From the Department of Learning, Informatics, Management and Ethics
Karolinska Institutet, Stockholm, Sweden

THINK TWICE BEFORE YOU CLICK!

EXPLORING THE ROLE OF HUMAN FACTORS IN CYBERSECURITY AND PRIVACY WITHIN HEALTHCARE ORGANIZATIONS

Sokratis Nifakos

Stockholm 2023

All previously published papers were reproduced with permission from the publisher.
Published by Karolinska Institutet.
Printed by Universitetsservice US-AB, 2023

ISBN 978-91-8017-082-6
Cover illustration: Jose-Luis Olivares, MIT

Think twice before you click!

Exploring the role of Human Factors in Cybersecurity and Privacy within healthcare organizations

Thesis for Licentiate Degree (Ph.Lic.)

By

Sokratis Nifakos

The thesis will be defended in public at Wangari room, Widerströmska huset, Tomtebodavägen 18a, Solna, on Friday, 22nd September 2023

Principal Supervisor:
Assistant senior lecturer Stefano Bonacina
Karolinska Institutet, Sweden
Department of Learning, Informatics, Management and Ethics, Health Informatics Center

Co-supervisor(s):
Professor Sabine Koch
Karolinska Institutet, Sweden
Department of Learning, Informatics, Management and Ethics, Health Informatics Center

MD, PhD Panos Papachristou
Karolinska Institutet, Stockholm, Sweden
Department of Neurobiology, Care Sciences and Society, Division of Family Medicine and Primary Care

Examination Board:
Professor Audun Jøsang
University of Oslo, Department of Informatics

Professor Fredrik Karlsson
Örebro University, School of Business

Professor Aggeliki Tsohou
Ionian University, Department of Informatics

This thesis is dedicated to my parents, for their support and love and my partner in life, love, and logic Elinor Skarby Hay. Also, to my supervisors, Stefano Bonacina, Sabine Koch and Panos Papachristou who guided me through the labyrinthine corridors of academia at Karolinska Institutet. The invaluable lessons learned within these walls will forever be etched in my heart and mind. Finally, to all my colleagues in LIME for the beautiful deep discussions especially during afterworks.

For the history, the studies in this thesis were conducted during pandemic (COVID-19).

“Every action has consequences”

1 Contents

2 List of abbreviations

PII	Personally Identifiable Information
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
CIO	Chief Information Officer
CISO	Chief Security Information Officer
CH	Cyber hygiene
CIS	Center for Internet Security
STS	Socio-Technical Systems theory
CUREX	Secure and Private Health Data Exchange
HO1	Healthcare Organization 1
HO2	Healthcare Organization 2
HO3	Healthcare Organization 3
HCO	Healthcare Organization
PANACEA	Protection and Privacy of Hospital and Health Infrastructures with Smart Cyber Security and Cyber Threat Toolkit for Data and People
NCSAM	National Cybersecurity Awareness Month
ECSM	European Cybersecurity Month

3 Popular science summary of the thesis

In today's digitally connected world, healthcare organizations as well as healthcare research infrastructures are increasingly relying on technology to manage patients and research data and deliver efficient care. However, with this reliance comes the critical need to ensure cybersecurity and protect privacy. While advanced technology and security measures are essential, it is equally important to recognize the significant impact of human behavior on the security landscape. In our quest to fortify cybersecurity and privacy in healthcare organizations, our research focuses on human aspects. We explore the intricate relationship between human behavior and the vulnerabilities that can compromise sensitive data, aiming to raise awareness and promote effective strategies for safeguarding information that is managed by healthcare organizations. Understanding the human vulnerabilities in these organizations is particularly essential because human behavior plays a significant role in cybersecurity incidents. Employees within healthcare organizations, including doctors, nurses, administrators, and IT personnel, interact with sensitive data on a daily basis and their actions, both intentional and unintentional, can inadvertently expose the organization to risks.

Human vulnerabilities can manifest in various ways; for Instance, employees may fall victim to social engineering attacks, such as phishing emails or phone scams, which manipulate their trust and exploit their willingness to help. Similarly, employees may unintentionally mishandle data, such as sharing sensitive information with unauthorized individuals or using weak systems'[1] passwords that can be easily compromised. Lack of awareness, inadequate training, and a lack of a security-conscious culture can further exacerbate these vulnerabilities. Healthcare research organizations also hold significant amounts of valuable data, including research findings, experimental results, and intellectual property. Protecting the integrity and confidentiality of research data is crucial not only for the organization's reputation but also for scientific progress and patient safety. Exploring the cybersecurity and privacy aspects within healthcare research organizations is vital because they are at the forefront of medical advancements and breakthroughs and the data they hold can be highly sought after by cybercriminals, rival institutions, or even nation-state actors. Understanding the human vulnerabilities within healthcare organizations can help identify potential weaknesses that could be exploited, such as inadequate data management practices or gaps in data sharing protocols. By studying the cybersecurity and privacy aspects within healthcare organizations, we can gain valuable insights into the unique challenges they face and use this knowledge for the development of tailored strategies and solutions that address the specific needs of these organizations. Moreover, it can contribute to the establishment of best practices, guidelines, and policies that promote a culture of security and privacy, ultimately enhancing the protection of sensitive data and ensuring the continued delivery of quality healthcare services and medical advancements.

4 Abstract

The urgent need to protect sensitive patient data and preserve the integrity of healthcare services has propelled the exploration of cybersecurity and privacy within healthcare organizations [1]. Recognizing that advanced technology and robust security measures alone are insufficient [2], our research focuses on the often-overlooked human element that significantly influences the efficacy of these safeguards. Our motivation stems from the realization that individual behaviors, decision-making processes, and organizational culture can be both the weakest link and the most potent tool in achieving a secure environment. Understanding these human dimensions is paramount as even the most sophisticated protocols can be undone by a single lapse in judgment. This research explores the impact of human behavior on cybersecurity and privacy within healthcare organizations and presents a new methodological approach for measuring and raising awareness among healthcare employees. Understanding the human influence in cybersecurity and privacy is critical for mitigating risks and strengthening overall security posture. Moreover, the thesis aims to place emphasis on the human aspects focusing more on the often-overlooked factors that can shape the effectiveness of cybersecurity and privacy measures within healthcare organizations. We have highlighted factors such as employee awareness, knowledge, and behavior that play a pivotal role in preventing security incidents and data breaches [1]. By focusing on how social engineering attacks exploit human vulnerabilities, we underline the necessity to address these human influenced aspects. The existing literature highlights the crucial role that human factors and awareness training play in strengthening cyber resilience, especially within the healthcare sector [1]. Developing well-customized training programs, along with fostering a robust organizational culture, is vital for encouraging a secure and protected digital healthcare setting [3]. Building on the recognized significance of human influence in cybersecurity within healthcare organizations, a systematic literature review became indispensable. The existing body of research might not have fully captured all ways in which human factors, such as psychology, behavior, and organizational culture, intertwined with technological aspects. A systematic literature review served as a robust foundation to collate, analyze, and synthesize existing knowledge, and to identify gaps where further research was needed. In complement to our systematic literature review and investigation of human factors, our research introduced a new methodological approach through a concept study based on an exploratory survey [4]. Recognizing the need to uncover intricate human behavior and psychology in the context of cybersecurity, we designed this survey to probe the multifaceted dimensions of cybersecurity awareness. The exploratory nature of the survey allowed us to explore cognitive, emotional, and behavioral aspects, capturing information that is often overlooked in conventional analyses. By employing this tailored survey, we were able to collect insights that provided a more textured understanding of

how individuals within healthcare organizations perceive and engage with cybersecurity measures.

5 List of scientific papers

I. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. **Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review**. *Sensors* 2021, *21*, 5119.

II. Argyridou E, Nifakos S, Laoudias C, Panda S, Panaousis E, Chandramouli K, Navarro-Llobet D, Mora Zamorano J, Papachristou P, Bonacina S. **Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study.** J Med Internet Res. 2023 Jul 27;25:e41294.

6 Introduction

Cyberattacks targeting healthcare organizations continue to rise, with hackers exploiting vulnerabilities created by human error or manipulation[5]. Healthcare organizations play a critical role in society as they handle vast amounts of sensitive and confidential patient data [6]. This data includes, among others, personal and medical information, financial records, and other personally identifiable information (PII). Protecting this data is of utmost importance to maintain patient trust, comply with privacy regulations [2], and ensure the integrity of healthcare services. However, healthcare organizations are increasingly becoming targets of cyberattacks due to the value and sensitivity of the data they possess [1]. The consequences of a successful breach can be severe, ranging from compromising patient privacy to disrupting healthcare services, and even putting lives at risk [2]. Therefore, exploring the cybersecurity and privacy aspects within these organizations is crucial to identify vulnerabilities and develop effective countermeasures [1]. Our research endeavors to create awareness and devise effective strategies for risk mitigation. Through a detailed investigation of the human factors involved, we aspire to offer insights that aid healthcare organizations in developing comprehensive frameworks for cybersecurity and privacy that consider human elements. We seek to bridge the technology-people gap, focusing on behavioral and cultural aspects to drive meaningful change and fortify healthcare organizations against evolving cyber threats. In order to interpret our studies, we relied on the Socio-Technical Systems (STS) theory, recognizing the relationship between social and technical factors within organizations [7]. Leveraging the STS framework, we constructed an exploratory survey to measure and raise cybersecurity and privacy awareness within healthcare organizations. This survey aims to uncover the prevailing attitudes, practices, and vulnerabilities, paving the way for targeted interventions and improvements. One important factor in our research was to focus on delineating the key concepts of 'cybersecurity,' 'information security,' and 'privacy,' understanding their distinctive threats, risks, and mitigation strategies. These differentiations enable a targeted and comprehensive approach to managing risks and implementing safeguards within healthcare organizations. Below, we highlight the key distinctions in tables 1 and 2 [8]:

Term	Definition
Cybersecurity	Focuses on protecting computer systems, networks, and data from unauthorized access, breaches, and attacks.
Information Security	Pertains to safeguarding data integrity, confidentiality, and availability across all forms of information.
Privacy	Revolves around protecting individuals' personally identifiable information (PII) and sensitive healthcare data.

Table 1: Definitions of Key Concepts

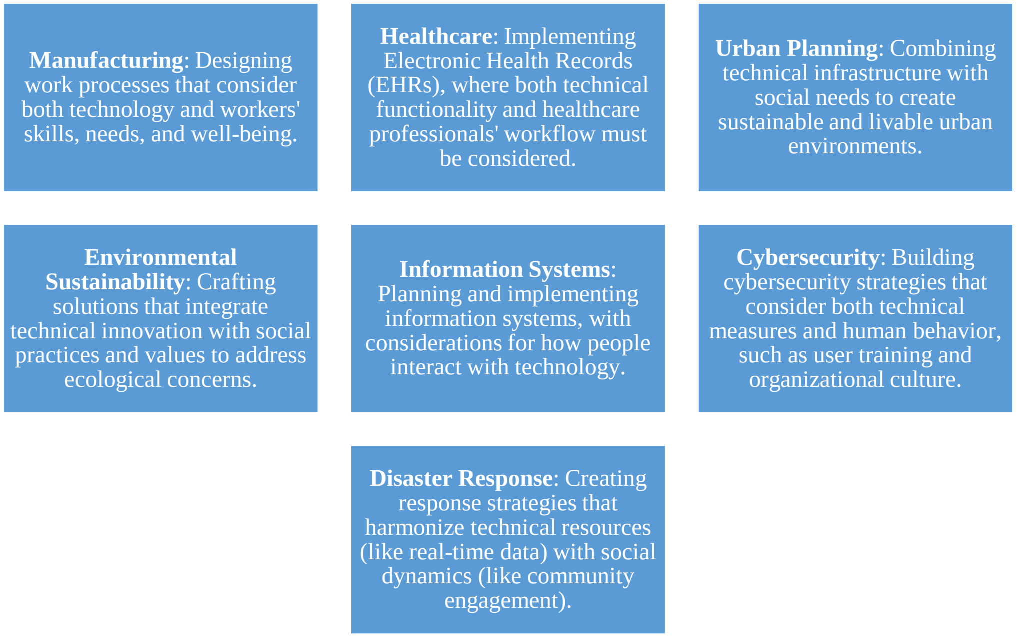
Aspect	Cybersecurity	Privacy
Threats & Risks	Unauthorized access, breaches, attacks.	Legal and ethical requirements, consent management
Mitigation Strategies	Firewalls, encryption, intrusion detection systems, vulnerability management.	Regulatory compliance, data governance, privacy policies.

Table 2: Differentiation Between Cybersecurity and Privacy-Related Threats

Clear differentiation between cybersecurity and privacy-related threats is essential for compliance with jurisdiction-specific regulations, such as GDPR in the European Union and HIPAA in the United States [2]. By identifying and assessing risks separately, healthcare organizations can develop targeted mitigation strategies and allocate resources effectively [1]. This understanding is instrumental in the creation of appropriate controls and frameworks, promoting comprehensive risk assessments [4]. However, it's crucial to recognize the interdependencies between cybersecurity and privacy. They are intertwined, and comprehensive protection requires a coordinated approach that integrates cybersecurity measures with privacy-related safeguards [9]. This holistic perspective ensures robust protection of sensitive healthcare data [9]. Our research further explores the human aspects of cybersecurity and privacy within European healthcare organizations. By understanding the complex interplay between human behavior, technology, and organizational culture, we strive to aid policymakers in developing strategies and policies to protect patient data, ensure privacy, and uphold healthcare integrity. In conclusion, the goal of this thesis is to enhance the understanding of human factors contributing to cybersecurity risks in healthcare organizations, thereby informing decision-making, resource allocation, and the implementation of safeguards. This thesis aims to make significant contributions in shaping European and national policies as well as regulations, fostering patient data protection, privacy maintenance, and the continuous delivery of quality healthcare services. Through detailed exploration of these interconnected themes, we intend in the future to contribute to the design of more tailored guidelines, best practices, and regulatory frameworks, promoting a harmonized and effective cybersecurity approach across the European healthcare sector.

7 Theoretical Framework

As was mentioned before, in this thesis we used the Socio-Technical Systems (STS) theory as our theoretical framework. STS is an approach to understanding the complex relationships that exist between people, technology, and the environment within organizational systems. It emphasizes the interconnectedness and interdependence of the social and technical aspects of a system [7]. STS theory provides a framework that acknowledges the complexity of healthcare organizations, recognizing the integral roles of both human behavior and technological components [7]. By applying STS to structure an exploratory survey for measuring cybersecurity and privacy awareness, we gained insights into the multifaceted challenges and opportunities within healthcare systems. This holistic perspective sets STS apart from other approaches that might focus more narrowly on either technical or human aspects, making it a robust choice for this specific research context.



Manufacturing: Designing work processes that consider both technology and workers' skills, needs, and well-being.

Healthcare: Implementing Electronic Health Records (EHRs), where both technical functionality and healthcare professionals' workflow must be considered.

Urban Planning: Combining technical infrastructure with social needs to create sustainable and livable urban environments.

Environmental Sustainability: Crafting solutions that integrate technical innovation with social practices and values to address ecological concerns.

Information Systems: Planning and implementing information systems, with considerations for how people interact with technology.

Cybersecurity: Building cybersecurity strategies that consider both technical measures and human behavior, such as user training and organizational culture.

Disaster Response: Creating response strategies that harmonize technical resources (like real-time data) with social dynamics (like community engagement).

Figure 1: STS theory applied in different areas

STS theory is particularly focused on the interplay between social (people, roles, culture) and technical (tools, processes) elements within an organization [10]. It views these as intertwined and seeks to optimize them in tandem. Compared to broader theories like General Systems Theory (GST) or more specific approaches like Actor-Network Theory (ANT), STS provides a balanced focus that can be particularly relevant in technological or organizational contexts [10]. It's more concerned with design and optimization, in contrast to Soft Systems Methodology (SSM) problem-solving or Complex Adaptive Systems (CAS) emergent phenomena [10]. In fields like cybersecurity and privacy, where both human behavior and technology play crucial roles, STS offers a valuable perspective by recognizing the complexity and interdependence of these factors. It facilitates a more holistic approach compared to theories that might focus more narrowly on either technical or human aspects alone [7].

STS theory has proven to be a valuable approach in areas where technology is heavily intertwined with human activity [10]. By emphasizing joint optimization and human-centered design, it has been applied to sectors as diverse as healthcare, manufacturing, and urban planning. Particularly in contexts like cybersecurity, where both technical acumen and human behavior play critical roles, STS provides a robust framework for addressing complex challenges [10].

8 Thesis Background

The healthcare sector's cybersecurity posture is of significant importance, given the critical nature of the services it offers and the sensitivity of the data it holds. However, there are concerns regarding vulnerabilities, particularly those that arise from an oversight of the magnitude and implications of cyber threats[12] . The current body of literature provides insights into how human behavior can inadvertently create security gaps, potentially undermining the cyber defense strategies of healthcare organizations. This thesis stems aims to highlight and understand these nuances. In our approach, we undertook a comprehensive review of the literature. This involved an analysis of articles that addressed national case studies, focusing on the financial and societal impacts following service disruptions triggered by cyberattacks. These studies provided invaluable insights into the tangible repercussions of security breaches within the healthcare industry. Our endeavor was to coalesce the accumulated wisdom from organizational case studies, expert viewpoints, and the latest developments in both information security and cybersecurity. At the heart of our exploration was a desire to discern the significance of the human element in bolstering cyber defenses in healthcare. There's an emerging consensus that while there's an abundance of methodologies to gauge and amplify cybersecurity and privacy awareness within healthcare settings, the awareness levels among staff could be worryingly inadequate. This thesis aims to explore the underlying causes of this trend. **Can we obtain a more granular understanding of cybersecurity and privacy awareness across diverse employee groups? And can this understanding guide us toward formulating more effective awareness strategies?** The subsequent sections present our findings, including a graphical representation pinpointing six primary reasons derived from our systematic review.

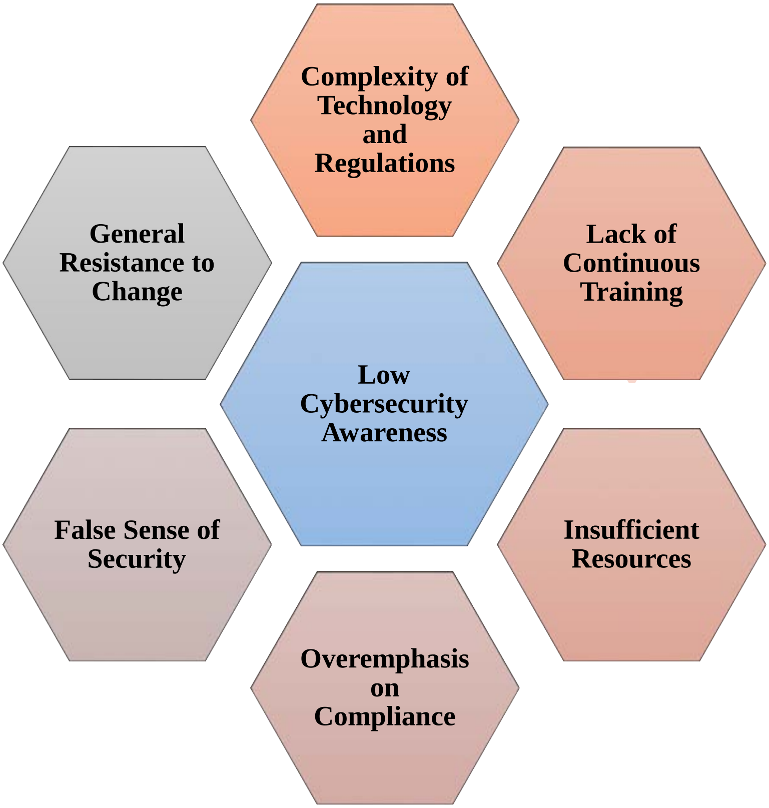

Complexity of Technology and Regulations
General Resistance to Change
Lack of Continuous Training
Low Cybersecurity Awareness
False Sense of Security
Insufficient Resources
Overemphasis on Compliance

Figure 2: Reasons for low cybersecurity awareness between healthcare staff based on the results from the systematic review.

Raising cybersecurity and privacy awareness in healthcare is a deeply intricate endeavor that extends beyond the surface challenges [1]. While it is vital to institute methodologies that measure and impart awareness, achieving robust cybersecurity in a healthcare setting demands a holistic understanding of various underlying dimensions [8]. Firstly, the organization's culture plays a pivotal role. An environment that inherently prioritizes security and treats it as an integral component, rather than an added layer, is likely to have employees who align with these values. The cultural ethos dictates how protocols are received and followed, and how seriously breaches or near-misses are treated. Secondly, one must take into account the unique nature of healthcare work. Healthcare professionals often operate under high-pressure environments, attending to emergencies, making split-second decisions, and managing sensitive patient data. The implementation of cybersecurity measures shouldn't hamper these critical processes but should seamlessly integrate with them.

Furthermore, the landscape of cyber threats isn't static. With the rapid evolution of technology, threats mutate and evolve, often at an alarming pace. The challenge then becomes two-fold: keeping the organization updated about current threats and ensuring that protective measures evolve in tandem with these threats, without causing operational disruptions. Lastly, the needs and attitudes of the staff cannot be underestimated. A one-size-fits-all approach to cybersecurity may be counterproductive [11]. Different departments, roles, and even individual staff members can have varied requirements and attitudes towards cybersecurity. Some might be tech-savvy and quick to adapt, while others might require more guidance. This thesis highlights the importance of training and awareness programs that need to be tailored to cater to these diverse needs, ensuring that every member understands, values, and practices secure behaviors. From these observations, our hypothesis emerged: Current tools and strategies might be overlooking vital organizational and human factors. These oversights could potentially compromise the integrity of the cybersecurity and privacy framework within healthcare organizations. Addressing these challenges is important so to introduce a truly secure and privacy-conscious healthcare environment.

9 Research Aims

The primary objective of this research is to emphasize on the realm of cybersecurity awareness among healthcare staff within healthcare organizations. To achieve this aim, a systematic review of the existing literature was conducted (study I), with the intent of consolidating and synthesizing the current body of knowledge pertaining to human behavior and its impact on the cyber defense strategies adopted by healthcare organizations. Based on the hypothesis mentioned In the previous section that despite different methods we have In place for measuring and raising cybersecurity and privacy awareness, the level of awareness In healthcare staff remains low, we decided to structure a concept study (study II) In order to explore the performance of a an exploratory survey for measuring cybersecurity awareness between healthcare staff and provide optimal controls (mitigation actions) In order to raise awareness. By identifying both strengths and areas for improvement in cybersecurity awareness among healthcare professionals, the research aims to Introduce a holistic approach of measuring and raising cybersecurity and data privacy awareness measures within healthcare organizations.

The findings and insights gleaned from this investigation are expected to recommend more robust cybersecurity protocols and training initiatives, ultimately fortifying the defense against cyber threats in the healthcare domain. Moreover, a better understanding of human factors influencing cybersecurity awareness will aid in designing targeted interventions and educational programs to foster a cybersecurity-aware culture within healthcare organizations, thus mitigating security gaps and bolstering overall cyber defense strategies. The research is driven by the necessity to safeguard sensitive patient data and critical healthcare information against the ever-evolving cyber threats, thereby promoting the overall resilience of healthcare organizations in the face of a dynamic cybersecurity landscape.

9.1 Research Questions

1. **What is the current state of cybersecurity awareness among healthcare staff, and how do human behaviors influence the cyber defense strategies adopted by healthcare organizations?**

    - This question aligns with the aim of conducting a systematic review to synthesize existing knowledge regarding human behavior and cybersecurity strategies in healthcare organizations.

2. **How effective are existing methods in measuring and raising cybersecurity and privacy awareness among healthcare staff, and what are the areas of improvement?**

    - This relates to the hypothesis that the current level of awareness remains low and reflects the need to explore the effectiveness of measurement tools and awareness-raising strategies.

3. **What are the optimal controls and mitigation actions that can be implemented to raise cybersecurity awareness among healthcare staff, and how can these contribute to enhancing information security measures within healthcare organizations?**

    - This corresponds to the goal of the concept study (study II) and involves the exploration of specific controls and interventions to raise cybersecurity and data privacy awareness.

4. **How can a better understanding of human factors in cybersecurity awareness aid in the design of holistic interventions, thereby fostering a cybersecurity-aware culture and promoting overall resilience against cyber threats in healthcare organizations?**

    - This question integrates several aims from the research, including the understanding of human factors, the development of holistic interventions and the promotion of overall cybersecurity resilience.

10 Materials and Methods

10.1 Study I: Systematic Review

Study one was conducted for a comprehensive understanding of the research landscape concerning the chosen topic. By collecting and analyzing all relevant peer-reviewed studies and expert opinions, we gained a holistic view of existing knowledge, including both published and unpublished research, thus minimizing the risk of bias and ensuring a balanced perspective. The review process helped us to identify gaps in the current body of knowledge. This allowed us to ascertain areas that have been extensively studied and those that require further investigation.

In this section, we present the step-by-step methodology used for conducting a systematic review on the topic of cybersecurity within the healthcare domain. The methodology follows the recommendations and guidelines outlined in the PRISMA framework, which ensures a rigorous and transparent approach to the review process.

10.1.1 Protocol and Eligibility Criteria

The systematic review structure was derived from the PRISMA framework [49]We considered articles eligible for inclusion in this review if they were published within the last 11–12 years and were available as Open Access in their full-text version. We acknowledge that this approach may have limitations, such as potentially excluding valuable research published in subscription-based journals. However, we believe that the benefits of transparency, accessibility, equity, and focus outweigh these limitations for the specific goals and context of this review. Only peer-reviewed articles were selected for inclusion. Given the vast volume of cybersecurity research within healthcare, we established specific eligibility criteria for papers, focusing on studies conducted in healthcare settings and clinical environments, where organizations are responsible for storing patient records, such as electronic health records.

We decided to include studies that were published up to 12 years so we ensure that the findings and insights were more likely to be relevant to the current cybersecurity challenges faced by healthcare organizations. Older studies might not adequately reflect the latest technologies, attack vectors, or defense strategies, potentially limiting the review's practical applicability. Moreover, over the past decade, there have been significant advancements in technology and the digitalization of healthcare systems. Including studies from the last 10 to 12 years allows the review to capture how these technological changes have impacted cybersecurity in healthcare. It enables the identification of novel threats and vulnerabilities associated with modern healthcare IT infrastructures. It is also important to mention that by focusing on recent studies, the review addressed the most up-to-date cybersecurity challenges faced by healthcare organizations. This knowledge is crucial for developing effective defense strategies and safeguarding sensitive patient data. Also, the regulatory landscape for healthcare data protection and cybersecurity has evolved significantly in recent years. Including more recent studies enables the review to consider how changes in regulations and policies have influenced cybersecurity practices within the healthcare industry. Additionally, studying recent cybersecurity incidents and breaches in healthcare can provide valuable insights into vulnerabilities and areas that need improvement. These lessons can inform best practices and help healthcare organizations enhance their cyber defense capabilities. Finally, including recent studies ensures that the review accounts for the latest ethical considerations and privacy concerns related to the protection of patient information.

This section outlines the research questions and provides background information that guided the systematic review.

One research question that arises is **R1**: What are the prevalent types of social attacks against individuals in healthcare organizations? It's recognized that an organization's resilience against cybersecurity threats heavily depends on comprehensive data governance policies, spanning data security, privacy, and IT infrastructure security. However, even with protection against traditional cyberattacks, such as Distributed Denial of Service (DDoS), there's been a significant surge in threats like ransomware attacks, leading to increased data breaches. Hence, another pressing research question is **R2:** Which policies and governance measures have healthcare organizations put in place for improved resilience? An integral aspect of cybersecurity is the methodologies used for cyber risk assessment. With the growing intricacy of healthcare services and increasing use of digital technologies, there's a heightened vulnerability to data breaches. While previous risk assessments mainly evaluated IT system security, the rise of social engineering attacks necessitates a re-evaluation of risks arising from human behaviors. This prompts the question **R3:** How do organizations assess cyber risks, particularly focusing on the human factor, to bolster cybersecurity? Furthermore, as cyber threats evolve, there's an increasing emphasis on cybersecurity education and training for healthcare professionals. For instance, training that teaches detection of phishing emails has become crucial. This gives rise to the question **R4:** How crucial are training programs in elevating healthcare professionals' cyber threat awareness, and how can one quantify the effectiveness of such training? Finally, healthcare, being a vital infrastructure globally and in Europe, can't afford disruptions as these could escalate into national emergencies. With entities like the European Union Agency for Cybersecurity (ENISA) offering guidelines to boost national cyber resilience and the reality of coordinated cyber attacks causing significant human and economic losses, it's pertinent to ask **R5:** What are the cyber defense strategies proposed by national and global bodies to fortify cyber resilience?

10.1.2 Information Sources

To conduct a comprehensive literature search, we employed eight different search strings across three major bibliographic databases: PubMed®/MEDLINE, Cumulative Index to Nursing and Allied Health Literature (CINAHL), and Web of Science (WoS). The search results from each database were exported and imported into the collaborative filtering platform Rayyan. Rayyan facilitates a blind review process by multiple authors, where imported results from PubMed, CINAHL, and WoS are individually assessed based on the previously defined inclusion and exclusion criteria. By enabling the "Blind On" feature, the results remain invisible to other researchers, mitigating potential biases. The literature search process strictly adheres to the recommendations provided by PRISMA to ensure the systematic review's credibility and validity.

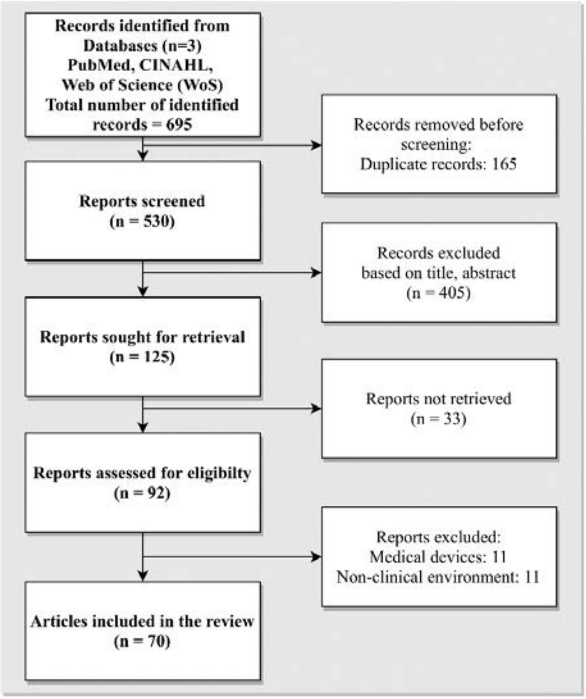

Records identified from Databases (n=3) PubMed, CINAHL, Web of Science (WoS) Total number of identified records = 695
Records removed before screening: Duplicate records: 165
Reports screened (n = 530)
Records excluded based on title, abstract (n = 405)
Reports sought for retrieval (n = 125)
Reports not retrieved (n = 33)
Reports assessed for eligibilty (n = 92)
Reports excluded: Medical devices: 11 Non-clinical environment: 11
Articles included in the review (n = 70)

Figure 3: Literature search process, according to PRISMA recommendations [1].

In addition to the detailed method for data collection, we conducted a rigorous analysis of the gathered data to synthesize the findings from the various studies included in the review. The data extraction was planned in a way that ensured all relevant information was extracted from each included study, such as the study design, population, interventions, outcomes, and key findings. This information was clustered for further analysis. The extracted data were synthesized through a thematic analysis approach. Themes and sub-themes were identified based on the research questions, and the findings were organized under these themes. Further, the synthesized findings were interpreted in the context of the existing literature, regulations, and industry practices. This provided a comprehensive understanding of the cybersecurity landscape in healthcare, including novel threats, vulnerabilities, and potential mitigation strategies.

In summary, this section outlines the meticulous methodology adopted for the systematic review on cybersecurity in healthcare. The research questions were carefully formulated to cover various aspects of the topic, and specific search strings were designed to search the relevant databases. The eligibility criteria were established to include peer-reviewed articles within a specific time frame, focusing on studies conducted in healthcare settings. The search was conducted across multiple bibliographic databases, and the review process was carried out collaboratively using the Rayyan platform, following the PRISMA guidelines for transparency and quality assurance.

10.2 Study II: A concept study

Study II, is a cross-sectional, exploratory survey study that is complemented by a proposed risk-based survey analysis approach, providing a comprehensive understanding of its context, significance, and **potential impact** on healthcare organizations. **As a concept study, it explores the novelty of the idea and its potential implications.** We conducted a thorough investigation into the background of the concept, including the results from the systematic review of the literature, Study I. and we gained a deeper understanding of the underlying challenges and opportunities in healthcare cybersecurity and data privacy awareness. The central aim was to introduce a novel methodology to measure cybersecurity awareness among varying employee groups in healthcare organizations and introduce different strategies to enhance the awareness levels.

The study was structured in two phases. During phase 1 we utilized a unique survey-based risk assessment tool and we tried to explore specific needs and gaps for different employees' roles within a healthcare organization. This human-centric approach aimed to recommend tailored controls like training programs, awareness initiatives, and incentives, customized to the specific employees role and responsibilities, as well as to the organization's unique culture. During phase 2 we measured the awareness level of different groups of employees within three different healthcare organizations by applying the survey-based risk assessment tool and conceptually suggest different controls for raising awareness among the staff that captured with low or medium cybersecurity and privacy awareness.

Ultimately, the paper's methodology presents a systematic strategy to cultivate a security-aware culture within healthcare organizations. By gathering key insights into current awareness levels and practices across various employee groups, it enables organizations to gain a well-rounded view of their strengths, weaknesses, and potential areas of vulnerability.

A key differentiator of the presented methodology is its explicit recognition of the human factor in cybersecurity defense. It acknowledges that employees play a critical role in the organization's security posture [4]. **By addressing the specific needs and challenges faced by different employee groups**, the methodology aims to strengthen the organization's overall security resilience [4]. The primary objective is to recommend **targeted human-centric controls that go beyond technical measures** [4]. These controls focus on nurturing a security-conscious mindset among employees. Examples include regular awareness activities, tailored training programs, and incentives or rewards for exemplary security practices. Empowering employees to proactively identify and mitigate cyber threats enhances the organization's security posture. Moreover, it emphasizes the importance of tailoring controls to suit each healthcare organization's unique culture, personnel backgrounds, and operational roles. A customized approach maximizes the impact and effectiveness of controls, recognizing that a one-size-fits-all approach may not yield desired outcomes. Finally, a significant advantage lies in its cost-effectiveness. By carefully selecting controls from a smaller subset of candidate controls, organizations optimize their resources while achieving desired outcomes. This approach enhances cybersecurity and data privacy awareness without imposing undue financial burdens.

10.2.1 Definition of Cyber Hygiene

Cyber hygiene refers to the best practices and habits that individuals and organizations should adopt to maintain a secure online environment [4]. Just like personal hygiene helps prevent illness and promotes well-being, cyber hygiene helps prevent cyber threats and promotes digital safety. The CH methodology involves implementing a structured set of practices, protocols, and controls that focus on maintaining the security and privacy of an organization's digital assets [4]. The survey-based risk assessment approach used in this study involves collecting data through a well-designed survey that targeted different employee groups within organizations.

10.2.2 Survey Construction

This survey was carefully crafted to assess the employees' awareness, knowledge, and adherence to cybersecurity and data privacy best practices. By gathering information directly from the workforce, the assessment becomes more comprehensive and representative of the organization's overall cybersecurity posture. The methodology was structured through a systematic process, started with the collection and analysis of survey responses, aiming to identify and evaluate the unique needs and gaps within four employee groups (Administrative, Medical/Clinical, IT/Technical, and Executive/Security) across three European healthcare organizations. In conducting a cross-sectional exploratory survey study, accompanied by a risk-based analysis approach, the methodology provided an all-encompassing assessment of cybersecurity and privacy awareness. The designed online survey, comprised of 28 questions, targeted specific cybersecurity and data privacy risks within each employee group, categorizing them into seven distinct risk areas. With 356 responses collected and analyzed, the systematic approach went further than just gathering information. It encompassed a collaborative effort involving the CUREX project working group and representatives from the three healthcare organizations. Together, we formed a consensus group of sixteen members with diverse expertise. This group conducted a comprehensive review of existing literature, integrating findings from the systematic review, Study I, and aligning them with documents, reports, and recommendations from leading healthcare and cybersecurity authorities. The result was a coherent and methodically developed tool to assess employee awareness in critical areas such as cybersecurity, data privacy, training, and the use of connected devices, reflecting a concerted effort to enhance security within healthcare organizations.

The consensus group identified four main employee groups within healthcare organizations: Administrative, Medical/Clinical, IT/Technical, and Executive/Security personnel. Each group's awareness level in cybersecurity and data privacy, as well as their daily tasks and potential exposure to risks, were considered to be different. After consulting with representatives from the healthcare organizations, various risks related to cybersecurity were recognized, and these risks were then clustered into representative risk categories. An initial set of questions was developed, each associated with a specific risk category to quantify the relevant risks based on the respondents' answers. The questions went through multiple iterations of review and refinement, and new risks were considered, leading to the creation of new risk categories or adaptations of existing ones, followed by the addition of more questions. After several rounds of review, the consensus group finalized a comprehensive survey comprising 28 questions. The survey questions were originally prepared in English and later translated into the native languages of the healthcare organizations involved in the CUREX project. The survey was then administered in three languages (Catalan, Spanish, English) to ensure accurate data collection and analysis. The process of creating the final survey questionnaire for mapping the Cyber Hygiene landscape involved a comprehensive review of existing literature and available resources. The aim was to gather essential insights to design targeted questions that would shed light on various aspects of employee awareness and preparedness in the healthcare sector, particularly regarding the identified top threats.

Among the 28 survey questions, each question could be of single-answer or multiple-answer format. Furthermore, the survey questions utilized a Likert scale to assess the respondents' awareness, agreement, frequency in adopting cyber hygiene practices, knowledge, and satisfaction.

The Likert scale options for different types of questions were as follows:

- For questions related to awareness: YES/NO/I don't know
- For questions related to agreement: 1 = I strongly disagree | 5 = I strongly agree
- For questions related to frequency in use (adoption of cyber hygiene practices): 1 = Never | 5 = In every daily activity
- For questions related to knowledge: 1 = I have no knowledge | 5 = I am an expert
- For questions related to satisfaction: 1 = Very disappointing | 5 = Very Satisfying

In the scale, 1 represented the lowest impact value, while 5 denoted the highest impact value for each question. By analyzing these marks, we assessed the awareness and understanding of cyber hygiene for individual respondents and each employee group.

Each member of the employee groups was presented with specific statements to evaluate their awareness and relevance concerning the survey's purpose. They provided ratings on a scale from 1 to 5, where 1 indicated low awareness or relevance, and 5 indicated high awareness or relevance.

Based on the responses collected from the participants, we evaluated the extent of awareness and relevance within each employee group. Consequently, we proposed an appropriate strategy and associated controls to enhance cybersecurity and data privacy awareness. These strategies aimed to address the identified gaps and improve the overall cybersecurity posture within the organizations. The study explored only the recommendation of different controls based on the awareness levels, without evaluating the performance/effectiveness of the suggested controls. You will find further Information regarding the results captured after the analysis of the data collected In the "Results" section under Study II.

The questionnaire included specific questions to gauge employees' familiarity with these top threats, their awareness of relevant incidents both within and outside their organization, their ability to recognize such incidents at early stages, and their confidence in handling them. To ensure clarity and distinction, the risk categories and associated survey questions were structured in a way that clearly differentiated between cybersecurity risks and data privacy risks, considering the specific nature of these top threats. Incorporating recommendations from cybersecurity agencies and organizations, the survey covered several risk categories. These recommendations encompassed important areas such as:

i) Raising cybersecurity awareness: Assessing the level of knowledge and consciousness among employees about cybersecurity best practices and potential risks.

ii) Securing medical and portable devices, including Bring-Your-Own-Device (BYOD) and Bring-Your-Own-App (BYOA) schemes: Examining the extent to which employees follow secure practices when using personal devices for work purposes.

iii) Ensuring secure physical access and health information: Evaluating the measures taken to safeguard physical access to sensitive data and health-related information.

iv) Educating users against social engineering attacks (e.g., phishing emails): Understanding the level of preparedness among employees to identify and respond appropriately to social engineering attempts aimed at manipulating them into compromising security.

10.2.3 Study Population

The study Included four primary employee groups within each healthcare organization, all of whom were eligible participants for the survey study:

1. Administrative (e.g., administration manager, secretary, reception, call center, human resources, etc.)
2. Medical/Clinical (e.g., department/unit manager, doctor, nurse, etc.)
3. IT/Technical (e.g., IT manager, IT staff, software developer, etc.)
4. Executive/Security (e.g., Director, Sub Director, Hospital Manager, Chief Information Security Officer (CISO), Chief Security Officer (CSO), Data Protection Officer (DPO), etc.)

It is worth noting that the Administrative and Medical/Clinical groups typically had a larger number of employees in comparison to the IT/Technical and Executive/Security groups.

10.2.4 Participant Recruitment

During the implementation and testing stage (phase 2), a systematic recruitment process was employed to engage users in the study. The recruitment was initiated using both proprietary methods (such as internal e-Learning tools or email campaigns) and open online survey tools, including the EU Survey tool. Additional recruitment channels involved reaching out to potential participants through email and utilizing existing eLearning platforms commonly accessed by hospital doctors for medical learning and other events. The user recruitment phase commenced in mid-June 2020 and continued until the end of September 2020.

Prior to participating in the survey, all respondents were presented with a survey preamble that provided information about the survey's purpose. To ensure ethical compliance, all participants were required to provide their digital consent before proceeding with the survey questions. To avoid duplicate entries, measures were implemented to prevent users with the same IP address from accessing the survey multiple times.

Confidence Interval Calculation

To ascertain the confidence interval based on the survey responses relative to the population size, a significance level of $P < 0.05$ (95% confidence level) was adopted. The online confidence interval calculator was utilized for this calculation.

10.2.5 Risk Categories

To facilitate risk analysis and profiling of each employee group, the survey questions were organized into seven distinct risk categories based on their respective topics and structure. This categorization allowed for a clear understanding of the risks pertaining to each group.

The table comprises three columns:

1. The first column denotes the name of the risk category.
2. The second column specifies the number of survey questions associated with each category.
3. The third column provides a detailed description of the risks encompassed within the corresponding category.

Risk Category	Numbers Of Survey Questions	Risk Description
Cyber hygiene	2, 3, and 4	Not aware of what cyber hygiene is
Cybersecurity awareness	8, 11, and 13	Not aware of cybersecurity threats in health care and related incidents
Data privacy and protection awareness	5, 6, 8, 12, and 14	Not aware of what GDPR is or of data privacy and protection threats in health care and related incidents
Cybersecurity training	9, 15, 17, and 20	Not attending existing training, not considering cybersecurity during daily work, not knowing about internal procedures for cybersecurity threats, and limited knowledge about cybersecurity (self-assessed)
Data privacy and protection training	7, 10, 16, 18, 19, and 21	Not attending existing training, not considering data privacy during daily work, not knowing about internal procedures for data privacy threats and who is responsible for data protection, managing personal data frequently, and limited knowledge about data privacy (self-assessed)
Communication channels	22, 23, and 24	Limited number of communication channels that are available in the organization or preferred by employees and limited communication with IT personnel
Secure connection and use of devices	25, 26, 27, and 28	Not aware of or not following policies, guidelines, or best practices regarding remote connection, using public access networks, using personal devices (BYOD), and using personal USB sticks

Table 3: Risk categories for all employee groups

10.2.6 Risk evaluation matrix

In this section, we outline the risk-based approach specifically designed for analyzing survey responses, with the goal of enhancing cybersecurity awareness. This approach encompasses various processes tailored to each healthcare organization's needs, including the identification, analysis, monitoring, evaluation, and management of different risks [50]. Utilizing a risk matrix and a scoring system ranging from 1 to 5, we classified the risks, followed by a thorough evaluation that led to specific strategies for handling them. These strategies aimed at increasing cybersecurity and data privacy awareness across diverse employee groups and were linked to recommended controls for managing the unique risks faced by each group.

The impact probability risk matrix consists of two dimensions: risk probability, indicating how likely a risk is to occur, and risk impact, reflecting the significance and severity of that risk. By multiplying risk probability and risk impact, we derived a risk evaluation score that categorizes the risk as low, medium, or high.

Risk Probability	**Negligible [1]**	**Minor [2]**	**Moderate [3]**	**Considerable [4]**	**Severe [5]**
Very likely (5)	Low-medium	Medium	Medium-high	High	High
Likely (4)	Low	Low-medium	Medium	Medium-high	High
Possible (3)	Low	Low-medium	Low-medium	Medium	Medium-high
Unlikely (2)	Low	Low	Low-medium	Low-medium	Medium
Very unlikely (1)	Low	Low	Low	Low	Low-medium

Table 4: Impact probability risk matrix

Table 5 displays the risk evaluation matrix, guiding specific risk strategies based on the determined risk evaluation marking. Each strategy aligns with specific controls for managing risks, whether by mitigating, reducing, monitoring, checking, or accepting them. For example, higher risks necessitate more frequent training sessions (such as weekly), beginning with basic, beginner-level material. Conversely, lower risks may call for less frequent training (monthly or quarterly), encompassing more advanced, detailed content. If the risk is deemed very low, it is considered acceptable, and employees may be acknowledged and rewarded.

Risk Marking	Risk Evaluation	Risk Strategy	High-level Action Plan
20-25	High	Mitigation	Mitigate the risk: improve skills, raise awareness, monthly or weekly actions for beginner level
15-19	Medium-high	Reduction	Reduce the risk: improve skills, raise awareness, quarterly or monthly actions for intermediate level
10-14	Medium	Monitoring	Monitor the risk: increase awareness, semiannual or quarterly actions for intermediate or advanced level
5-9	Low-medium	Checking	Check the risk: retain awareness, annual or semiannual interventions for advanced level
1-4	Low	Acceptance	Accept the risk: acknowledgment and rewards

Table 5: Risk Evaluation Matrix

Now for using the risk evaluation matrix we define below the ***risk impact*** and the ***risk probability.***

The risk impact is determined through a scoring system that ranges from 1 to 5, reflecting the structure of the survey questions. A score of 1 signifies the lowest risk impact, while a score of 5 indicates the highest impact. Scores between 2 and 4 correspond to medium levels of risk impact [4].

Risk impact number	Risk impact	Frequency	Agreement	Knowledge	"Yes," "no," or "I don't know"	Multiple answers
1	Low	Daily	Strongly agree	In depth	"Yes"	All selected
2	Low-medium	Weekly	Agree	Very well	N/Aa	Many selections
3	Medium	Monthly	Cannot say	Well	"I don't know"	Enough selections
4	Medium-high	Rarely	Disagree	Heard of it	N/A	Few selections
5	High	Never	Strongly disagree	Never heard of it	"No"	One or nothing

a N/A: not applicable.

Table 6: Risk impact definition for different types of survey questions.

The risk probability is determined by the total number of responses. A high number of responses indicates a greater likelihood of the risk occurring, while a low number of responses suggests a lower likelihood of the risk happening [4].

Risk probability number	**Risk probability**	**Range**
1	Very unlikely	0 – Re × (1/5)
2	Unlikely	Re × (1/5) – Re × (2/5)
3	Possible	Re × (2/5) – Re × (3/5)
4	Likely	Re × (3/5) – Re × (4/5)
5	Very likely	Re × (4/5) – Re

Note: Re represents the number of responses.

Table 7: Risk probability definition

We applied the following formula for calculating the risk marking [4]:

$$\boldsymbol{Risk\ Marking} = \sum_{i=1}^{n} \boldsymbol{risk\ impact(i) * risk\ probability(i) * RF}$$

where *i*=1,..., *n* is the number of responses and RF is the risk factor.

The risk factor is calculated using the formula: Risk Factor = 5 / (NoQ) × (NoR), where NoQ represents the total number of questions in each risk category, and NoR is the total number of responses from each employee group within each organization. The value 5 is selected as the maximum score in the system to represent the highest possible level of risk [4].

Risk impact number	Risk impact	Frequency	Agreement	Knowledge	"Yes," "no," or "I don't know"	Multiple answers
1	Low	Daily	Strongly agree	In depth	"Yes"	All selected
2	Low-medium	Weekly	Agree	Very well	N/Aa	Many selections
3	Medium	Monthly	Cannot say	Well	"I don't know"	Enough selections
4	Medium-high	Rarely	Disagree	Heard of it	N/Aa	Few selections
5	High	Never	Strongly disagree	Never heard of it	"No"	One or nothing

aN/A: not applicable.

Table 8: Risk impact definition for different types of survey questions.

11 Results

The results section presents a comprehensive analysis and interpretation of the data collected in studies I and II and aims to highlight the key findings and insights related to the research aims. It begins by providing an overview of the main findings in Study I. and in continuation, it presents the main findings In Study II.

11.1 Study I, main findings

The significance of cybersecurity in conjunction with organizational awareness and training cannot be overstated. This importance is further underscored by the increasing frequency of published articles on this subject, as evident even in the relatively short span of six months in 2021.

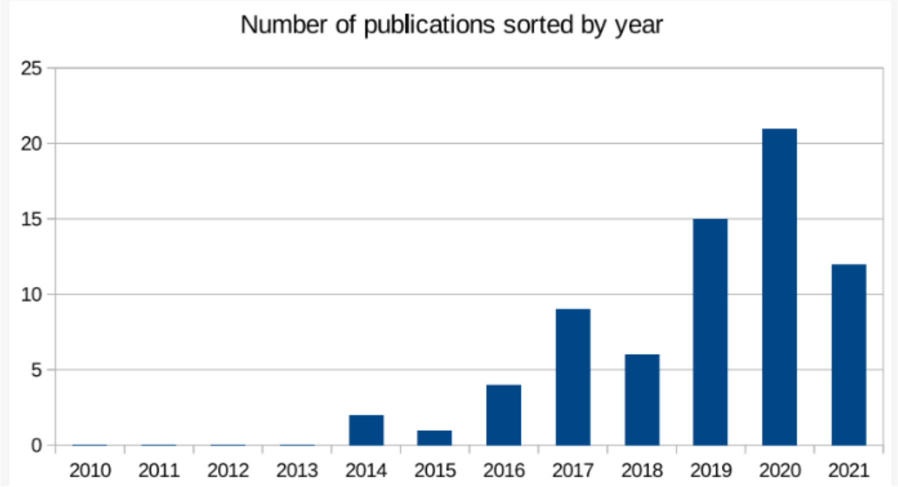


Figure 4: The selected 70 articles grouped according to the year of publication [1].

The total number of articles in this domain has already reached nearly half the number of articles published last year, indicating a significant increase in research activity. Furthermore, these articles represent over 75% of the publications from 2019, highlighting the growing attention given to the topic of interest. Additionally, the individual rankings and relevance of these articles offer valuable insights into the specific challenges that researchers are addressing within the field, as presented in figure 4.

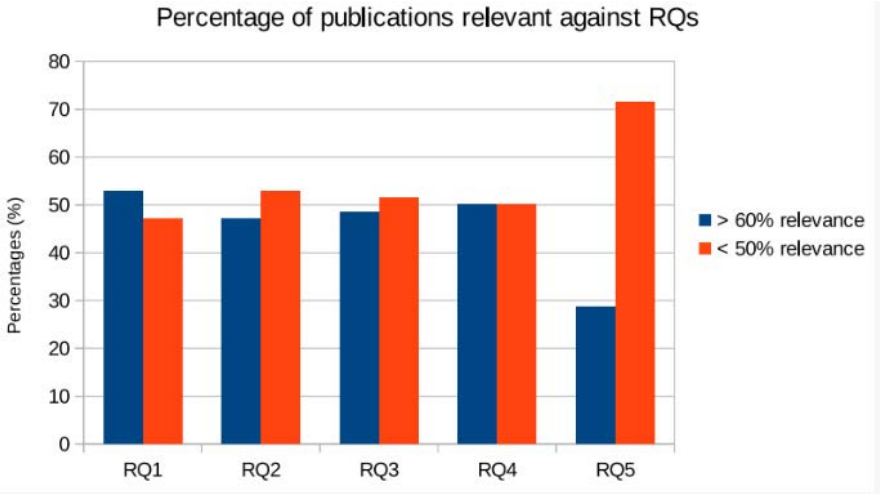


Figure 5: Relevance of articles addressed against each RQs [1].

The analysis of the literature reveals varying degrees of focus on different aspects of cybersecurity in the healthcare industry. For Research Question 2 (RQ2), the percentage of articles addressing organizational cyber resilience policies and governance is relatively low. Similarly, Research Question 3 (RQ3) finds a limited number of articles covering methodologies for healthcare organizations to conduct cybersecurity risk assessments. On the other hand, articles related to training and awareness of cybersecurity among healthcare stakeholders are more evenly distributed in the literature, as demonstrated in Figure 4 for RQ4. Regarding Research Question 5 (RQ5), the results in Figure 4 indicate a significant lack of national audits within the healthcare industry that report on cyber resilience. In terms of source credibility, among the total articles selected for the survey, the majority (91.43% or 64 articles) originate from peer-reviewed, high-impact journals, while a smaller portion (8.57% or 6 articles) are selected from reputed conferences.

11.1.1 Common Cyber Threats Faced by Healthcare Organizations

The literature concerning cyber threats faced by healthcare organizations can be broadly categorized into three main groups: (i) attacks exploiting IT infrastructure vulnerabilities, such as misconfigurations, denial of service (DoS), DDoS, SQL injections, privilege escalation, man-in-the-middle (MITM) or eavesdropping, and cryptographic attacks; (ii) ransomware attacks, aimed at disrupting services and holding healthcare data hostage for financial gains; and (iii) emerging threats targeting human vulnerabilities to gain access to healthcare infrastructure. The historical development of cyber threats against IT systems dates back to 1982 when the first computer virus, "Elk Cloner," was released by a high-school student, marking the beginning of sophisticated cyberattacks over the last two decades. The changing nature of cyber attacks in healthcare and clinical environments is evident as healthcare organizations increasingly adopt digital technologies. The significance of protecting patient data and electronic health records from both external and internal attacks has become a major focus.

Ransomware attacks gained prominence with the Hollywood Presbyterian Medical Center paying a ransom in 2016, leading to a rise in attacks motivated by financial incentives and service disruption. Efforts have been made to raise awareness of ransomware's impact, and best practices have been suggested to enhance cyber hygiene for healthcare professionals. Social engineering attacks, particularly phishing, have emerged as a notable threat, exploiting public information from social media platforms to compromise healthcare professionals. Research has analyzed the impact of phishing attacks and the need for enhancing cybersecurity strategies, involving high-level management teams and international standards like ISO/IEC 80001-1. Despite the consensus on the need to enhance service quality, economic barriers hinder the adoption of cyber defense solutions.

11.1.2 Strengthening Organizational Cybersecurity Capabilities: Strategies and Approaches

Healthcare data breaches pose a growing threat to the industry, leading to data loss, monetary theft, and even endangering human lives due to attacks on medical devices and infrastructure [29]. The increasing frequency and evolving nature of cyber attacks against healthcare and clinical environments necessitate comprehensive risk prevention and mitigation efforts across organizations.

However, several healthcare organizations face challenges in implementing effective cybersecurity measures due to the complexity of their operations, numerous legacy systems, and a "if it ain't-broke-don't fix it" approach among senior management [25]. Healthcare organizations operate in technology-saturated environments, managing diverse devices, workflows, and specialized services, adding to the complexity. Regulatory pressures, particularly concerning the security of personally identifiable information (PII), further add to the challenges [26],[27],[29]

In this multi-disciplinary field of cybersecurity, a specialized cyber security workforce framework is suggested, comprising seven roles to counteract cyberattacks effectively. These roles involve conceptualizing and building secure ICT systems, overseeing governance, identifying and mitigating internal threats, and performing specialized intelligence analysis and investigation [28]. However, cybersecurity strategies should adopt a top-down approach, with CIOs and CSIOs setting the vision for enhancing cyber resilience [29].

The literature review reveals two main categories of organizational strategies: technical solutions and human factor approaches. Collaborative information sharing systems are recommended, where cyber attack incidents are shared with other healthcare organizations for blacklisting origins and swift reconfiguration of IT systems [29]. International standards like ISO/IEC 27002:2013 and ISO 27799:2016 are proposed for enhancing cyber resilience, providing guidelines for information security controls and securing the ICT infrastructure [25]. Technical mitigation measures include regular backups, firewall implementation, network segmentation, least privilege principle, regular updates, virus protection, data encryption, intrusion detection, secure system configurations, and mobile device protection [31]. Emphasizing system configuration and user-focused strategies can help ensure reliable system defense [31].

11.1.3 Cyber Risk Assessment Methodology for Healthcare Organizations

The integration of digital technologies and digitalization strategies has significantly transformed healthcare organizations, enabling them to provide teleconsultation, teleexpertise, electronic storage of patient records, and seamless interfacing with connected health devices [32]. This pervasive reliance on digital solutions necessitates a detailed analysis of the various risk assessment methodologies adopted within healthcare institutions.

In line with the ISO/IEC 27000:2018 standard [25], information security is defined as the preservation of data confidentiality, integrity, and availability processed by computer systems. However, given the complex nature of healthcare systems, a broader terminology is advocated [32]. Historically, threats to healthcare organizations were primarily physical in nature, encompassing issues like fire or power interruptions, unauthorized physical or electronic access, and authorized physical or electronic access [25]. However, the landscape of threats has evolved significantly, and healthcare organizations now face substantial challenges related to cyber attacks.

Authors in [32] emphasize the critical importance of modeling various forms of cyber threats and building threat intelligence on evidence-based knowledge. Such intelligence should include context, mechanisms, indicators, implications, and actionable advice to counter emerging threats and safeguard assets. Numerous attempts to formalize threat modeling methodologies and classification models have been reported in the literature, such as STIX, OCTAVE, STRIDE, VAST, and others [32][33]. **These frameworks provide valuable insights into structuring threat assessments for the development of cyber risk assessments within healthcare organizations.** Integration of connected medical devices introduces additional risks, prompting recommendations on organizational policies and risk assessment methodologies [34]. Authors suggest [34] the adoption of international standards, like ISO/IEC 80001, to document, manage change, handle risks, and assign responsibilities from a management perspective.

It is observed that employee negligence and carelessness surrounding information security contribute significantly to data breaches [11]. Therefore, the cybersecurity risk methodology should focus on modeling employee behavior, for which the Information Security Climate Index (ISCI) offers a concise and validated tool.

A three-stage cybersecurity risk management roadmap is proposed in [26], which involves understanding cybersecurity risks, valuing these risks along with mitigation measures, and effectively communicating cybersecurity actions and solutions. The methodology includes identifying core mission-critical functions and processes, creating an inventory of vulnerable assets associated with these functions, and assigning risk impact scores to each asset. A case study on the WannaCry attack on the U.K. NHS services [27] highlights the importance of adapting to evolving technological challenges to mitigate the impact of cyberattacks on healthcare service delivery. The review highlights "social engineering" attacks as an evolving threat to healthcare services. Several articles assess the response of organizations in promoting cyber hygiene among healthcare professionals and stakeholders. While existing practices have focused on technical developments, it is recognized that the evolving nature of cyber threats requires a deeper analysis of human behavior. **Thus, organizational strategies to enhance cyber threat awareness and provide training for healthcare professionals on cyber hygiene practices are recommended.**

11.1.4 Enhancing Cyber Resilience through Human Factors

The role of human factors in enhancing cyber resilience has been the subject of extensive research, with 21 articles addressing this topic [35]. These articles were evaluated by the authors, who assigned individual scores to each publication. In this section, we provide a concise analysis of the key aspects discussed in the literature, specifically focusing on the impact of "social engineering" attacks on healthcare professionals. The publications are categorized into three main groups:

(i) training and awareness activities related to social engineering attacks (e.g., phishing)

(ii) activities aiming to promote general information security awareness against cyber attacks

(iii) best practice recommendations from other industries to enhance cyber hygiene

One of the earliest studies that addressed behavior training in healthcare and its role in strengthening organizational defense against cyber attacks was published in AMCIS 2016 [36]. **This study developed a training program targeting employee habits, using the Martin-Morich model of consumer behavior.** The authors emphasized that repetitive tasks often become automatic, leading to low habitual practice in cybersecurity, even with increasing governance regulations. To address this, the training program focused on phishing, password sharing, and cloud service attacks, highlighting the importance of habit-changing training policies for enhancing cyber resilience in healthcare organizations. Subsequent studies continued to explore ways to improve cybersecurity awareness

Phishing attacks were identified as a significant cause of data breaches in healthcare, despite organizational efforts to mitigate them. Several studies investigated the reasons why hospital employees are susceptible to phishing attacks. For instance, one study examined the positive correlation between workload and the click rate on phishing links [37]. Another study emphasized the need for "cyber hygiene" training programs to enhance understanding of cybersecurity risks [38]. Long-term and short-term cognition factors affecting human susceptibility to social engineering attacks were also identified [39]. Some studies conducted large-scale field experiments to evaluate the effectiveness of awareness and training programs. One study observed that personal experience was more effective in threat identification, while email information dissemination had limited impact [40]. It was evident from the literature that promoting awareness among healthcare professionals is crucial. While technologies are essential, they must be supported by a strong organizational culture and internal environment that prioritize governance and compliance [32]. Additionally, healthcare professionals' use of personal devices for accessing healthcare records under the BYOD scheme raised cybersecurity concerns due to a lack of awareness [41]. Studies also discussed cybersecurity training in other contexts beyond phishing attacks. The importance of targeted training programs and simulations to raise awareness and build knowledge and skills in cybersecurity measures was emphasized [30]. The categorization of connected medical devices based on risk assessment was proposed to increase cybersecurity measures [42]. Furthermore, a study focused on evaluating participants' perception and motivation to secure their mobile devices, highlighting the need for targeted security awareness programs [43]. Beyond the healthcare industry, cybersecurity training has been extensively investigated. One notable study proposed curriculum development based on practical challenges prepared by security experts and formal study programs facilitated by educators [44]. Threat perception and coping appraisals were identified as mediators for positively influencing information security in employees [45]. A training program methodology was developed, encouraging participants to apply learned insights from personal life experiences to cybersecurity, aiming to minimize security fatigue [46]. While several articles emphasized the need for training programs, some studies highlighted the lack of attention given to cybersecurity in comparison to other critical issues, such as epidemics or natural disasters [47]. The importance of updating the content of training programs and increasing their frequency to address evolving cyber threats was also noted [48]. **Overall, the literature emphasized the significant role of human factors and awareness training in enhancing cyber resilience, particularly in healthcare. Properly tailored training programs and a strong organizational culture are essential for promoting a secure and safe digital healthcare environment.**

11.2 Study II, main findings

The purpose of this study introduces a novel Cyber Hygiene (CH) methodology that employs a distinctive survey-based risk assessment approach to measure cybersecurity and data privacy awareness among various employee groups within healthcare organizations (HCOs) and recommend optimal controls. Since Study II is a concept-based study, the efficiency of these controls is uncertain, and it Is planned Investigate It further from our research group in the near future [4]. The survey-based assessment helped uncover specific risk areas that require attention and resources.

With a better understanding of the organization's risk landscape, decision-makers can prioritize investments in cybersecurity measures that provide the highest impact. To complement the risk management strategy, the study recommends human-centric controls. Human-centric controls focus on the human element within cybersecurity, acknowledging that employees play a crucial role in safeguarding the organization's data and systems. These controls include targeted training programs, awareness campaigns, regular security reminders, and establishing a security-conscious culture within the organization. By addressing human behavior and attitudes towards cybersecurity, these controls could contribute significantly to reduce human errors and strengthening the organization's overall security posture.

11.2.1 Application of the Exploratory CH Methodology

The analysis of the results encompassed three distinct aspects. In the subsequent sections, we provide an overview of the survey demographics and present a selection of results, accompanied by comprehensive discussions pertaining to the following dimensions [4]:

1. Dimension 1: Health Care Organization (HCO2)
2. Dimension 2: Employee Group (Medical and Clinical)
3. Dimension 3: Risk Category (Cybersecurity Awareness)

Each dimension was scrutinized individually to gain valuable insights into the responses and to foster a better understanding of the survey data.

11.2.2 Dimension 1—Health Care Organization

We are showcasing the baseline of implementing the risk-based approach in our CH methodology In the following figure, specifically for the risk categories associated with all employee groups at HCO2.

On the x-axis of Figure 5, we represent the various risk categories, while the y-axis denotes the risk evaluations categorized as low [1], low-medium [2], medium [3], medium-high [4], and high [5]. These risk evaluations help identify specific risk strategies and associated controls to effectively address the underlying risks[4].

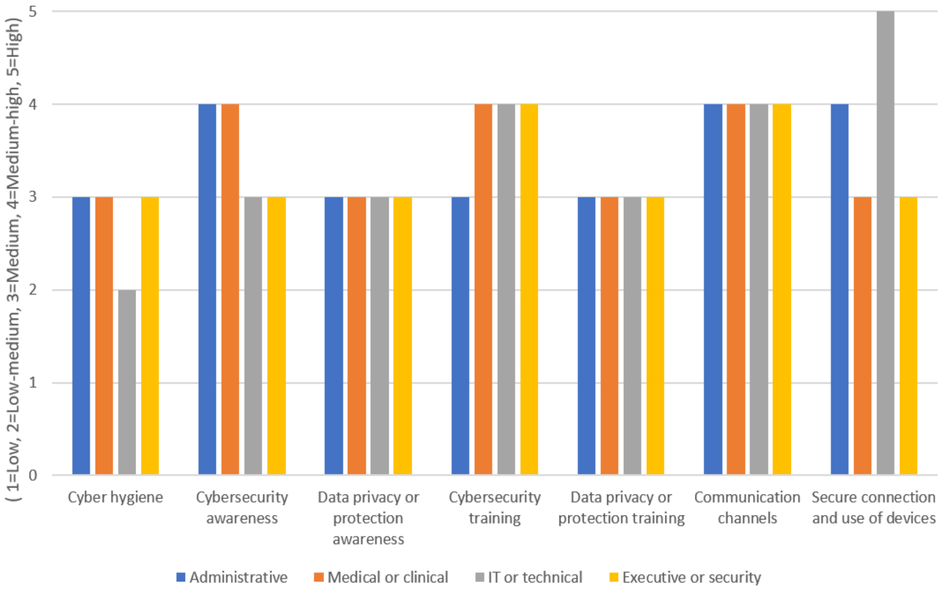


Figure 6: Findings for all employee groups at health care organization 2 [4].

For all employees depicted in Figure 5, the risks predominantly fell within the medium and medium-high categories, indicating the applicability of risk strategies like Monitoring and Reduction, respectively. Notably, the IT and technical group displayed high awareness concerning CH, with the risk level for this category being assessed as medium-low. However, this group exhibited heightened risk in the "Secure Connection and use of devices" category, necessitating the implementation of controls tailored to manage this risk in comparison to the other three employee groups [4].

11.2.3 Dimension 2—Employee Group

The survey findings pertaining to the medical and clinical employee group at HCO1, HCO2, and HCO3 are illustrated in the following figure. As in the previous graph, the x-axis indicates the risk categories specific to each employee group, while the y-axis represents the risk evaluation scores.

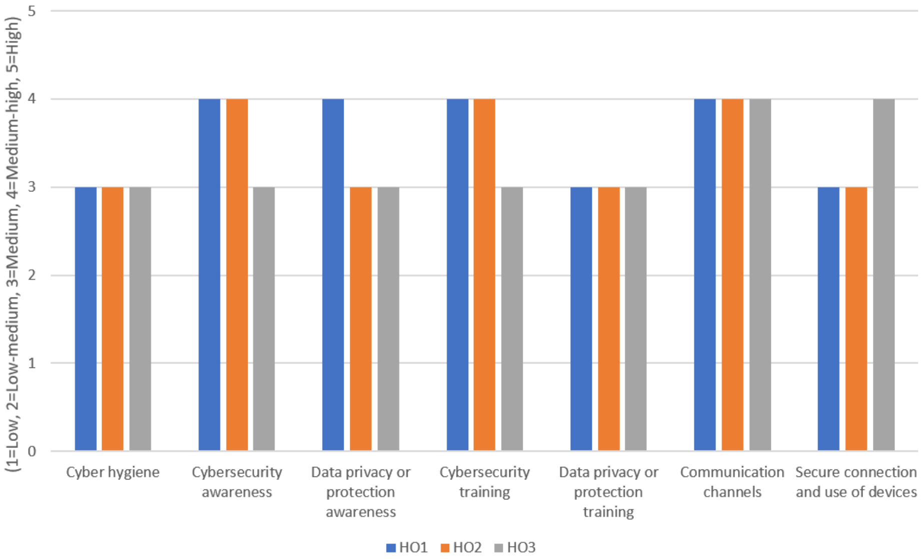


Figure 7: Findings for the medical and clinical employee group at the Secure and Private Health Data Exchange (CUREX) health care organizations. HCO1: health care organization 1; HCO2: health care organization 2; HCO3: health care organization 3 [4].

The findings for this employee group reveal interesting insights. The risk categories of "Cyber hygiene and Data Privacy and Protection Training" were assessed as medium, indicating the need for ongoing monitoring with mild controls. Conversely, the risk associated with the "Communication Channels" category reached a medium-high level across all three CUREX healthcare organizations. To manage this risk effectively, controls C3, C4, C5, and C17 are recommended, see table 6 below. These controls should be implemented on a quarterly or monthly basis, with content at an intermediate level to ensure employees can comprehend and internalize the awareness messages conveyed through communication channels [4].

Additionally, healthcare organizations might consider incorporating other channels that are preferred by employees and not currently in use for disseminating cybersecurity and data privacy messages. This proactive approach can enhance the overall effectiveness of the communication process and further mitigate potential risks [4].

Notably, employees at HCO3 demonstrated lower risks compared to those at HCO1 and HCO2, with most of their risks assessed at the medium level. This observation highlights the importance of understanding the unique risk profiles of different healthcare organizations and tailoring risk management strategies accordingly. By identifying and addressing these risk levels, healthcare organizations can reinforce their cybersecurity and data privacy measures and foster a safer digital environment for both employees and patients [4].

11.2.4 Dimension 3—Risk Category

The bar chart encompassing the findings for the "Cybersecurity Awareness" risk category, considering all employee groups across the three CUREX health care organizations.

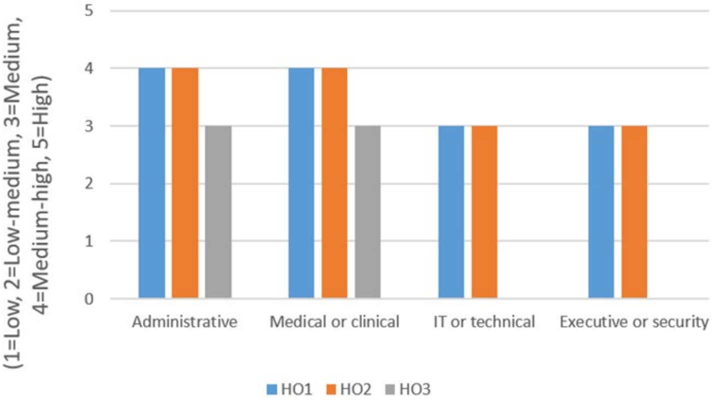


Figure 8: Findings for the cybersecurity awareness risk category at the Secure and Private Health Data Exchange (CUREX) health care organizations. HCO1: health care organization 1; HCO2: health care organization 2; HCO3: health care organization 3 [4].

The results indicate that the "Cybersecurity Awareness" risk category received relatively high evaluations across all employees in the CUREX health care organizations. Specifically, at HCO1 and HCO2, the risk was assessed as medium-high for administrative and medical and clinical personnel. Conversely, the remaining risk evaluations were classified as medium level [4].

Given the medium-high risks identified, the recommended risk strategy is "Reduction." This strategy entails implementing specific controls, including C3, C5, and C11, which should be applied on a monthly or quarterly basis. Furthermore, the awareness and training content for these controls should be set at an intermediate level. Additionally, controls C12 and C17 are recommended to motivate desirable cybersecurity behaviors among employees [4]. Addressing the "Cybersecurity Awareness" risk category with the prescribed controls and strategies is vital for promoting a heightened level of awareness and preparedness within the organization.

Number	Control title	Control description	Related resource
C1	Perform a skill gap analysis	Perform a skill gap analysis to understand the skills and behaviors that employees are not adhering to; using this information to build a baseline education road map	CISa subcontrol 17.1
C2	Deliver training to fill the skill gap	Deliver training to address the skill gap identified to positively affect employees' security behavior	CIS subcontrol 17.2
C3	Implement a cybersecurity awareness program	Create a cybersecurity awareness program for employees to ensure that they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization	CIS subcontrol 17.3
C4	Implement a data privacy awareness program	Create a data privacy awareness program for employees to ensure that they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization	CIS subcontrol 17.3
C5	Update awareness content frequently	Ensure that the organization's security awareness program is updated frequently to address new technologies, threats, standards, and business requirements	CIS subcontrol 17.4
C6	Train workforce on secure authentication	Train employees on the importance of enabling and using secure authentication	CIS subcontrol 17.5
C7	Train workforce on identifying social engineering attacks	Train employees on how to identify different forms of social engineering attacks such as phishing, phone scams, and impersonation calls	CIS subcontrol 17.6
C8	Conduct mock social engineering exercises	Conduct mock social engineering attacks (phishing, phone scams, and impersonation calls) to assess the readiness and response level of the employees	CIS subcontrol 17.6
C9	Train workforce on sensitive data handling	Train employees on how to identify and properly store, transfer, archive, and destroy sensitive information	CIS subcontrol 17.7

Number	**Control title**	**Control description**	**Related resource**
C10	Train workforce on causes of unintentional data exposure	Train employees to be aware of causes of unintentional data exposure, such as losing their mobile devices or a USB stick with sensitive data and emailing the wrong person	CIS subcontrol 17.8
C11	Train workforce members on identifying and reporting incidents	Train employees to be able to identify the most common indicators of an incident and report such an incident	CIS subcontrol 17.9
C12	Include cybersecurity in the meeting agendas	Set cybersecurity as a standing agenda item at meetings	CUREXb project
C13	Include data privacy in the meeting agendas	Set data privacy as a standing agenda item at meetings	CUREX project
C14	Introduce nudges to motivate cybersecurity behaviors	Introduce nudges as behavioral interventions to motivate and encourage employees to adopt desirable cybersecurity behaviors that they are already aware of	PANACEAc project
C15	Introduce nudges to motivate data privacy behaviors	Introduce nudges as behavioral interventions to motivate and encourage employees to adopt desirable data privacy behaviors that they are already aware of	PANACEA project
C16	Acknowledge employees who behave in a cybersecurity- and data privacy–responsible way	Acknowledge employees who demonstrate cybersecurity and data privacy behaviors (e.g., report scam emails and suspicious incidents to the IT department) and reward them (e.g., introduce awards such as "Cybersecurity Employee of the Year")	CUREX project
C17	Introduce a cybersecurity and data privacy champion role	Nominate an employee within each department or team in the organization who, given some specific skills and knowledge, will be responsible for promoting cybersecurity and data privacy best practices in daily work	CUREX project
C18	Celebrate cybersecurity awareness on specific occasions	Introduce a specific day, week, or month during the year for celebrating cybersecurity (e.g., the NCSAMd	CUREX project

Number	Control title	Control description	Related resource
		observed in the United States and the ECSMe, both celebrated in October)	
C19	Celebrate data privacy and protection awareness on specific occasions	Introduce a specific day, week, or month during the year for celebrating data privacy and protection (e.g., the Data Privacy Day in the United States and the European Data Protection Day, both observed every January 28)	CUREX project

Table 9: Candidate human-centric controls [4]

12 Discussion

This thesis aims to present the importance of exploring the influence of human factors in cybersecurity and privacy within healthcare organizations and how this information can offer valuable insights to strategic-level decision-makers and policy makers. While organizations have invested heavily in technological defenses, the human factor often remains an overlooked and critical vulnerability [1] The exploration of human factors in cybersecurity and privacy within healthcare organizations is imperative for building a robust defense against evolving cyber threats. By recognizing the significance of human behavior, decision-makers can craft targeted interventions to improve cybersecurity awareness, mitigate insider threats, and create a security-conscious culture. Ultimately, this knowledge will empower the cybersecurity policy making bodies to formulate comprehensive policies that protect patient data, enhance healthcare resilience, and ensure the continued advancement of secure and patient-centric digital healthcare ecosystems across Europe.

12.1 The Significance of Human Factors in Healthcare Cybersecurity

Human error and behavior play a pivotal role in determining the overall security posture of healthcare organizations [1]. From inadvertent data breaches due to improper handling of sensitive information to targeted social engineering attacks, human actions can expose critical vulnerabilities that adversaries exploit. Employees' cybersecurity awareness, education, and adherence to best practices are essential for safeguarding patient data and protecting against cyber threats [1]. Therefore, understanding the human factors affecting cybersecurity is paramount to fortifying healthcare systems against attacks**.** One of the most common and impactful aspects of human factors in cybersecurity is based on human error [1][8][9][11].

Advocacy for Human-Centric Controls: The Cyber Hygiene methodology's emphasis presented in this thesis on human-centric controls highlights a paradigm shift in the domain. Recognizing that the employees – from the front desk to the board room – are the first line of defense, these controls serve a dual purpose. On one hand, they address the prevalent gaps in knowledge and behavior; on the other, they endeavor to instill a pervasive culture of security consciousness. Such an approach not only bolsters the organization's defenses but potentially reduces the magnitude and frequency of human-induced cybersecurity lapses. Employees, whether intentionally or unintentionally, can make mistakes that compromise security for Instance by clicking on phishing emails, mishandling sensitive data, using weak passwords, or falling victim to social engineering attacks. Identifying the root causes of these errors can lead to targeted training and awareness programs to mitigate their occurrence. Human factors also play a significant role in the design and implementation of healthcare systems and technologies. Systems that are intuitive, user-friendly, and minimize the potential for errors contribute to enhanced cybersecurity [2]. Conversely, overly complex systems or cumbersome security measures may lead to user frustration and circumvention of security protocols [2]. Investing in cybersecurity training and awareness programs for employees is a critical component of human factor consideration [3]. Educating staff about the latest cybersecurity threats, best practices for data handling, and incident reporting empowers them to become the first line of defense against cyber threats [3].

The emphasis on human-centric controls in the Cyber Hygiene methodology, as presented in this thesis, highlights the importance of implementing such methodologies. While this approach recognizes the significant role of employees, as the primary line of defence, there are inherent challenges to consider. An overemphasis on human behaviour might underestimate the critical role of automated, technical solutions. We must remember that even the most trained and conscious employee can make mistakes or overlook threats. Furthermore, implementing such a methodological approach, might face resistance from staff members, especially those accustomed to established routines or who might not immediately see the benefits of changing their behaviors. While the methodology aims for consistency in practices across the organization, achieving this uniformity can be challenging, given the diverse roles and responsibilities of different employee groups. A strategy that works for one segment might not necessarily resonate with another. The evolving nature of cyber threats also poses a challenge. Human-centric controls, despite aiming to address current knowledge and behaviour gaps, will need continuous updates to remain relevant. This continuous training and adaptation can be resource-intensive and may demand significant time and effort. Moreover, quantifying the effectiveness of human-centric controls presents its own set of problems. The abstract nature of concepts like a "culture of security consciousness" makes them hard to measure and define in concrete terms. Furthermore, there's a potential risk of organizational complacency. Emphasizing employees as the first line of defence might inadvertently lead to underinvestment in other vital cybersecurity infrastructures.

12.2 Identifying Weaknesses and Enhancing Resilience-Comparison with other studies

By exploring why and how the human factors affecting healthcare cybersecurity, organizations and policy makers can identify specific weaknesses in the human-technology interface. This knowledge allows for targeted training programs to improve employees' cybersecurity awareness and behavior. Moreover, understanding the psychological and sociotechnical aspects of cybersecurity can lead to the development of more intuitive and user-friendly security measures, reducing the likelihood of errors and encouraging compliance. Other studies [12][13][14] have used comprehensive vulnerability assessments, penetration testing, and risk analyses as methodological approaches to identify potential entry points for cyber threats and vulnerabilities in the security infrastructure. Our hypothesis is that by understanding the specific human factors that contribute to these weaknesses, such as employee awareness gaps or inadequate training, organizations can tailor targeted interventions to address these shortcomings. Moreover, developing a proactive incident response plan, which incorporates human-centered decision-making processes and emphasizes continuous improvement, could strengthen the organization's resilience to potential cyber incidents. By integrating these strategies, healthcare organizations can bolster their cybersecurity and privacy defenses, reduce the likelihood of successful cyberattacks, and maintain the trust of patients and stakeholders in safeguarding sensitive healthcare data.

Differences	**This Thesis**	**Other Studies**
Geographical Scope	Focuses on the European context	May focus on other regions, leading to different insights and policy recommendations
Specific Emphasis on Policy Recommendations	Strong emphasis on strategic-level decision-making	Might have more technical, organizational, or educational focuses
Healthcare Focus	Specific to the healthcare sector	May be conducted in other sectors where human factors in cybersecurity have been examined

Table 10: Thesis focus and comparison with other research on human factors in cybersecurity: Differences and Gaps

Research concerning human factors in cybersecurity has extended beyond healthcare to encompass other critical information infrastructure domains such as energy, transportation, and telecommunication [15][16][17]. These sectors are integral to the functioning of modern society and are equally vulnerable to cyber threats. Studies within these areas often focus on the intersection between technology and human behavior, examining how individual and organizational practices contribute to security risks. For example, research in the energy sector [16] aimed to explore how human error can impact the security of power grids, while studies [15] in finance and energy aimed to analyze insider threats stemming from a lack of cybersecurity awareness. The emphasis on human factors in these studies underscores a growing recognition that technology alone cannot provide a robust defense against cyber threats. Although the methods and findings may vary across these diverse domains, a common thread is the acknowledgment that human behavior, culture, and decision-making are pivotal in shaping cybersecurity resilience. Insights gleaned from these various fields contribute to a more nuanced understanding of how to mitigate human-related vulnerabilities, emphasizing the importance of education, training, and a security-conscious organizational culture. The specificity of the healthcare sector in this thesis, with its unique regulatory, ethical, and patient-centered concerns, distinguishes it from these other critical domains, yet it shares with them the foundational principle that human factors are vital in cybersecurity defense.

There's a compelling narrative that intertwines human behaviour with technological facets. When we talk about the frailties of the human-technology interface, it's not difficult to envision scenarios where a healthcare staff member reuses simple password across platforms, simply for the sake of convenience and recall. Or, we can consider another commonplace scenario where, despite rigorous awareness campaigns, an unsuspecting employee becomes ensnared by a phishing attempt because the malicious email was convincingly disguised as an authentic internal communication. To fortify against such vulnerabilities, interactive workshops have emerged as more effective compared to traditional methods like distributing manuals or online courses [28][31]. These workshops, sometimes enhanced by controlled phishing attacks on employees, not only test their vigilance but also offer real-time feedback, ensuring lessons are both learned and retained. Yet, focusing purely on training might not capture the full spectrum of challenges. Healthcare security can sometimes induce cognitive overload among healthcare professionals, leading to unintentional lapses. This underscores the necessity for security measures that are as intuitive as they are robust. Sometimes, healthcare workers get overwhelmed with too much information, which can lead to mistakes. This means we need easy-to-use security tools. For example, instead of hard-to-remember passwords, we could use fingerprint logins. Also, if security steps are seen as too complicated or unnecessary, people might not follow them carefully. So, it's important to make security as important as patient care in the workplace culture. While comprehensive vulnerability assessments from various studies[1] have explored technical vulnerabilities, it's essential to blend this knowledge with insights from human factors. Every system, no matter how technically secure, can be rendered vulnerable by an uninformed or careless act from an individual. This accentuates the criticality of understanding and addressing awareness gaps and ensuring that training is tailored to the diverse technical proficiencies within an organization.

Anticipating future challenges, this thesis highlights the importance for healthcare institutions to have a proactive incident response strategy in place. Such a strategy should be underpinned by a comprehensive understanding of personnel roles and responsibilities within the system. A robust plan serves not only as a mechanism for swift problem resolution but also as an indicator of the institution's commitment to continuous improvement. By adopting this holistic approach, healthcare entities can enhance the resilience of their information systems, thereby reinforcing their dedication to the safeguarding of confidential health data to patients and stakeholders.

13 Studies' limitations

In this section we summarize the limitations of **Study I** and **Study II.**

13.1 Limitations Of Study I

The review process implemented employs a subjective ranking system to gauge the relevance of different pieces of literature to our research questions. This method, being subjective, might lead to certain biases, both in terms of which sources are selected for consideration and how our contents are interpreted. These biases could tilt the results or conclusions of the review in a particular direction that may not be completely objective.

Moreover, the field of study has a noticeable gap when it comes to literature that specifically investigates the human factors of cybersecurity within the healthcare sector. This scarcity means that to provide a comprehensive review, we were compelled to expand our search to encompass more general topics in cybersecurity. This broader focus might mean that some of the information included might not be precisely tailored to the unique cybersecurity challenges within healthcare but draws from cybersecurity practices and concerns in other domains.

Limitations	**Description**
Subjective Ranking	The review incorporates a subjective ranking by the authors concerning the relevance of literature to the specific research questions. This may introduce **biases in the selection and interpretation of sources.**
Limited Focus on Healthcare	Literature specifically addressing human factors of cybersecurity in healthcare is **limited**. As a result, the review had to encompass **broader, well-established topics in cybersecurity.**

Table 11: Limitations and Scope of the Literature Review on Human Factors in Cybersecurity within Healthcare

13.2 Limitations Of Study II

A significant limitation of Study II is that it was conducted across only **three health care organizations.** Consequently, the development of the controls was **constrained**, based solely on the limited feedback gathered from the study participants. The controls' performance could be validated in a future study. This narrow scope may impact the **generalizability of the findings**. In addition, the study period coincided with the COVID-19 pandemic, which further restricted the responses obtained, resulting in an even more limited number. These factors must be considered when interpreting the results.

14 Conclusions

The exploration of cybersecurity awareness among healthcare staff within healthcare and healthcare research organizations, as presented in this thesis, stands as a comprehensive inquiry into a critical contemporary concern. By employing a systematic review and novel survey approach, our research has unearthed significant insights into human behavior and its intricate relationship with cyber defense strategies in the healthcare sector. Study I revealed a complex web of behaviors, attitudes, and awareness levels that influence the overall cybersecurity posture of healthcare organizations. This systematic review served to consolidate and synthesize the current body of knowledge, allowing us to understand the challenges and opportunities that healthcare organizations face in defending against cyber threats. Study II took a pioneering step in developing a unique cyber hygiene concept tailored to the healthcare sector. By delving deeply into the specific knowledge, attitudes, and practices of healthcare staff, the research has identified key areas of strength and vulnerability. These insights are not only instrumental in promoting better cybersecurity protocols but also in crafting targeted training and interventions that resonate with the healthcare professionals' unique context and needs. By fostering a cybersecurity-aware culture, healthcare organizations can address existing security gaps and erect more robust defenses against the ever-evolving landscape of cyber threats. Such an approach is paramount in safeguarding sensitive patient data and crucial healthcare information, thereby reinforcing the resilience of healthcare systems at large.

However, it is essential to acknowledge the limitations of this research. Future work might consider a more diverse and broader participant pool, explore the impact of specific interventions based on the cyber hygiene concept, or assess the long-term effects of awareness campaigns and training.

In conclusion, by weaving together a rich tapestry of insights and recommendations, this thesis offers a strategic roadmap towards a more secure, resilient, and informed healthcare sector. The continuous battle against cyber threats demands a vigilant and adaptive approach, and this research lays down significant markers to guide and support ongoing efforts to fortify healthcare's digital frontiers.

15 Points of perspective

Future research can explore more deeply the human-centric approaches to cybersecurity and privacy within healthcare organizations. This includes studying the effectiveness of various training programs, awareness campaigns, and behavioral interventions in mitigating human vulnerabilities and promoting a security-conscious culture. Investigating innovative techniques such as gamification, immersive training, or social engineering simulations can provide valuable insights into enhancing human resilience against cyber threats [18]. Examining the interplay between human factors and technology within the context of healthcare organizations is another promising area [19]. Research can focus on understanding how the design of user interfaces, access controls, and workflow processes can influence employee behavior and cybersecurity outcomes [20]. Exploring socio-technical systems perspectives can contribute to the development of user-friendly, secure technologies that align with the unique requirements of healthcare environments [21]. Moreover, further research can explore further the development of advanced threat intelligence and incident response strategies tailored to healthcare organizations [22]. This includes studying proactive threat detection, automated incident response mechanisms, and effective collaboration between IT security teams and healthcare professionals. Investigating the use of artificial intelligence, machine learning, and data analytics can help identify patterns and anomalies, enabling timely responses to emerging cyber threats [23]. From the policy perspective, future policy efforts can focus on refining and adapting regulatory frameworks to address the evolving landscape of cybersecurity and privacy within healthcare organizations. This involves considering the specific challenges faced by healthcare organizations, harmonizing regulations across jurisdictions [24], and promoting international cooperation to combat cross-border cyber threats. Balancing regulatory compliance requirements with practical implementation considerations can help foster a secure and privacy-respecting healthcare ecosystem. Enhancing collaboration between public and private sectors could be beneficial for effective cybersecurity and privacy governance in healthcare. Future policies can encourage public-private partnerships that facilitate information sharing, threat intelligence exchange, and joint initiatives to address common challenges. By fostering these partnerships, authorities can leverage the expertise and resources of both sectors to develop comprehensive strategies, best practices, and guidelines that align with the rapidly evolving cybersecurity landscape. Encouraging the adoption of international standards and certifications specific to healthcare cybersecurity can be beneficial. Additionally, the rise of machine learning attacks poses a formidable threat, as cyber attackers leverage advanced algorithms to breach defenses and create sophisticated, evasive malware/ As technology evolves, privacy issues become more complex, with the growing prevalence of data collection, surveillance, and data-sharing practices raising concerns about personal information protection [21]. Ensuring a secure and private digital landscape demands a concerted effort to enhance cybersecurity awareness among individuals, implement robust defense mechanisms against machine learning attacks, and formulate stringent privacy regulations that safeguard user data from potential misuse or unauthorized access. It is crucial to state that the future challenges in cybersecurity and privacy are complex and multifaceted. Defending against machine learning attacks requires innovative ML-powered solutions, while countering social engineering demands heightened cybersecurity awareness and vigilance among individuals and employees. Addressing privacy issues entails a collaborative effort between governments, corporations, and technology providers to enact robust data protection measures that safeguard user information and uphold individual privacy rights. Proactive and holistic approaches are essential to navigate the evolving cyber threat landscape and preserve the security and privacy of users in the digital age.

16 References

[1] Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, Bonacina S. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors. 2021; 21(15):5119. https://doi.org/10.3390/s21155119

[2] Digital technologies: shaping the future of primary health care. World Health Organization. URL: https://www.who.int/docs/default-source/primary-health-care-conference/digital-technologies.pdf

[3] Wash R, Cooper MM. Who provides phishing training?: facts, stories, and people like me. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. 2018 Presented at: CHI '18: CHI Conference on Human Factors in Computing Systems; Apr 21 - 26, 2018; Montreal, QC, Canada

[4] Argyridou E, Nifakos S, Laoudias C, Panda S, Panaousis E, Chandramouli K, Navarro-Llobet D, Mora Zamorano J, Papachristou P, Bonacina S, Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study,J Med Internet Res 2023;25:e41294 URL: https://www.jmir.org/2023/1/e41294,DOI: 10.2196/41294

[5] Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res 2018 May 28;20[5]:e10059

[6] World Health Organisation (WHO) on Primary Health Care. Available online: https://www.who.int/docs/default-source/primary-health-care-conference/digital-technologies.pdf?sfvrsn=3efc47e0_2.

[7] Enrico Coiera, Putting the technical back into socio-technical systems research, International Journal of Medical Informatics, Volume 76, Supplement 1, 2007, Pages S98-S103, ISSN 1386-5056, https://doi.org/10.1016/j.ijmedinf.2006.05.026.

[8] Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Chalandri, Greece: ENISA; 2019.

[9] Kim, D.W.; Choi, J.Y.; Han, K.H. Risk management-based security evaluation model for telemedicine systems. BMC Med Inform. Decis. Mak. 2020, 20, 106.

[10] Malatji, M., Von Solms, S. and Marnewick, A. (2019), "Socio-technical systems cybersecurity framework", Information and Computer Security, Vol. 27 No. 2, pp. 233-272. https://doi.org/10.1108/ICS-03-2018-0031

[11] Montañez, R.; Golob, E.; Xu, S. Human Cognition Through the Lens of Social Engineering Cyberattacks. Front. Psychol. 2020, 11, 1755.

[12] He, W.; Zhang, Z.J. Enterprise cybersecurity training and awareness programs: Recommendations for success. J. Organ. Comput. Electron. Commer. 2019, 29, 249–257.

[13] Dameff, C.J.; Selzer, J.A.; Fisher, J.; Killeen, J.P.; Tully, J.L. Clinical Cybersecurity Training Through Novel High-Fidelity Simulations. J. Emerg. Med. 2019, 56, 233–238.

[14] Azad, M.A.; Bag, S.; Ahmad, F.; Hao, F.; Azad, M.A.; Bag, S.; Ahmad, F.; Hao, F. Sharing is Caring: A collaborative framework for sharing security alerts.

[15] López-Aguilar P, Batista E, Martínez-Ballesté A, Solanas A. Information Security and Privacy in Railway Transportation: A Systematic Review. Sensors. 2022; 22(20):7698. https://doi.org/10.3390/s22207698

[16] J. Liu, Y. Xiao, S. Li, W. Liang and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," in IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 981-997, Fourth Quarter 2012, doi: 10.1109/SURV.2011.122111.00145.

[17] Marianna Lezzi, Mariangela Lazoi, Angelo Corallo, Cybersecurity for Industry 4.0 in the current literature: A reference framework, Computers in Industry, Volume 103, 2018, Pages 97-110, ISSN 0166-3615, https://doi.org/10.1016/j.compind.2018.09.004. (https://www.sciencedirect.com/science/article/pii/S0166361518303658)

[18] Alshaikh, M.; Adamson, B. From awareness to influence: Toward a model for improving employees' security behaviour. Pers. Ubiquitous Comput. 2021.

[19] Back, S.; Guerette, R.T. Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. J. Contemp. Crim. Justice 2021.

[20] Canfield, C.I.; Fischhoff, B.; Davis, A. Quantifying Phishing Susceptibility for Detection and Behavior Decisions. Hum. Factors J. Hum. Factors Ergon. Soc. 2016, 58, 1158–1172.

[21] Dawson, J.; Thomson, R. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Front. Psychol. 2018, 9, 744.

[22] Ghafur, S.; Grass, E.; Jennings, N.R.; Darzi, A. The challenges of cybersecurity in health care: The UK National Health Service as a case study. The Lancet Digital Health 2019, 1, e10–e12.

[23] Sarker, I.H., Furhad, M.H. & Nowrozy, R. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN COMPUT. SCI. 2, 173 (2021). https://doi.org/10.1007/s42979-021-00557-0

[24] Hewitt, B.; Dolezel, D.; McLeod, A.J. Mobile Device Security: Perspectives of Future Healthcare Workers. Perspect. Health Inf. Manag. 2017, 14, 1c

[25] ISO/IEC 27000:2018—Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. Available online: https://www.iso.org/standard/73906.html (accessed on 16 July 2021).

[26] Abraham, C.; Chatterjee, D.; Sims, R.R.; Abraham, C.; Chatterjee, D.; Sims, R.R. Muddling through cybersecurity: Insights from the US healthcare industry. *Bus. Horizons* **2019**, *62*, 539–548

[27] Ghafur, S.; Grass, E.; Jennings, N.R.; Darzi, A. The challenges of cybersecurity in health care: The UK National Health Service as a case study. *The Lancet Digital Health* **2019**, *1*, e10–e12.

[28] Dawson, J.; Thomson, R. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Front. Psychol.* **2018**, *9*, 744.

[29] Azad, M.A.; Bag, S.; Ahmad, F.; Hao, F.; Azad, M.A.; Bag, S.; Ahmad, F.; Hao, F. Sharing is Caring: A collaborative framework for sharing security alerts. *Comput. Commun.* **2021**, *165*, 75–84.

[30] Eichelberg, M.; Kleber, K.; Kämmerer, M. Cybersecurity Challenges for PACS and Medical Imaging. *Acad. Radiol.* **2020**, *27*, 1126–1139

[31] DF, S.; Singh, H. A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Appl. Clin. Inform.* **2016**, *7*, 624–632.

[32] Spanakis, E.G.; Bonomi, S.; Sfakianakis, S.; Santucci, G.; Lenti, S.; Sorella, M.; Tanasache, F.D.; Palleschi, A.; Ciccotelli, C.; Sakkalis, V.; et al. Cyber-attacks and threats for healthcare—A multi-layer thread analysis. In Proceedings of the 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), Montreal, QC, Canada, 20–24 July 2020; Volume 2020, pp. 5705–5708.

[33] Rainer, R.K.; Snyder, C.A.; Carr, H.H. Risk Analysis for Information Technology. *J. Manag. Inf. Syst.* **1991**, *8*, 129–147.

[34] Coronado, A.J.; Wong, T.L. Healthcare cybersecurity risk management: Keys to an effective plan. *Biomed. Instrum. Technol.* **2014**, *48*, 26–30

[35] Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E.; Kessler, S.R.; Pindek, S.; Kleinman, G.; Andel, S.A.; Spector, P.E. Information security climate and the assessment of information security risk among healthcare employees. *Health Inform. J.* **2020**, *26*, 461–473.

[36] Zafar, H. Cybersecurity: Role of Behavioral Training in Healthcare. In Proceedings of the AMCIS 2016 Proceedings, San Diego, CA, USA, 11–14 August 2016.

[37] Jalali, M.S.; Bruckes, M.; Westmattelmann, D.; Schewe, G. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *J. Med. Internet Res.* **2020**, *22*, e16775.

[38] Priestman, W.; Anstis, T.; Sebire, I.G.; Sridharan, S.; Sebire, N.J. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health Care Inf.* **2019**, *26*, e100031.

[39] Montañez, R.; Golob, E.; Xu, S. Human Cognition Through the Lens of Social Engineering Cyberattacks. *Front. Psychol.* **2020**, *11*, 1755.

[40] Baillon, A.; de Bruin, J.; Emirmahmutoglu, A.; van de Veer, E.; van Dijk, B. Informing, simulating experience, or both: A field experiment on phishing risks. *PLoS ONE* **2019**, *14*, e0224216.

[41] Alami, H.; Gagnon, M.P.; Ahmed, M.A.A.; Fortin, J.P.; Alami, H.; Gagnon, M.P.; Ahmed, M.A.A.; Fortin, J.P. Digital health: Cybersecurity is a value creation lever, not only a source of expenditure. *Health Policy Technol.* **2019**, *8*, 319–321.

[42] Johansson, D.; Jonsson, P.; Ivarsson, B.; Christiansson, M.; Johansson, D.; Jonsson, P.; Ivarsson, B.; Christiansson, M. Information Technology and Medical Technology Personnel's Perception Regarding Segmentation of Medical Devices: A Focus Group Study. *Healthcare* **2020**, *8*, 23.

[43] Schmidt, T.; Nøhr, C.; Koppel, R. A Simple Assessment of Information Security Awareness in Hospital Staff Across Five Danish Regions. *Stud. Health Technol. Inform.* **2021**, *281*, 635–639.

[44] Švábenský, V.; Čeleda, P.; Vykopal, J.; Brišáková, S. Cybersecurity knowledge and skills taught in capture the flag challenges. *Comput. Secur.* **2021**, *102*, 102154

[45] Li, L.; He, W.; Xu, L.; Ash, I.; Anwar, M.; Yuan, X. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *Int. J. Inf. Manag.* **2019**, *45*, 13–24.

[46] He, W.; Zhang, Z.J. Enterprise cybersecurity training and awareness programs: Recommendations for success. *J. Organ. Comput. Electron. Commer.* **2019**, *29*, 249–257.

[47] Maggio, L.A.; Dameff, C.; Kanter, S.L.; Woods, B.; Tully, J. Cybersecurity Challenges and the Academic Health Center: An Interactive Tabletop Simulation for Executives. *Acad. Med.* **2021**, *96*, 850–853.

[48] Tan, Z.; Beuran, R.; Hasegawa, S.; Jiang, W.; Zhao, M.; Tan, Y. Adaptive security awareness training using linked open data datasets. *Educ. Inf. Technol.* **2020**, *25*, 5235–5259.

[49] 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 2021;372:n71. doi: 10.1136/bmj.n71

[50] Pascarella G, Rossi M, Montella E, Capasso A, De Feo G, Botti G, Nardone A, Montuori P, Triassi M, D'Auria S, Morabito A. Risk Analysis in Healthcare Organizations: Methodological Framework and Critical Variables. Risk Manag Healthc Policy. 2021 Jul 8;14:2897-2911. doi: 10.2147/RMHP.S309098. PMID: 34267567; PMCID: PMC8275831.