR "risk management" OR management OR process* OR administrat* OR

organiz*)

Web of Science (WoS) Search Strategy

TS=(("electronic health record*" OR EHR OR "electronic medical record*") AND
("cybersecurity" OR "data security" OR "information security" OR "data privacy" OR
"confidentiality") AND ("data sharing" OR "health information exchange" OR interoperability)
AND (workflow OR "risk management" OR management OR process* OR administrat* OR
organiz*))

Appendix 2: Overview of the included studies (Data Charting)

Author(s)	Publication year	Title of article	Country	Study type / design	Main findings
Ray Hales Hylock, Xiaoming Zeng	2019	A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study	United States	Quantitative Experimental Study / Proof-of-Concept Evaluation involving performance testing of 16 system configurations across various cryptographic setups	HealthChain enables secure, patient-controlled health data exchange using smart contracts, FHIR, and blockchain. AES-based setups are fastest, while PRE-based ones are most secure. Demonstrates blockchain's strong potential for scalable, interoperable, privacy-preserving medical records.
Rahul Ganpatrao Sonkamble, Anupkumar M. Bongale, Shraddha Phansalkar, Deepak Sudhakar Dharrao	2024	A Secure Interoperable Method for Electronic Health Records Exchange on Cross Platform Blockchain Network	India	Quantitative Experimental Study / Prototype Implementation tested on hepatitis dataset to evaluate cross-chain interoperability between Ethereum and Hyperledger Fabric	Proposed a hash lock-based, secure, cross-platform EHR exchange method. Combined blockchain (on-chain) with IPFS (off-chain) and SPAKE protocol for session security. Validated successful secure exchange of patient data.
Clemens Scott Kruse, Benjamin Frederick, D. Kyle Monticone	2017	Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends	United States	Systematic Literature Review based on a structured search of 3 databases (CINAHL, PubMed, ProQuest)	The review found that healthcare lags significantly behind other industries in cybersecurity readiness. Key vulnerabilities include poor upgrade practices, lack of training, and insufficient breach response protocols.
Raul Luna, Emily Rhine, Matthew Myhra, Ross Sullivan, Clemens Scott Kruse	2016	Cyber Threats to Health Information Systems: A Systematic Review	United States	Systematic Literature Review conducted across four databases (CINAHL, Academic Search Complete, PubMed, and ScienceDirect),	Identity theft through data breaches is the most prevalent threat in healthcare cybersecurity. Other emerging concerns include internal/external threats, cyber-squatting, denial-of-service attacks, and cyberterrorism.

Clemens Scott Kruse, Brenna Smith, Hannah Vanderlinden, Alexandra Nealand	2017	Security Techniques for the Electronic Health Records	United States	Systematic Literature Review Analyzed 55 peer-reviewed articles from databases like CINAHL, PubMed, and Academic Search to evaluate techniques for securing EHRs	The study identified encryption, access control, audit logs, secure messaging, and blockchain as critical security techniques for protecting EHRs. It emphasized the gap between technical solutions and their actual implementation.
Zaidan, Haiqi	2015	A Security Framework for Nationwide Health Information Exchange Based on Telehealth Strategy	Malaysia	Mixed-Methods Conceptual & Evaluative Study Includes critique of nationwide HIE elements for evaluation of security techniques.	There is no fully defined global framework for securing nationwide HIE. The proposed framework integrates central cloud infrastructure with telehealth compatibility, addressing major HIE security vulnerabilities.
Trude Holen-Rabbersvik	2018	Barriers to Exchanging Healthcare Information in Inter-Municipal Healthcare Services: A Qualitative Case Study	Norway	Qualitative Case Study based on 18 participants using methods such as individual and focus group interviews, observation studies, and a workshop	Identified four key barriers to healthcare information exchange in inter-municipal services: (1) IT capability/usability, (2) differences between systems, (3) privacy/security issues, and (4) lack of awareness and shared understanding.
Zhang	2016	Consent-Based Access Control for Secure and Privacy-Preserving Health Information Exchange	China	Quantitative Cryptographic Framework Design & Performance Evaluation	The CBAC mechanism allows patients to explicitly authorize access, protecting data via conditional proxy re-encryption. The system ensures privacy, mutual authentication, contextual privacy, and collusion resistance.
Shrivastava	2021	Do Data Security Measures, Privacy Regulations, and Communication Standards Impact the Interoperability of Patient Health Information? A	Europe	Quasi-Experimental Quantitative Study in over 30 European countries.	Strong workstation access controls reduced technical interoperability (TI) issues by 44%. However, strict privacy rules at regional/organizational levels increased semantic (SI) and organizational (OI) issues by 85% and 76%, respectively. Hospitals with

		Cross-Country Investigation			single EMR systems had fewer interoperability issues.
Kataria	2020	Electronic Health Records: A Critical Appraisal of Strengths and Limitations	United Kingdom	Narrative review / critical Appraisal Synthesizes existing evidence and expert insights to evaluate the real-world effectiveness, limitations, of EHR systems	While EHRs improve transparency and access, they often cause clinician burnout, introduce administrative overload, and suffer from poor interoperability. Data breaches still occur despite security measures, affecting trust and safety.
Rezaeibagha, Win	2015	A Systematic Literature Review on Security and Privacy of Electronic Health Record Systems: Technical Perspectives	Australia	Systematic Literature Review, reviewed to assess the use of ISO/IEC 29100 and ISO/IEC 27002 security/privacy frameworks	Identified 13 essential features for secure and private EHR systems, including access control, cryptography, compliance, scalability, consent mechanisms, and interoperability. These are crucial for safeguarding patient data effectively.
Linda Kloss, Melinda Brodnik	2018	Access and Disclosure of Personal Health Information: A Challenging Privacy Landscape in 2016–2018	United States	Scoping Literature Review, focused on regulations, health data usage trends, and privacy management practices	Regulatory frameworks are evolving but lag behind the growing demand and complexity of health data access and use. Consent and authorization are increasingly inadequate, requiring broader stewardship-based privacy management.
Jayabalan, O'Daniel	2016	Access Control and Privilege Management in Electronic Health Record: A Systematic Literature Review	Malaysia	Systematic literature review, Reviewed articles using ISO 22600 as the evaluation framework.	Identified three main access control classes: EHR access, interoperability-based control, and risk-aware control. Context-aware models (temporal, spatial, semantic) and ontology-based rule engines offer more adaptable access control.
Lenert, McSwain	2020	Balancing Health Privacy, Health Information Exchange, and Research in the Context of the COVID-19 Pandemic	United States	Policy Commentary / Expert Perspective, Discusses regulatory conflicts and reforms in health information privacy	The pandemic highlighted urgent conflicts between outdated privacy laws and the need for fluid health information exchange across care and research systems. Disjointed systems

					(telehealth, testing.) suffer under current HIPAA constraints.
Munung Nchangwi Syntia, Staunton, Mazibuko, Wonkam	2024	Data Protection Legislation in Africa and Pathways for Enhancing Compliance in Big Data Health Research	Multi-country (Pan-African study; authors affiliated with institutions in South Africa and Cameroon)	Comparative Legal and Policy Analysis, Reviewed 37 national data protection laws across African countries to evaluate their impact on health data sharing	Significant variation exists in national laws governing health/genetic data sharing in Africa. Although common principles (consent, confidentiality, purpose limitation) are observed, legal inconsistencies hinder cross-border research collaboration.
Katerina Svandova, Zdenek Smutny	2024	Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review	Czech Republic	Scoping Review (PRISMA-ScR Guidelines) for risk assessment and management frameworks for IoMT security	Most frameworks focused on technical IoMT risk management; none covered organizational security measures. Need for comprehensive frameworks across all IoMT layers.
Ourania Koutzampasopoulou Xanthidou, Dimitrios Xanthidis, Christos Manolas, Han-I Wang	2021	Security and Privacy Consideration for the Deployment of Electronic Health Records: A Qualitative Study Covering Greece and Oman	Greece and Oman	Qualitative Study ,Conducted interviews with 40 healthcare professionals across Greece and Oman to examine EHR security, access, and IT preparedness	Professionals supported role-based access and logging of third-party access. Most were satisfied with current backup/recovery mechanisms and ICT training. Opinions were divided on full patient access to records.
Jieun Chang	2017	Privacy and Security Concerns in Online Health Services	South Korea	Quantitative Empirical Study , Investigated user behavior using statistical analysis to examine privacy/security concerns	Privacy and security concerns are negatively associated with the use of online health services. However, when strong privacy regulations are in place, this negative relationship is moderated, improving usage confidence.
Mubashir Aslam Arain, Rima Tarraf, Armghan Ahmad	2019	Assessing Staff Awareness and Effectiveness of Educational Training on IT Security and Privacy in a Large Healthcare Organization	Canada	Quantitative Survey Study , Online survey conducted with 586 healthcare professionals to assess awareness and training effectiveness on IT security/privacy	80.9% completed IT training; 57.5% found it effective. Training was linked to improved behavior (e.g., 4.2× more likely to act correctly on spam). Few staff knew how to encrypt emails; significant correlation found between training and satisfaction.

Sahi, et al	2017	Privacy Preservation in E-Healthcare Environments: State of the Art and Future Direction		Narrative Review / State-of-the-Art Review, Summarizes and evaluates existing privacy-preserving methods in electronic healthcare environments	Reviewed techniques like anonymization, encryption, and access control. Identified critical gaps in scalability, context-awareness, policy flexibility, and integration with real-time healthcare workflows.
Muneeb Ahmed Sahi, Haider Abbas, Kashif Saleem, Xiaodong Yang, Abdelouahid Derhab, Mehmet A. Orgun, Waseem Iqbal, Imran Rashid, Asif Yaseen	2017	Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions	Multi-national (Pakistan, Saudi Arabia, China, Australia, Macau)	Narrative Review / State-of-the-Art Review, published in IEEE Access, this review surveys privacy-preserving mechanisms. for e-healthcare	Identified the limitations of current privacy methods: lack of scalability, context-awareness, and unified standards. Emphasized the need for integrated, flexible, and patient-centric frameworks to ensure secure healthcare data handling.
Azeez Nureni Ayofe, Van der Vyver Glen	2019	Security and Privacy Issues in E-Health Cloud-Based Systems: A Comprehensive Content Analysis	South Africa (based on author affiliation with Nelson Mandela University)	Comprehensive Content Analysis / Literature Review, Synthesized academic literature and gray sources on cloud-based e-health security and privacy trends	Identified key concerns including unauthorized access, lack of data ownership clarity, vendor lock-in, and inadequate legal/regulatory compliance. The review highlighted cloud dependency, insider threats, and limited control mechanisms.
Ofir Ben-Assuli	2015	Electronic Health Records, Adoption, Quality of Care, Legal and Privacy Issues and Their Implementation in Emergency Departments	Israel	Narrative Review / Thematic Integration, Synthesized literature on EHR	While EHRs can improve care quality and coordination in emergency departments, adoption is hampered by privacy concerns, legal uncertainties, workflow disruptions, and inconsistent policy implementation.
Valeria Casola, Alessandra De Benedictis, Massimiliano	2016	Healthcare-Related Data in the Cloud: Challenges and Opportunities	Italy	Narrative Review / Technical Perspective – Analyzed challenges and enabling technologies for securely storing, managing, and	Cloud computing offers scalable solutions for healthcare data management but introduces significant risks in privacy, security, and legal compliance. Issues include data

Rak, Umberto Villano				sharing healthcare data in cloud environments	sovereignty, trust, interoperability, and standard enforcement.
Hamed Habibzadeh, Brian H. Nussbaum, Fatemeh Anjomshoa, Burak Kantarci, Timur Soyata	2019	A Survey on Cybersecurity, Data Privacy, and Policy Issues in Cyber-Physical System Deployments in Smart Cities	United States & Canada	Survey / Thematic Literature Review, Surveyed the cybersecurity and data privacy challenges in cyber-physical systems (CPS)	CPS in smart cities face severe risks due to data leakage, lack of real-time protection, and fragmented policy frameworks. Healthcare-related CPS like IoMT suffer from weak encryption and unclear privacy responsibilities.
Soni, M.; Barot, Y.; Gomathi, S.	2020	A Review on Privacy-Preserving Data Preprocessing	India	Literature Review / Technical Synthesis, reviewed modern access control, encryption, anonymization, and audit strategies for preserving patient data privacy in EHR systems	RBAC and ABAC are effective but limited in medical applications. Cloud-based anonymization is weak; improved techniques like k-anonymity, l-diversity, and t-closeness are needed to minimizemization is weak; improved techniques like k-anonymity, l-diversity, and t-closeness are needed to minimize re-identification risks.
Shahid, J. et al.	2022	Data Protection and Privacy of the Internet of Healthcare Things (IoHTs)	Pakistan	Review and Risk Analysis, investigated root causes of data leaks and challenges in securing Internet of Healthcare Things (IoHTs) systems	Key causes of data leakage in IoHT environments include legal conflicts across jurisdictions, low-quality devices, poor public and institutional awareness, and the absence of specialized local enforcement bodies.
Jayabalan, S.; Jayapriya, S.; Jeyanthi, N.	2022	Scalable Blockchain Model Using Off-Chain IPFS Storage for Healthcare Data Security and Privacy	India	Experimental Blockchain Architecture Study, Designed and tested a blockchain-based healthcare data model with IPFS for off-chain storage	The proposed model demonstrated improved big data retrieval performance compared to existing schemes. By combining blockchain with IPFS, the system achieves scalability and maintains privacy and security in healthcare data storage.
Esposito, C.; De Santis, A.;	2018	Blockchain: A Panacea for Healthcare Cloud-	Italy, Taiwan, Australia	Conceptual Review and Threat Analysis ,Explored security and	Healthcare data is highly valuable to cybercriminals and third parties. Data

Tortora, G.; Chang, H.; Choo, K. K. R.		Based Data Security and Privacy	(multi-national affiliations)	privacy risks in cloud-based healthcare systems	breaches may result from both reputationalacks and internal misuse (e.g., rogue employees or cloud vendors). Breaches can lead to liability and reputational damage.
Kantarcioglu, M.; Ferrari, E.	2019	Research Challenges at the Intersection of Big Data, Security and Privacy	United States and Italy	Thematic Review / Position Paper, Discussed emerging barriers and open challenges in balancing privacy, security	Privacy and competitive concerns hinder health data sharing and interoperability. Organizations may withhold data to avoid exposing vulnerabilities. Differential privacy, though promising, often requires too much noise for healthcare use, limiting its suitability.
Chukwu, E.; Garg, L.	2020	A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations	United States	Systematic Literature Review , Analyzed 61 blockchain-related healthcare articles focusing on privacy, security	Blockchain offers secure and privacy-preserving health information exchange, but at significant trade-offs in cost, scalability, and performance. Most literature focused on EHR/EMR/PHR sharing, identity management, and auditability. Implementation remains a challenge. Healthcare use cases include clinical trials, insurance, diabetes, oncology, and provider communication. Three architecture types dominate: One-CA, Multi-CA, and Client-Self-CA.
Zhu, S.; Saravanan, V.; Muthu, B.	2020	Achieving Data Security and Privacy Across Healthcare Applications Using Cybersecurity Mechanisms	China and India	Framework Proposal / Conceptual Review, Introduced a big data analytics-based cybersecurity framework	Proposed a cybersecurity framework for securing healthcare big data systems. Highlighted that while EHR sharing enhances service quality, it raises major privacy concerns. Existing solutions have limitations that hinder trust in EHR ecosystems.
Shi, S., He, D., Li, L., Kumar, N., Khan, M. K.,	2020	Applications of Blockchain in Ensuring the Security and Privacy	China, India, Australia, Saudi Arabia	Survey / Literature Review, Reviewed blockchain-based EHR systems and their roles in	Interoperability is crucial for quality care and is categorized into syntactic, semantic, and cross-domain levels.

& Choo, K. K. R. (2020).		of Electronic Health Record Systems: A Survey	(multi-national affiliations)	enhancing data security, privacy, and interoperability across healthcare providers	The lack of unified global standards like HL7, CEN, and DICOM limits high-performance data exchange across institutions.
Patil, H. K.; Seshadri, R.	2014	Big Data Security and Privacy Issues in Healthcare	United States	Conceptual Review / Position Paper , Explored challenges of integrating IoT and big data analytics in cloud-based healthcare environments	Successful IoT-based healthcare big data systems require scalability, interoperability, and decentralization (via blockchain). Existing privacy laws are insufficient for modern data analytics, creating a legal and ethical gap.
Abouelmehdi, K.; Beni-Hssane, A.; Khaloufi, H.; Saadi, M.	2017	Big Data Security and Privacy in Healthcare: A Review	Morocco	Review Paper / Comparative Analysis ,Assessed various cryptographic and access control mechanisms	Some proposed secure data sharing models lack key mechanisms like re-encryption, insider access control, and forward/backward secrecy, reducing trust in cryptographic servers and complicating model interpretation and reliability.
Wu, Z.; Xuan, S.; Xie, J.; Lin, C.; Lu, C.	2022	How to Ensure the Confidentiality of Electronic Medical Records on the Cloud: A Technical Perspective	China	Technical Design and Evaluation, Proposed and evaluated a cloud-based confidentiality preserving model for electronic medical records	The proposed solution ensures the confidentiality of EMRs even on untrusted cloud platforms, while maintaining the full functionality and availability of existing healthcare information management systems.
Al-Issa, Y.; Ottom, M. A.; Tamrawi, A.	2019	eHealth Cloud Security Challenges: A Survey	Jordan	Survey Review, Analyzed existing cloud security solutions applied to eHealth systems and evaluated their scope and limitations	Current security approaches only address isolated concerns such as access control, authentication, or data integrity. No comprehensive framework exists to manage all conflicting requirements in eHealth cloud environments.
Costa Lima, V.; Alves, D.; Andrade Bernardi, F.;	2023	Security Approaches for Electronic Health Data Handling Through the Semantic Web: A Scoping Review	Brazil & Portugal	Scoping Review, Investigated the state of security mechanisms, attributes, and gaps in handling health data over Semantic Web technologies	Semantic Web use in healthcare is growing, with various robust security mechanisms available. However, significant gaps remain in coverage and standardization. The right solution

Charters Lopes Rijo, R.P.					depends on the context of data usage and privacy requirements.
Sivan, R.; Zukarnain, Z. A.	2021	Security and Privacy in Cloud-Based E-Health System	Malaysia	Review / Conceptual Analysis ,Explores cloud-based healthcare data protection strategies, access controls, and risks.	Identified access control methods (RBAC, ABAC, MAC, IBAC) and emphasized the importance of policy-based and multi-factor authentication (2FA, OTP). Cloud risks include account hijacking, insider threats, misconfigurations, API vulnerabilities, and poor understanding of shared security responsibility.
Anya, O.; Tawfik, H.; Alani, M. M.; Hu, J.	2019	Cybersecurity Design Considerations for Cross-Boundary Clinical Decision Support	UK and China	Conceptual / Technical Perspective, discusses cybersecurity architecture design considerations for distributed clinical systems.	Emphasized the need for designing cross-boundary clinical decision support systems (CDSS) that are patient- and practice-centered, especially in IoT and remote collaboration contexts. Cybersecurity in such systems must account for privacy and security when sharing patient data.
Xiang, D.; Cai, W.	2021	Privacy Protection and Secondary Use of Health Data: Strategies and Methods	China	Review / Conceptual Analysis ,Evaluates international privacy regulations using federated learning and anonymization	Only a few regulations globally (e.g., GDPR, PIPEDA, CCC & PIPLRC) cover consumer health data (Category 2); most others protect only clinical data (Category 1). This regulatory gap hinders the secure secondary use of health data.
He, Y.; Zamani, E.; Yevseyeva, I.; Luo, C.	2023	Artificial Intelligence–Based Ethical Hacking for Health Information Systems: Simulation Study	United Kingdom	Simulation Study / Experimental Evaluation, compared optimized vs. unoptimized AI-based ethical hacking techniques in healthcare systems.	The optimized AI-based ethical hacking method achieved higher efficiency and effectiveness than unoptimized methods. Successful attacks included remote code execution, cross-site request forgery, improper authentication, and known vulnerabilities in systems like Oracle BI Publisher and Linux Virtual Server.

Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.	2022	Blockchain for healthcare data management: Opportunities, Challenges, and Future Recommendations	UAE	Narrative Review / Conceptual Analysis, Reviewed blockchain applications, technical enablers, and barriers in healthcare data management.	Blockchain presents significant opportunities for improving data integrity, access control, and traceability in healthcare. However, scalability, high latency, legal compliance, and lack of standardized protocols remain major challenges to mainstream adoption.
Vazirani, A. A.; O'Donoghue, O.; Brindley, D.; Meinert, E.	2019	Implementing Blockchains for Efficient Health Care: Systematic Review	United Kingdom	Systematic Review, Analyzed the use of blockchain for improving healthcare efficiency and security.	Blockchain has promising applications in healthcare for improving data integrity, reducing costs, and enhancing interoperability. However, risks such as 51% attacks exist if public blockchains are used without safeguards.
Dias, F. M.; Martens, M. L.; de Paula Monken, S. F.; da Silva, L. F.; Santibanez-Gonzalez, E. D. R.	2021	Risk Management Focusing on the Best Practices of Data Security Systems for Healthcare	Brazil	Qualitative Study, Focused on best practices in cybersecurity and risk management in healthcare .	Although no system can fully prevent all cyberattacks, integrating cybersecurity into healthcare management processes is crucial. Healthcare data is rich and valuable, yet cybersecurity remains neglected in Industry 4.0 settings.
Hathaliya, J. J.; Tanwar, S.	2020	An Exhaustive Survey on Security and Privacy Issues in Healthcare 4.0	India	Survey / Literature Review , Comprehensive analysis of security and privacy challenges using block chain	The study identified numerous limitations in current security schemes for Healthcare 4.0. Blockchain faces latency and scalability issues; ML models suffer from poor performance and data scarcity; Telehealth lacks regulations and is difficult to scale; policy-based schemes have high costs and low analytical flexibility; authentication schemes are vulnerable to impersonation and replay attacks; network-based systems struggle with real-world applicability and scalability.

Abouzakhar, N. S.; Jones, A.; Angelopoulou, O.	2017	Internet of Things Security: A Review of Risks and Threats to Healthcare Sector	UK	Literature Review, Synthesizes known IoT-related risks and attack vectors relevant to healthcare	The paper highlights that IoT devices introduce significant vulnerabilities in healthcare, including weak authentication, poor patching, data interception, and unauthorized access. The high interconnectivity and lack of standardized protocols exacerbate these risks.
Bertino, E.	2016	Data Security and Privacy: Concepts, Approaches, and Research Directions	United States	Conceptual Paper / Research Review ,The paper synthesizes data security and privacy.	The paper outlines key security and privacy challenges related to big data, IoT, and cloud computing, particularly in sectors like healthcare. It emphasizes the complexity of managing secure data sharing and access control in dynamic, distributed environments.
Supriya, S., & Padaki, S.	2016	Data Security and Privacy Challenges in Adopting Solutions for IoT	India	Review / Conceptual Analysis, Discusses emerging challenges on IoT-related data security and privacy concerns.	Highlights the massive data generation by IoT devices and the vulnerabilities that arise due to resource constraints, heterogeneous networks, and lack of unified standards. Emphasizes that existing security mechanisms are not directly applicable to the IoT environment.
Joshi, N., & Kadhiwala, B.	2017	Big Data Security and Privacy Issues—A Survey	India	Literature Review, Survey of big data lifecycle, with focus on privacy and security vulnerabilities across each stage	The authors outline a basic flow: collect → store → extract → derive knowledge. They emphasize that with each stage, unique security and privacy risks emerge.
Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E.	2023	Blockchain's Coming to Hospital to Digitalize Healthcare Services: Designing a Distributed Electronic Health Record Ecosystem	Italy	Conceptual Research / Design Science (Framework Development)	Despite EHR digitalization trends in advanced countries, many current systems still lack advanced privacy and security capabilities. A patient-centric, scalable solution is lacking.

Sharma, P., Namasudra, S., Crespo, R. G., Parra-Fuente, J., & Trivedi, M.C.	2023	EHDHE: Enhancing Security of Healthcare Documents in IoT-enabled Digital Healthcare Ecosystems using Blockchain	India	EHDHE: Enhancing Security of Healthcare Documents in IoT-enabled Digital Healthcare Ecosystems using Blockchain	Traditional healthcare data storage systems are outdated and untrustworthy in terms of data protection. EHDHE framework improves data security.
Gupta, B. B., Gaurav, A., & Panigrahi, P. K.	2023	Analysis of Security and Privacy Issues of Information Management of Big Data in B2B-Based Healthcare Systems	India	Analytical review of existing big data and B2B healthcare system security mechanisms	Highlights critical gaps in security and privacy in managing healthcare big data in B2B ecosystems; points out inefficiencies in current data handling.
Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B.	2024	Security and Privacy Oriented Information Security Culture (ISC): Explaining Unauthorized Access to Healthcare Data by Nursing Employees	Slovenia	Empirical study examining correlation between ISC and privacy breaches among nursing employees	Identifies an indirect relationship between information security culture (ISC) and unauthorized access to health data. Training boosts ethical and compliant behavior.
Alexeis Garcia-Perez, Juan Gabriel Cegarra-Navarro, Mark Paul Sallos, Eva Martinez-Caro, Anitha Chinnaswamy	2023	Resilience in healthcare systems: Cyber security and digital transformation	Multinational (UK, Spain, India)	Empirical + Theoretical Analysis of factors impacting cybersecurity resilience in digital healthcare transformation	Digital resilience in healthcare depends on: 1.Cybersecurity knowledge, 2.Uncertainty management, 3.Systemic and organizational interdependence. - Poor performance in these areas correlates with lower success in secure digital transformation.
Choi, S. J., Chen, M., & Tan, X.	2023	Assessing the impact of health information exchange on hospital data breach risk	USA	Empirical study using longitudinal data (2010–2017) to assess data breach trends and HIE engagement	HIE participation increased from 18% in 2010 to 68% in 2017 •Data breaches also rose sharply, especially: •Hacking incidents (0 → 13) •Unauthorized access/disclosure (1 → 26) •Higher breach risk was found in hospitals exchanging data with external providers.

					•No increased risk when HIE was limited to internal providers. •Small hospitals and clinics are more vulnerable due to weaker data governance and cybersecurity infrastructure.
Paul, M., Maglaras, L., Ferrag, M. A., & Almomani, I.	2023	Digitization of healthcare sector: A study on privacy and security concerns	UK, Saudi Arabia,UAE& Jordan	Review and analysis of existing literature and emerging threats in healthcare digitization	Digitization has improved service delivery but increased attack surfaces for cyber threats •Key challenges include unauthorized access, data leakage, malware attacks, and ransomware •There is a lack of standard security frameworks across digitized healthcare systems •Mobile health apps, IoT, and telemedicine introduce complex privacy issues •Insider threats and third-party services remain critical risks

Sociotechnical Cybersecurity Response Framework for Managing Cyber Incidents in Health Care

Pius Ewoh[1] School of Technology and Innovation, University of Vaasa, Vaasa, Finland

Tero Vartiainen[2] PhD, School of Technology and Innovations, Information Systems Science, University of Vaasa, Vaasa, Finland

Tero Haukilehto[3] South Ostrobothnia Welfare Services Region, Seinäjoki, Finland

Corresponding Author:
Pius Ewoh
Email: pius.ewoh@uwasa.fi
Phone: +358414888477
Postal Address: School of Technology and Innovations, University of Vaasa, Wolffintie 32, Vaasa, 65200, Finland

Abstract

Background: The frequency and sophistication of cyberattacks targeting healthcare organizations have escalated. Finnish health care providers are not immune to the increasing challenges of maintaining continuity of care and safeguarding sensitive patient data.

Objective: This study examined the management of cyberattack incidents within Finnish healthcare organizations by analyzing the sociotechnical factors that influence effective incident response and management.

Methods: Data were collected through an open-ended questionnaire administered to information technology professionals, managers, and healthcare staff across Finnish healthcare organizations. Qualitative content analysis was used to identify key challenges.

Results: The challenges that hinder effective incident response and management include: Inadequate awareness training, delays in incident alert detection, inadequate communication, ambiguous cybersecurity policies, and updates. Based on these challenges, a sociotechnical cybersecurity response framework is proposed to enhance the effectiveness of incident response.

Conclusions: This study offers insights into the sociotechnical dynamics of healthcare cybersecurity and provides practical guidance for ongoing improvement and resilience in Finnish healthcare organizations. It recommends implementing a cybersecurity awareness campaign, training programs, procurement of automated incident detection and alert systems, effective communication and team coordination, clear cybersecurity policies and procedures, advanced technology infrastructure, regular audits, and collaboration with the risk-pooling sector through insurance coverage as strategies to manage cybersecurity incidents.

Keywords: cyber incident, response strategy, healthcare, cybersecurity, preparedness

Introduction

Globally, healthcare organizations have increasingly become targets for cybercriminals and state-sponsored actors because of their substantial reliance on digital technology to enhance healthcare service delivery and the high value of patient health information in the dark market [1]. The implementation of electronic health record technology has improved the continuity and safety of care through cross-data sharing and by providing information via the Internet of Medical Devices (IMD) and applications. The adoption of these technologies by healthcare providers to enhance healthcare delivery services is progressively expanding the digital landscape, rendering healthcare organizations vulnerable to cyberattacks because of the use of complex endpoint devices, interconnected medical devices, and infrastructure [2,3].

Reported instances of WannaCry ransomware cyberattacks within the National Health Service (NHS) in the United Kingdom have significantly disrupted healthcare services [4,5]. The frequency of these attacks continues to escalate. A known attack vector involves ransomware, malicious software masquerading as legitimate software within a healthcare network, which causes damage and encrypts hospital- and patient-sensitive information for ransom payment. This software encrypts sensitive health information and operational environments, thereby restricting access to health care services until a ransom is paid [6]. In certain instances, even after a ransom is paid, healthcare organizations may not regain access. The compromised information may be released to the public network, resulting in data loss, identity theft, reputational damage, and financial penalties. Consequently, healthcare providers are required to integrate proactive cybersecurity measures into their systems to enhance their resilience against potential cyberattacks.

Finnish healthcare organizations are not immune to such cyberattacks, which can have significant repercussions, including compromise of sensitive health information, disruption of critical healthcare infrastructure and services, and threats to patient safety [7]. Despite the implementation of technical cybersecurity controls to address these issues, these methods remain inadequate [8]. Therefore, an effective incident response is imperative to mitigate the occurrence or impact of cyber breaches or disruptions and ensure the continuity of secure healthcare service delivery. A sociotechnical perspective on cybersecurity incident response is essential. Overreliance on network-connected smart healthcare systems increases vulnerability [2,3]. According to a study by [9], the integration of digital X-ray technology in radiology departments can create vulnerabilities during diagnostic processes, and the data stored in the Picture Archiving and Communication System (PACS) of X-rays can be hacked or exploited by cybercriminals.

The 2020 cyberattacks and data breach on Vastaamo Oy highlighted significant vulnerabilities in the cybersecurity preparedness of healthcare organizations, underscoring the necessity for Finnish healthcare entities to implement comprehensive cybersecurity measures [10]. A sociotechnical perspective on cybersecurity incident responses is crucial. Despite advancements in digitalization and technological investments within healthcare systems, sociotechnical factors, such as cybersecurity culture, training, technological applications, and policy clarity, remain insufficiently explored in shaping effective incident responses [11,12]. This study seeks to address this gap by bridging the sociotechnical issues that connect technology, human factors, and organizational policy processes, thereby formulating a robust cybersecurity incident management strategy to safeguard and continuously enhance the operational environment and resilience of Finnish healthcare organizations against cyberattacks and breaches of sensitive health information. While research has been conducted on cyber incidents, cyber preparedness, incident reporting, cybersecurity, and management, there is a paucity of studies focusing on cybersecurity incident response strategies [6,12,13]. Ultimately, awareness, reporting, and policies related to cyber incidents require further improvement. This study is motivated by the demand and appeal of civil society and scholars to inform cybersecurity incident management and enhance the preparedness of Finnish healthcare organizations [14].

Research Questions

How can we manage cyberattack incidents in healthcare organisations?

Objective: This study examines the management of cyberattack incidents within Finnish healthcare organizations by analyzing the sociotechnical factors that influence effective incident response and management.

Literature review

Cyber Incident management or preparedness against any form of attack in Finnish healthcare organisations has been a topic on the front burner, necessitating the need for a comprehensive response model [15]. One cannot forget the Vastaamo psychotherapy data breach in Finland, attributed to a lack of management oversight, data privacy governance, perimeter defense, multi-factor authentication, and regulatory compliance standards [10]. Cybersecurity hygiene must be taken seriously. The study conducted by [16] on cybersecurity competence among healthcare nurses revealed significant sharing of passwords and usernames, which underscores the need for cybersecurity hygiene. Furthermore, the authors recommended cybersecurity awareness training for nurses and called for further cybersecurity clinical education, as the current competence is deficient. In addition, [17] revealed that awareness is essential in responding to emergencies, as their study provides understanding on situational awareness and highlighted a lack of cooperation due to interoperability and preparedness in responding to incidents, and alluded to the call of [16] on situational awareness and revealed a shortage of manpower

and lack of collaborations[18]. The study conducted by Simola & Lehto further addresses incident crisis management for situational awareness through organisational, technical, and structural alternatives for crisis management. However, the study further calls for a comprehensive or dynamic cyber response model for incident situations[19]. The study by Gomes et al.[20] reveals that future digital hospitals will be vulnerable to cybersecurity threats due to their dependence on digital device networks for a better hospital cybersecurity business model and calls for incident preparedness to sustain the cybersecurity of hospitals by proposing (Internet of Things – mobile devices management (IOT- MDM) systems from a management perspective. However, studies are limited from the technical perspective. Rajamäki and Pirinen [21] propose a trust and secure design towards resilient cyber-physical systems (CPS) of healthcare. Their study acknowledges that the cyber resilience of CPS in healthcare is an interconnected social, technical network that creates large complexities and risk assessment in the Finnish information society, which alludes to the instance of Sillanpääet al.[22] on technical failure of such systems dependence on technological systems and solutions, and that the flipped side effect is comprehensive security, as threats are no longer separable between internal and external security due to its multifaceted nature. There is a need for a sociotechnical approach in tackling incident response in the Finished healthcare sector [14]. Furthermore the study conducted by [23] highlighted on the issue of healthcare digitalization as healthcare consist of ICT systems intertwine with medical devices and clinical systems and proposed solutions by noting that vulnerabilities exist in people, processes and technology and called for comprehensive cybersecurity in healthcare systems which this study allude to by examine incident response using the sociotechnical lens as this limitations show that there where limited study on empirically incident response framework developed specifically for Finnish healthcare using a sociotechnical as a comprehensive lenses [10,14,23], in responding to cyberattack incident management in Finnish Health care organizations.

Method

Study Design

This study employed a qualitative exploratory design to examine how healthcare professionals experience and manage cybersecurity incidents in Finnish healthcare organizations. Given the limited research on cybersecurity incident management (CIM) within healthcare settings [12]. This approach allows for an in-depth exploration of practical experiences, challenges, and organizational responses to cyber incidents. A 13-question open-ended questionnaire was designed and deployed through an online platform targeting only health care professionals and IT cybersecurity experts within healthcare organizations in Finland.

Participants and Recruitment

The study recruited 12 participants involved in cybersecurity, IT, or health information management roles within healthcare organizations. The Participants were selected using purposive sampling and recruited through Prolific, a secure, online research platform. Recruitment was restricted to individuals' healthcare professionals, security experts, and healthcare business founders located or working in Finland, to ensure contextual relevance to the national healthcare cybersecurity environment. Eligibility criteria included current or recent involvement in cybersecurity or incident response functions within healthcare settings.

Data Collection

Data were collected using an open-ended, self-administered questionnaire distributed electronically through Webropol, an online survey tool, in May and June 2025, and the Questionnaire instrument can be found in Multimedia Appendix 1. The questions were designed to elicit rich narrative responses focused on participants' direct experiences with incident management without collecting any personally identifiable information. The Participant characteristics are listed in Table 1.

Table 1. Participant data characteristics

Code	Job Title	Year Experience	Work Sector	Location
P1	CISO	8	Health care	Finland
P2	Systems Developer	5	Health care	Finland
P3	Software Engineer	4	Health care	Finland
P4	Integration Developer	3	Health care	Finland
P5	Practical nurse	1.7	Health care	Finland
P6	Owner	1	Health care	Finland
P7	Industrial Control Systems Security Technician	6	Health care	Finland
P8	IT Support Specialist	1	Health care	Finland
P9	Project manager	2	Health care	Finland
P10	Social Services IT Coordinator	3	Health care	Finland

P11	IT Technical Support	3	Health care	Finland
P12	Developer	2	Health care	Finland

Ethical Considerations

The questionnaire does not collect identifiable personal information, organizational names, or clinical data, participation is voluntary and anonymous, and formal ethical approval may not be required. However, the participants were informed of the purpose of the study, data handling procedures, and their right to withdraw at any time. This study followed ethical research practices in accordance with the institutional guidelines.

Data Analysis

Participants' responses were electronically exported into spreadsheet and was analyzed using qualitative content analysis [24]. An inductive approach was used over statistical inferences to identify recurring themes and patterns that emerged from the text content. Data coding was conducted manually using sticky notes and inputted in word documents, with responses reviewed line-by-line and grouped into categories based on semantic similarity where the concepts and themes emerged. This allows us to continuously refine our understanding of whether the empirical findings supported by theory and inductive coding enabled the categories and themes to emerge naturally from the empirical data, thereby enabling the representation of respondent experiences and perspectives. This approach allows for the development of an evidence-based understanding of incident response practices, enabling the identification of both the strengths and gaps in current cybersecurity management within healthcare environments.

Results

Of the 12 participants who began answering the open-ended questionnaires, 12 completed the questionnaire. The themes that emerged from the coded content analysis are as follows: Inadequate awareness training, incident alert detection delay, inadequate communication, and ambiguous cybersecurity policy and updates**.** The data extracted from the participants for each theme quoted are presented in the results themes below.

Inadequate Awareness training

Awareness training is essential for healthcare organizations that aim to engage employees in mitigating cyberattacks and breaches of sensitive health information. A significant proportion of participants reported that inadequate cybersecurity awareness training among healthcare staff impedes effective cybersecurity incident response. The operational practices within healthcare organizations, such as the identification of phishing attempts,

are not well understood. Awareness training is crucial for healthcare professionals to minimize human-related errors. An example of the quote extract related to the awareness training reported by the participant is shown below:
("Our IT team spotted the suspicious login attempt quickly, blocked the account and sent out a warning. It gave us an opportunity to improve staff awareness and practices")- (P6, P7, P8, P12)

("Enhancing Staff Training – Provide regular cybersecurity and phishing awareness training.")- (P2,P4,P5, P10, P11)
Some respondents emphasized the importance of training in managing cyber incidents, noting that when training sessions are generic and lack detail, they fail to incorporate updated tools and software used in smart healthcare. Consequently, there is a demand for automated tools to address evolving cyber threats such as malware and phishing attacks. This deficiency increases the risks of phishing and other social engineering attacks. Effective training of healthcare staff can benefit from a sociotechnical approach in designing a healthcare awareness training program. The application of sociotechnical techniques can significantly enhance the awareness levels of healthcare staff, thereby facilitating the detection of anomalies and effective responses to cybersecurity incidents.

Incident Alert detection delay

Alert detection and response systems are essential cybersecurity tools designed to identify anomalies within medical networks, thereby notifying IT security managers and healthcare organizations to address cyber threats and attacks. A significant challenge is the delay in detecting cyber incidents, as evidenced by past successful cyber-attacks. Participants reported that intrusion detection systems were either absent or improperly configured, leading to substantial cyber threats and attacks. However, in some instances, the respondents reported their ability to respond promptly. The reported extract of a successful cyberattacks is reported as follows: "*A year prior to our recent success, we faced an incident involving credential stuffing that targeted our patient portal. Unfortunately, the SOC was overloaded with false positives from unrelated phishing attempts, which delayed proper alert triage. By the time we confirmed the nature of the attack, hundreds of accounts were already compromised. Though no sensitive data was breached, the delay in detection and response allowed attackers to exploit basic patient account functions".- (P2,P6,P8,P9,P12).*

("The incident like personal identification and contacts details were compromised this was due to delay detection and also inadequate security measure".)- P3, P7, P11,

It was also observed that delays in multifactor authentication often result in breaches of sensitive information. Detection gaps contribute to prolonged system compromise and data exposure, and some respondents acknowledged the insufficiency of cybersecurity and IT professionals during non-working hours and reliance on manual or outdated threat detection tools as factors contributing to a successful breach that previously occurred. Delays in detection allow attackers to inflict greater damage on healthcare organizations' critical infrastructure systems, resulting in denial-of-service attacks or successful breaches of patient-sensitive information.

Inadequate Communication

Inadequate communication and coordination in incident reporting and responses among various healthcare departments and stakeholders can significantly hinder effective responses. Participants reported a communication breakdown among the IT department, security operations center (SOC), and clinical department during shift changes, which resulted in successful cyberattacks and breaches of sensitive healthcare information. The data transcript information is reported as follows: (*"During response, inadequate training and poor communication can exacerbate issues")- (P1, P3, P4 P5,P6,P9, P11, P12,)*

(Communication Gaps: Lack of a predefined communication strategy led to confusion among staff and delayed notifications to patients and partners.)- (P2, P7,P8,).

Additionally, some participants highlighted the complexity of systems and the design of incident response management, noting that inter-organizational communication during incidents was described as fragmented. The data further indicates unclear chains of command and reporting delays. This identified communication breakdown constitutes a major barrier to timely responses in health-IT systems. Participants emphasized the necessity for a centralized incident command center with a clear communication plan and pre-established roles for stakeholders and actors in managing pre- and post-incident responses within the healthcare system.

Ambiguous cybersecurity policy and updates

Cybersecurity policy is a vital component of healthcare organizations, influencing their operational culture and forming an essential part of their resilient framework, thereby ensuring the delivery of effective and secure health services. Participants reported challenges in adhering to policies, noting that outdated cybersecurity policies create confusion and impede incident-response efforts. They emphasized that policies must be clear, comprehensive, and regularly updated to address cybersecurity challenges and emerging threats. The report of the respondent's data is extracted and presented below.

("Healthcare organization could make policies clearer and easier to follow. Regular training and practical drills would help staff stay prepared and reduce mistakes during incidents.") – (P2, P4, P5, P7, P8, P9,)

("By updating the IT policies regularly".)- (P2, P3, P6, P8, P11, P12)
Deviations or uncertainties regarding protocols during an incident can lead to inconsistent responses, compromising protection levels, and rendering organizations vulnerable to cyberattacks and breaches. Regular policy reviews, policy development, and employee engagement are crucial to effective policy dissemination. The participants underscored the necessity of a localized version of the policy that aligns with and responds to the specific

contexts and operational modes of individual healthcare departments and units within the healthcare service delivery framework.

Proposed Sociotechnical Cybersecurity Response Framework

Our analysis highlights the necessity of a cybersecurity incident response strategy, informed by the issues identified through empirical data collected from participants. We propose a sociotechnical cybersecurity incident response framework designed to address each identified challenge by offering the corresponding pre- and post-incident solution mechanisms, as illustrated in Figure 1.

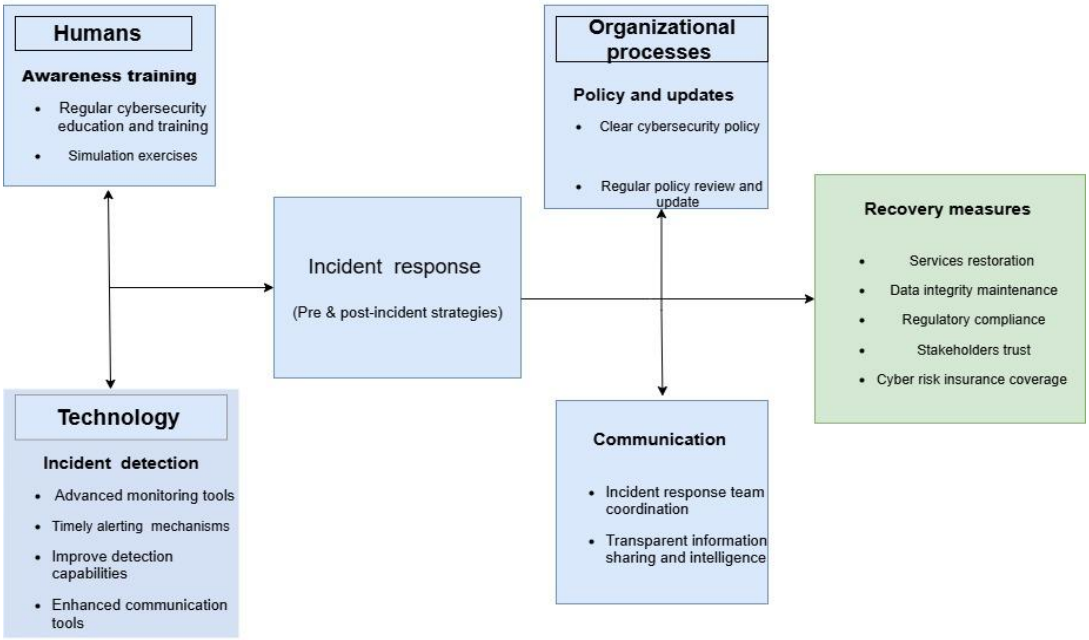


Figure 1. Conceptual sociotechnical cybersecurity incident response framework

Humans

Human employees and patients are frequently targeted in cyber-attacks or breaches, and are often considered the weakest link in such events [25,26]. A key objective of the reform agenda of the Finnish Institute for Health and Welfare is to enhance security because the cybersecurity of healthcare is intrinsically linked to patient safety [27]. Although healthcare management cannot forgo investment in awareness training, the financial demands of cybersecurity investment can be substantial, posing challenges for smaller

organizations in maintaining cybersecurity maturity capabilities. Nevertheless, cybersecurity awareness can be fostered through informal methods, such as word-of-mouth or experiential learning, whereby employees cultivate an awareness mindset among their colleagues. This strategy can enhance organizational cybersecurity awareness with minimal financial investment [28]. [29] also highlighted that social engineering attacks, such as phishing, present significant psychological challenges by exploiting weaknesses in human cognitive functions, thereby taking advantage of employees' lack of awareness. Education and training on human factors remain insufficient for the identification and detection of various types of cyberattacks. Regular cybersecurity education and training are essential for healthcare organizations to respond effectively and proactively to cybersecurity incidents [30,31].

Ineffective training can jeopardize employees; thus, simulation-based blended training has been proposed as an effective approach to managing cybersecurity incidents [32]. Periodic cybersecurity assessments are crucial for understanding necessary skill sets and training requirements.

Technology

Consequently, effective incident detection and response mechanisms are imperative. These findings indicate that delays in incident detection are a critical factor contributing to the success of cyberattacks. Investment in automated detection tools can enable organizations to monitor and identify anomalies within networks of supervised and unsupervised medical devices [4]. Healthcare organizations can benefit from the implementation of advanced monitoring and intrusion detection systems, ensuring real-time alerts through continuous collaboration between automated systems and incident-monitoring teams. The utilization of endpoint detection and response tools can enhance rapid detection capabilities.

Organizations should adopt proactive strategies to enhance their detection systems by designing them with the capability to dynamically identify both known and unknown threats during cyber incidents. Furthermore, it is essential to enhance advanced communication tools by establishing secure communication channels to prevent information leaks.

Organizational Processes

The organizational process environment can be conceptualized as an integrated framework that shapes both technological and social contexts through targeted policies designed to enhance cybersecurity incident management. This framework aims to bolster resilience to cyberattacks and improve incident management outcomes, thereby fostering stakeholder trust. To advance the cybersecurity defences of healthcare organizations, policies and updates must be maintained at an optimal level [8].

A well-defined cybersecurity policy can eliminate ambiguity because employees are prone to resorting to shortcuts when policies are difficult to adhere to. For instance, a device policy that permits healthcare professionals to access information via mobile devices can facilitate a more rapid incident response even when they are not on-site [33]. Consequently, policies that enhance the protection of healthcare mobile devices and laptops should be encouraged, along with comprehensive security measures to ensure a swift incident response in the event of cyberattacks. Healthcare organizations cannot afford to neglect the importance of timely updates. Interconnected medical devices and applications necessitate continuous updates, including policy revisions, as technological advancements have evolved rapidly, particularly with the advent of the Internet of Medical Things (IoT) network. Medical devices currently offer hardware as a service (HAAS), and the evolving nature of software applications is now providing services known as software as a service (SaaS). When policies are not updated, they become obsolete, thereby increasing their vulnerability to cyberattacks. Regular policy review is essential because it allows for the incorporation of new incident patterns, anticipates the advanced persistent threat strategies of cybercriminals, and facilitates the development of more effective incident management plans.

Communication

Effective communication is an indispensable strategy in incident response, which cannot be undermined by technological, human, or organizational factors. The success of incident response management is contingent upon seamless communication, as emphasized by the framework, which underscores the necessity of a clearly defined plan and a well-coordinated incident response team, as established by healthcare managers [10,11,34]. This team should comprise well-trained experts, including IT security professionals, clinical operation specialists, data protection officers, compliance officers, and executive management leaders. It is imperative that clear roles and responsibilities be documented and explicitly delineated within the incident response protocol plan[18]. Regular training exercises and drills are essential to enhance preparedness.

Transparent information sharing and intelligence exchange among departments, Security Operations Centers (SOC), organizations, and external stakeholders such as government entities and other healthcare organizations facilitate the dissemination of intelligence, thereby improving cybersecurity incident management and fostering effective communication for rapid and resilient responses to cyber incidents[17]. Establishing clear and secure channels for information sharing and providing timely updates ensures that stakeholders remain informed and vigilant, thereby reducing confusion or misinformation. Transparency fosters trust both internally and externally with regulators, partners, and patients, thereby enhancing information sharing and promoting interoperable healthcare systems[35]. This approach also enables other organizations to learn from incident

responses and management practices. The acquisition of advanced communication tools, configured securely and aligned with the team's daily operations, is crucial. The sociotechnical incident response framework not only ensures an effective incident response but also bolsters the organization's overall cyber resilience.

Recovery measures

The implementation of recovery measures is a critical component of post-incident management, particularly when addressing sociotechnical incident challenges. These measures establish criteria for success and offer guidance for business continuity, ongoing improvement, and the extraction of valuable lessons. The outcomes function as a mechanism for obtaining feedback that evaluates the effectiveness of the incident response and informs future preparedness [6].

Services restoration: In the event of cyber threats or anomalies within healthcare systems, it is imperative to promptly restore services, including IT and clinical services, as part of the post-incident phase. This process should be outlined in pre-protocol planning documents, which serve as guides for action plans. This aspect of the framework encompasses technical redundancies, such as backups of healthcare-sensitive data and failover mechanisms, to facilitate the rapid recovery of healthcare organizations [36]. A manual operational workflow will be implemented to ensure the continuity of services. Hybrid preparedness must be established and employed if the incident management process reaches these stages.

Data integrity maintenance: The protection of sensitive patient health information is imperative to maintain confidentiality, availability, and accessibility, thereby affirming conventional cybersecurity strategies within healthcare systems. The proposed framework advocates the enhancement of access control mechanisms and audit trails to prevent falsification or compromise of health information [10]. Furthermore, the incident response strategy must incorporate measures to verify the authenticity and accuracy of data following an incident.

Regular compliance: Compliance is a critical component of incident management within the framework of health care operations. An effective action plan should be integrated into the healthcare incident management strategy to ensure adherence to the Finnish National Acts 2019 concerning the secondary use of health and social data, as well as EU-level regulations, such as the General Data Protection Regulation (GDPR). This framework underscores the importance of embedding compliance in healthcare incident management to guarantee that stakeholders are informed, data protection measures are upheld, and regulatory requirements are met during crisis management. Furthermore, it is imperative that both pre- and post-incident procedures are incorporated into the plan [14]. Each phase of the incident management process must align with established legal and regulatory action

plans. Incident management charters also include actions such as timely breach notifications, comprehensive documentation, and transparency as integral components of operational plans for healthcare organizations.

Stakeholder trust: Stakeholder trust is integral to incident management as demonstrated in this framework. When incidents are not managed transparently, organizations risk losing public trust, which can lead to legal and regulatory challenges. An effective incident response is crucial for safeguarding the credibility of healthcare organizations and reinforcing public and patient trust in healthcare service providers. Transparency in post-incident reporting, timely communication with patients and partners, and evidence of compassionate proactive measures enhance stakeholders' trust and confidence. It is evident that transparent procedures and communication are essential in cultivating an organizational cybersecurity culture and strengthening stakeholder trust in cybersecurity incident management.

Cyber risk insurance coverage: In an era characterized by the vulnerability of digital records to Internet exposure, cybersecurity insurance has become essential for both patients and healthcare professionals, particularly for those dealing with victims of psychological trauma. Healthcare organizations require professional indemnity insurance to safeguard both patients and workers. This includes the protection of sensitive and digital assets, thereby enhancing security and facilitating post-incident management [37]. Consequently, this approach bolsters cybersecurity maturity and capabilities while also reinforcing compliance with general data protection regulations and Finnish data protection acts to ensure the protection of sensitive data

Discussion

Summary of Key Findings

A qualitative content analysis study conducted on Finnish healthcare organizations, involving cybersecurity professionals and other medical staff from various institutions, identified four critical sociotechnical barriers that may impede an efficient and effective cybersecurity incident response: awareness training, delays in incident alert detection, inadequate communication, and ambiguous cybersecurity policies and updates (Gordon et al., 2019). These challenges represent complex healthcare issues that are deeply rooted in sociotechnical misalignments, rather than purely technical deficiencies [8].

Awareness Training

This study identified that factors such as employee workload, vigilance, and stress significantly contribute to human error, which can lead to cyberattacks. This finding was

corroborated by several respondents' responses and data analysis, consistent with previous research conducted by [38,39]. Furthermore, the study highlighted that cybersecurity awareness training, if not adapted to a blended or hybrid format, may prove ineffective in equipping employees to respond to and manage cyber incidents efficiently. Additionally, the research underscored a pervasive lack of cybersecurity awareness among clinical and administrative staff, which is a critical factor affecting incident response and management in the healthcare sector. Cybersecurity awareness and training programs must be regularly developed and implemented for all staff, with a focus on phishing, malware, password security, and data protection [35,40,41].

Incident alert detection delay

This study identified that false positives and misconfigurations in intrusion detection tools frequently result in breaches of patient data or cyberattacks. This underscores the challenges posed by the complex IT infrastructure, which impedes rapid incident detection [42,43]. The integration of user-friendly incident response systems into healthcare workflows is therefore imperative. Our findings indicate that delays in alerts are attributable to technological gaps and staff miscommunications. This revealed that sophisticated intrusion-detection bypass algorithms were employed to compromise the intelligence systems. Furthermore, the study revealed that legacy technology is a significant factor contributing to breaches and successful cyberattacks.

Communication

The present study identified inadequate communication as a significant impediment to effective incident response management. Our findings indicate that a lack of clear communication during employee shift transitions, coupled with ambiguities in roles and responsibilities, contributes to delays in incident responses and increases vulnerability to cyberattacks. Furthermore, the absence of a standardized communication protocol has been identified as a critical bottleneck leading to an ineffective incident response [44]. Therefore, it is imperative to design improved procedures for handling alerts and managing shift changes. Establishing a clear communication channel and a coordinated mechanism across all departments and stakeholders is essential for enhancing incident response [11].

Ambiguous cybersecurity policy and updates

The present study identified a correlation between successful cyberattacks in healthcare organizations and the presence of unclear and non-standardized policies. These policies tended to be predominantly technocentric. Staff participants reported difficulties in understanding how to implement or adhere to these policies. Furthermore, the study highlights that ambiguity in cybersecurity policies stems from insufficient staff

involvement in the policydevelopment process, which in turn leads to inadequate engagement with the policies and confusion in their implementation and utilization. This lack of clarity impairs an organization's capacity to respond decisively under pressure. It is recommended that incident management policies undergo regular reviews to ensure that outdated policies are updated [45,46]. Policy clarity is crucial for effective and efficient engagement in enhancing cybersecurity incident management.

Theoretical Contributions

This study advances the field of sociotechnical systems theory by offering empirical evidence, identifying key challenges in incidents, and providing a comprehensive understanding of sociotechnical optimization and integration among human factors, technology, and organizational policy processes to enhance cybersecurity incident response and management within the context of healthcare cybersecurity [8,47]**.** Additionally, this study identifies and categorizes the barriers that may affect effective incident management in Finnish healthcare organizations and proposes a sociotechnical cybersecurity incident response framework. The study emphasizes key findings that highlight the necessity of a comprehensive approach, advocating that cybersecurity should not be perceived solely as a technical solution but should also be considered through the lens of human factors and within a framework of organizational processes and policies in shaping healthcare cybersecurity incident response management [48,49]**.**

Practical Implications

Healthcare managers should prioritize the integration of sociotechnical components within cybersecurity incident-response strategies. Investment in staff training, communication tools, and the acquisition of advanced automated technologies such as endpoint detection response (EDR) is essential to significantly enhance organizational resilience and ensure a swift response to incidents[50]. Employees must have clearly defined roles in incident response and management. Managers and development stakeholders in health care should establish explicit guidelines and responsibilities for employees, thereby eliminating ambiguous training methods, policies, and guidelines that may lead to confusion. The proposed framework serves as a diagnostic tool or blueprint for managing and enhancing incident response capabilities, protecting patient data, and ensuring business continuity within Finnish healthcare organizations.

Recommendations for Future Research

The study recommends that future research highlight the potential for further investigation into the role of AI and automation in accelerating sociotechnical incident detection in healthcare. Further studies can expand the sample sizes to cover larger healthcare organizations within Finland. Since the method used for this research is a qualitative method, future research can focus on the use of both qualitative and quantitative methods (mixed methods). It is essential to conduct further research to assess the effectiveness of

the proposed sociotechnical incident response framework within Finnish healthcare organizations. Additional studies are also needed to explore the cultural and organizational factors that influence cybersecurity behaviour in healthcare [6].

Limitations

The present study has several limitations. The sample size was relatively small, which may affect the generalizability of our findings to all Finnish healthcare organizations. Although the use of open-ended questionnaires yielded detailed insights, it restricted the potential for Physical interactions. Furthermore, the study faced challenges in data collection from mapped healthcare organizations owing to bureaucratic obstacles.

Conclusion

Cybersecurity incidents or breaches pose a substantial threat to Finnish healthcare organizations, with potential repercussions including data breaches and disruptions in patient care. This study underscores the socio-technical challenges that may affect effective incident response and management. Despite Finnish healthcare organizations exhibiting a high level of cybersecurity maturity and capability to address cybersecurity incidents, there remains a need for ongoing enhancements. Inadequately managed cybersecurity incidents can result in breaches of health information. Addressing the sociotechnical factors inherent in technology, human elements, and organizational policy processes will contribute to the enhancement of incident management in Finnish healthcare organizations. This study emphasizes that a purely technical approach to incident resolution is insufficient to shield healthcare organizations from cyberattacks. Moreover, human factors, organizational policies, and communication strategies are pivotal to advancing incident response outcomes. Insufficient awareness training, delays in anomaly detection and response, communication breakdowns, and unclear policies and updates are recognized as impediments to effective incident response management in healthcare organizations. To address this incident management issue, this study proposes a conceptual sociotechnical cybersecurity incident-response framework. This framework incorporates potential solutions such as cybersecurity awareness campaigns, training programs, the expansion of personalized indemnity insurance for healthcare patients and staff, automated incident detection and alert systems, effective communication and team coordination mechanisms, clear cybersecurity policies and procedures, advanced robust technology infrastructure, and regular audits as strategies to address cybersecurity incidents in healthcare organizations. The implementation of the proposed sociotechnical cybersecurity incident response framework will provide Finnish healthcare organizations with opportunities to enhance their resilience against cyberattacks, safeguard patient data, ensure the provision of safe healthcare services, and improve preparedness for a proactive response to cyber incidents.

Disclosure

The author(s) declared no conflicts of interest

Funding

The author is grateful to the Finnish Cultural Foundation [Grant No:10251726], and Suomen Vakuutusyhdistyksen for their support in funding this research

Multimedia Appendix 1

Questionnaire Sample

Note

Author's contributions: PE was responsible for the study design, screening, data extraction, synthesis of results, manuscript writing, and preparation.TV contributed by providing input and advice on protocols, data extraction, writing, and manuscript shaping. TH contributed to providing inputs for preparing the questionnaire instruments, data collection protocols, and dissemination channels for the questionnaire.

References

[1] Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care 2017;25. https://doi.org/10.3233/THC-161263.

[2] Tully J, Selzer J, Phillips JP, O'Connor P, Dameff C. Healthcare Challenges in the Era of Cybersecurity. Health Secur 2020;18. https://doi.org/10.1089/hs.2019.0123.

[3] Dameff CJ, Selzer JA, Fisher J, Killeen JP, Tully JL. Clinical Cybersecurity Training Through Novel High-Fidelity Simulations. Journal of Emergency Medicine 2019;56. https://doi.org/10.1016/j.jemermed.2018.10.029.

[4] Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas 2018;113. https://doi.org/10.1016/j.maturitas.2018.04.008.

[5] Coventry L, Branley-Bell D, Sillence E, Magalini S, Mari P, Magkanaraki A, et al. Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 12210 LNCS, 2020. https://doi.org/10.1007/978-3-030-50309-3_8.

[6] Sullivan N, Tully J, Dameff C, Opara C, Snead M, Selzer J. A National Survey of Hospital Cyber Attack Emergency Operation Preparedness. Disaster Med Public Health Prep 2023;17. https://doi.org/10.1017/dmp.2022.283.

[7] Bakheet A. Cybersecurity in Healthcare: New Threat to Patient Safety. Cureus 2025;17.

[8] Malatji M, Von Solms S, Marnewick A. Socio-technical systems cybersecurity framework. Information and Computer Security 2019;27. https://doi.org/10.1108/ICS-03-2018-0031.

[9] Giansanti D. Cybersecurity and the digital-health: The challenge of this millennium. Healthcare (Switzerland) 2021;9. https://doi.org/10.3390/healthcare9010062.

[10] Looi JCL, Allison S, Bastiampillai T, Maguire PA, Kisely S, Reutens S, et al. Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers. Australasian Psychiatry 2025;33:106–10. https://doi.org/10.1177/10398562241291340.

[11] He Y, Maglaras L, Aliyu A, Luo C. Healthcare Security Incident Response Strategy-A Proactive Incident Response (IR) Procedure. Security and Communication Networks 2022;2022:2775249.

[12] Jalali MS, Russell B, Razak S, Gordon WJ. EARS to cyber incidents in health care. Journal of the American Medical Informatics Association 2019;26. https://doi.org/10.1093/jamia/ocy148.

[13] Lohrke FT, Frownfelter-Lohrke C. Cybersecurity research from a management perspective: A systematic literature review and future research agenda. Journal of General Management 2023. https://doi.org/10.1177/03063070231200512.

[14] Haukilehto T. Cybersecurity management in healthcare: Policies, awareness and incident reporting 2024.

[15] Paananen R, Soikkeli M, Aro M, Kuusisto T, Rusila T, Tuulensuu T. Finland's Cyber Security Strategy 2024–2035 2024.

[16] Blek T, Solankallio-Vahteri T. Terveydenhuollon hoitohenkilöstön tieto-ja kyberturvallisuusosaaminen 2022.

[17] Simola J, Rajamäki J. Common Cyber Situational Awareness: An Important Part of Modern Public Protection and Disaster Relief 2016.

[18] Lehto M, Limnéll J. Strategic leadership in cyber security, case Finland. Information Security Journal: A Global Perspective 2021;30:139–48.

[19] Simola J, Lehto M. Effects of cyber domain in crisis management. Proceedings of the European conference on information warfare and security, Academic Conferences International; 2019.

[20] Gomes JF, Iivari M, Ahokangas P, Isotalo L, Niemelä R. Cybersecurity Business Models for IoT-Mobile Device Management Services in Futures Digital Hospitals. Journal of ICT Standardization 2017;5:107–28.

[21] Rajamäki J. Towards Resilient Cyber-Physical eHealth Systems. EQUATIONS 2021;1:78–82.

[22] Sillanpää A, Roivainen H, Lehto M. Finnish Cyber Security Strategy and Implementation. In: Lehto M, Neittaanmäki P, editors. Cyber Security: Analytics, Technology and Automation, Cham: Springer International Publishing; 2015, p. 129–44. https://doi.org/10.1007/978-3-319-18302-2_9.

[23] Lehto M, Neittaanmäki P, Pöyhönen J, Hummelholm A. Cyber Security in Healthcare Systems. In: Lehto M, Neittaanmäki P, editors. Cyber Security: Critical Infrastructure Protection, Cham: Springer International Publishing; 2022, p. 183–215. https://doi.org/10.1007/978-3-030-91293-2_8.

[24] Weber RP. Basic content analysis. vol. 49. Sage; 1990.

[25] Jalkanen J. Is human the weakest link in information security?: systematic literature review 2019.

[26] Yan Z, Robertson T, Yan R, Park SY, Bordoff S, Chen Q, et al. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Comput Human Behav 2018;84:375–82. https://doi.org/10.1016/J.CHB.2018.02.019.

[27] Kisekka V, Giboney JS. The effectiveness of health care information technologies: evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. J Med Internet Res 2018;20:e9014.

[28] Lehto M, Limnéll J. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017.

[29] Priestman W, Anstis T, Sebire IG, Sridharan S, Sebire NJ. Phishing in healthcare organisations: Threats, mitigation and approaches. BMJ Health Care Inform 2019;26:e100031.

[30] Limnéll J, Majewski K, Salminen M. Kyberturvallisuus. Docendo; 2014.

[31] 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. https://doi.org/10.1007/s10916-019-1507-y.

[32] Ewoh P, Vartiainen T. Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. J Med Internet Res 2024;26. https://doi.org/10.2196/46904.

[33] Wani TA, Mendoza A, Gray K. Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. JMIR Mhealth Uhealth 2020;8:e18175.

[34] He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review. J Med Internet Res 2021;23. https://doi.org/10.2196/21747.

[35] Simola J, Rajamäki J. Common cyber situational awareness: An important part of modern public protection and disaster relief 2022.

[36] Hines E, Trivedi S, Hoang-Tran C, Mocharnuk J, Pfaff MJ. Perspectives on Cybersecurity and Plastic Surgery: A Survey of Plastic Surgeons and Scoping Review of the Literature. Aesthet Surg J 2023;43. https://doi.org/10.1093/asj/sjad122.

[37] Looi JCL, Looi RCH, Maguire PA, Kisely S, Bastiampillai T, Allison S. Psychiatric electronic health records in the era of data breaches – What are the ramifications for patients, psychiatrists and healthcare systems? Australasian Psychiatry 2024;32:121–4. https://doi.org/10.1177/10398562241230816.

[38] Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors 2021;21. https://doi.org/10.3390/s21155119.

[39] Haney J, Lutters W. From compliance to impact: Tracing the transformation of an organisational security awareness programme. Cyber Security: A Peer-Reviewed Journal 2025;8:110–30.

[40] Niki O, Saira G, Arvind S, Mike D. Cyber-attacks are a permanent and substantial threat to health systems: education must reflect that. Digit Health 2022;8:20552076221104664.

[41] Branley-Bell D, Coventry L, Sillence E, Magalini S, Mari P, Magkanaraki A, et al. Your hospital needs you: Eliciting positive cybersecurity behaviours from healthcare staff. Annals of Disaster Risk Sciences 2020;3. https://doi.org/10.51381/adrs.v3i1.51.

[42] Jalali MS, Kaiser JP. Cybersecurity in hospitals: A systematic, organizational perspective. J Med Internet Res 2018;20. https://doi.org/10.2196/10059.

[43] Zhan Y, Ahmad SF, Irshad M, Al-Razgan M, Awwad EM, Ali YA, et al. Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems. Heliyon 2024;10. https://doi.org/10.1016/j.heliyon.2023.e22947.

[44] Noponen S, Parssinen J, Salonen J. Cybersecurity of cyber ranges: Threats and mitigations. International Journal for Information Security Research (IJISR) 2022;12:1032–40.

[45] Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: Insights from the U.S. healthcare industry. Bus Horiz 2019;62:539–48. https://doi.org/10.1016/j.bushor.2019.03.010.

[46] Wasserman L., Wasserman Y. Hospital cybersecurity risks and gaps Review for the non-cyber professional. Front Digit Health 2022;4:135–135. https://doi.org/10.3389/fdgth.2022.862221.

[47] Malatji M, Marnewick A, von Solms S. Validation of a socio-technical management process for optimising cybersecurity practices. Comput Secur 2020;95. https://doi.org/10.1016/j.cose.2020.101846.

[48] Pranggono B, Arabo A. COVID -19 pandemic cybersecurity issues . Internet Technology Letters 2021;4. https://doi.org/10.1002/itl2.247.

[49] Tikanmäki I, Ruoslahti H. Insights on Human Factors Enhancing Cybersecurity. Information & Security 2024;55:225–35.

[50] Rajamäki J. Cyber security education as a tool for trust-building in cross-border public protection and disaster relief operations. 2015 IEEE Global Engineering Education Conference (EDUCON), 2015, p. 371–8. https://doi.org/10.1109/EDUCON.2015.7095999.

Cybersecurity Incident Management (CIM)

1. What is your position or occupation?

Please enter job title.

2. How many years of experience do you have in your current field?

Please enter the number of years.

3. Which country are you currently working in?

Please specify the country.

4. Can you share a recent example where a healthcare organization successfully managed a cybersecurity incident?

5. What key factors contributed to the successful handling of that incident?

6. What technologies or tools and services have been most effective in your healthcare's incident response? Additionally, how does your organization detect cyber threats before they escalate?

7. What cybersecurity services (e.g., Security Operations Center (SOC), Managed Detection and Response (MDR), etc.) does your healthcare organization use, and how effective are they in incident response?

8. Can you describe a cybersecurity incident where the response did not go as planned?

9. What were the main reasons for the failure or delays in managing that incident?

10. What role does human error play in detect, response, and mitigate cybersecurity incident?

12. If you could change one thing to improve cybersecurity incident management (CIM) in healthcare, what would it be?

13. How could healthcare improve cybersecurity policies to reduce CIM failures?