ISCTE IUL
REPOSITÓRIO
INSTITUTO UNIVERSITÁRIO DE LISBOA

Repositório ISCTE-IUL

Deposited in *Repositório ISCTE-IUL*:
2025-06-03

Deposited version:
Accepted Version

Peer-review status of attached file:
Peer-reviewed

Citation for published item:
Rajamäki, J., Rathod, P., Ferreira, J., Ahonen, O., Serrão, C. & Gomes, M. C. (2024). Enhancing cybersecurity education for the healthcare sector: Fostering interdisciplinary ManagiDiTH approach. In 2024 IEEE Global Engineering Education Conference, EDUCON. Kos Island, Greece: IEEE.

Further information on publisher's website:
10.1109/EDUCON60312.2024.10578769

Publisher's copyright statement:
This is the peer reviewed version of the following article: Rajamäki, J., Rathod, P., Ferreira, J., Ahonen, O., Serrão, C. & Gomes, M. C. (2024). Enhancing cybersecurity education for the healthcare sector: Fostering interdisciplinary ManagiDiTH approach. In 2024 IEEE Global Engineering Education Conference, EDUCON. Kos Island, Greece: IEEE., which has been published in final form at https://dx.doi.org/10.1109/EDUCON60312.2024.10578769. This article may be used for non-commercial purposes in accordance with the Publisher's Terms and Conditions for self-archiving.

Use policy

Creative Commons CC BY 4.0
The full-text may be used and/or reproduced, and given to third parties in any format or medium, without prior permission or charge, for personal research or study, educational, or not-for-profit purposes provided that:

- a full bibliographic reference is made to the original source
- a link is made to the metadata record in the Repository
- the full-text is not changed in any way

The full-text must not be sold in any format or medium without the formal permission of the copyright holders.

Serviços de Informação e Documentação, Instituto Universitário de Lisboa (ISCTE-IUL)
Av. das Forças Armadas, Edifício II, 1649-026 Lisboa Portugal
Phone: +(351) 217 903 024 | e-mail: administrador.repositorio@iscte-iul.pt
https://repositorio.iscte-iul.pt

Enhancing Cybersecurity Education for the Healthcare Sector: Fostering Interdisciplinary ManagiDiTH Approach

Jyri Rajamäki
Cybersecurity Thematic RDI
Laurea University of Applied Sciences
Espoo, Finland
jyri.rajamaki@laurea,fi

Paresh Rathod
Cybersecurity Thematic RDI
Laurea University of Applied Sciences
Espoo, Finland
paresh.rathod@laurea,fi

Joao C Ferreira
ISCTE-IUL
Instituto Universitário de Lisboa
Lisboa, Portugal
jcafa@iscte.pt

Outi Ahonen
Digital Department
Laurea University of Applied Sciences
Espoo, Finland
outi.ahonen@laurea.fi

Carlos Serrão
ISCTE-IUL
Instituto Universitário de Lisboa
Lisboa, Portugal
carlos.serrao@iscte-iul.pt

Maria do Carmo Gomes
ISCTE-IUL
Instituto Universitário de Lisboa
Lisboa, Portugal
carmo.gomes@iscte-iul.pt

***Abstract*— The healthcare sector faces growing and evolving cybersecurity threats and pressing need to enhance its cybersecurity education programmes. Many research study confirms the growing gap of cybersecurity and digitalisation know-how for the healthcare professionals. Robust cybersecurity education is crucial to equipping healthcare professionals with the knowledge and skills necessary to safeguard sensitive patient information and maintain the integrity of healthcare systems. This paper presents a master's programme titled "Managing Digital Transformation in the Health Sector" (ManagiDiTH) jointly implemented by universities in four different countries. The innovative master's programme includes 3 focus areas- health sector skills, societal skills and digital skills. The ManagiDiTH programme integrates cybersecurity education into a broader framework of digital transformation skills for health professionals with interconnectedness of cybersecurity and healthcare innovation. The programme emphasises practical learning through hands-on exercises and case studies, allowing students to apply cybersecurity principles to real-world healthcare scenarios. It also fosters collaboration among students from diverse backgrounds, encouraging the exchange of knowledge and the development of a comprehensive understanding of cybersecurity threats and mitigation strategies. The ManagiDiTH framework addresses the very specific cybersecurity challenges faced by the healthcare sector, including data breaches, ransomware attacks, and the increasing use of technology in patient care. It equips healthcare students including nurses with the necessary skills to identify and respond to these threats, as well as to conduct risk assessments and implement cybersecurity best practices. The paper presents the novel education programme that combines cybersecure digitalisation aspects of critical field of the healthcare.**

Keywords— cybersecurity for healthcare sector, cybersecurity education, healthcare professionals, societal skills, digital skills, cybersecure digitalisation

I. INTRODUCTION

The healthcare sector is increasingly reliant on digital technologies, making it a prime target for cyber-attacks. These attacks can have devastating consequences, including the theft of sensitive patient data, disruptions to healthcare services, and even loss of life. It is essential to develop comprehensive cybersecurity education programmes specifically tailored to the healthcare industry.

The healthcare sector is undergoing a digital transformation with the integration of electronic health records (EHRs), connected medical devices, and telehealth solutions. This shift exposes healthcare organisations to new and evolving cybersecurity threats, making it essential to enhance the education of professionals working in this sector.

The consequences of a cybersecurity breach in healthcare can be severe, ranging from the compromise of patient data to disruptions in medical services, that may even impact the patient life. Addressing these challenges requires a proactive approach, including robust cybersecurity education programmes tailored to healthcare professionals.

This article presents a comprehensive framework for cybersecurity education, which forms part of a master's programme called "Managing Digital Transformation in the Health Sector" (ManagiDiTH) collaboratively implemented by universities in four distinct EU nations. The innovative master's programme includes 3 main components- health sector skills, societal skills and digital skills. The ManagiDiTH programme emphasises the development of cybersecurity competencies tailored to the unique challenges faced by healthcare organisations with equipping professionals with the skills to work effectively in interdisciplinary teams to address cybersecurity challenges.

This paper is structured as follows. The next section provides the background of the current landscape of cybersecurity education in healthcare, initially discussing cybersecurity challenges in healthcare and gaps, followed by an overview of the ManagiDiTH master's degree, which forms the foundation for the paper. The fourth section details framework for cybersecurity education in ManagiDiTH programme. The fifth section delves into the core the paper, focusing on how cybersecurity in the healthcare and finally the conclusion of a paper. The paper brings the novel ManagiDiTH master's programme integrates cybersecurity education into a broader framework of digital transformation skills for health professionals with interconnectedness of cybersecurity and healthcare innovation. cybersecurity education through hands-on exercises and case studies, allowing students to apply cybersecurity principles to real-world healthcare scenarios.

II. Current Landscape of Cybersecurity Education in Healthcare

Cybersecurity has emerged as a critical concern for healthcare organisations across the EU, particularly those handling vast amounts of sensitive patient data. In recent years, there has been a growing recognition of the need to strengthen cybersecurity measures and education in healthcare [1]. This section presents the state-of-the-art on the current landscape of cybersecurity education in healthcare sector.

A. Cybersecurity Challenges in Healthcare

The healthcare sector faces several significant cybersecurity challenges that can have severe consequences for patient safety, data integrity, and overall operational efficiency [2]. Some current problems in cybersecurity at hospitals and within the health sector include:

1) Ransomware Attacks: Hospitals are prime targets for ransomware attacks, where cybercriminals encrypt critical medical data and demand payment for its release [2].

2) Data Breaches and Patient Privacy: The vast amount of sensitive patient information stored in electronic health records (EHRs) makes healthcare organisations attractive targets for data breaches [3]. Unauthorised access to patient data can result in identity theft, insurance fraud, or other privacy violations.

3) Medical Device Vulnerabilities: The increasing connectivity of medical devices to networks poses a cybersecurity risk [4]. Vulnerabilities in these devices could be exploited to manipulate patient data, disrupt device functionality, or even compromise patient safety [5].

4) Insider Threats: Employees, contractors, or other individuals with access to healthcare systems may pose a risk through intentional or unintentional actions [6]. Insider threats can involve data theft, misuse of access privileges, or unintentional exposure of sensitive information.

5) Supply Chain Vulnerabilities: Healthcare organisations rely on a complex supply chain of vendors and third-party services [7]. Weaknesses in the cybersecurity measures of these external entities can introduce vulnerabilities, allowing attackers to gain access to the hospital's network.

6) Legacy Systems and Outdated Software: Many healthcare systems still use legacy software and outdated operating systems that may no longer receive security updates [8]. These systems are more susceptible to exploitation as they lack the latest protections against evolving cyber threats.

7) Lack of Cybersecurity Awareness: Insufficient training and awareness among healthcare staff about cybersecurity best practices can contribute to security lapses [9]. Human error, such as falling victim to phishing attacks, remains a prevalent concern.

8) Interconnected Healthcare Ecosystem: The interconnected nature of the healthcare ecosystem, with various entities sharing patient data, creates numerous entry points for cyber threats [10]. Weak links in the chain, such as less-secure partners or affiliates, can be exploited to access sensitive information.

9) Regulatory Compliance Challenges: Compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) is crucial for healthcare organisations [11]. Ensuring compliance while staying ahead of evolving cybersecurity threats can be challenging.

10) Limited Resources for Cybersecurity: Many healthcare organisations face resource constraints, both in terms of budget and skilled cybersecurity personnel [12]. This limitation hampers the implementation of robust cybersecurity measures and timely responses to emerging threats.

B. Cybersecurity Incidents in Healthcare

In the relentless pursuit of advancing treatment and patient care through innovative technologies, the healthcare sector, responsible for delivering life-critical services, has become a prime target for cybercriminals seeking to exploit vulnerabilities associated with these transformative changes. Over the past five years, notable cyber-attacks, such as those on Anthem Blue Cross (affecting 78.8 million individuals), the American Medical Collection Agency Data breach (25 million patients affected), Premera Blue Cross (11 million affected), Excellus BlueCross Blue Shield (10 million affected), and the University of California, Los Angeles Health (4.5 million affected), underscore the magnitude of the cybersecurity threat [13]. Healthcare data is also quite valuable in the black market because it often contains a large amount of sensitive, personally identifiable information (PII), which may be stolen and misused with malicious intent [14]. The average value of a healthcare record is 250 USD in the black market [15].

Given this landscape, it is imperative for healthcare professionals to be well-versed in cyber-secure and cyber-resiliency practices, understanding the potential repercussions of cyber-attacks on the healthcare system.

C. Existing Gaps and Challenges

Analysing the current state of cybersecurity education in the healthcare sector reveals gaps in curriculum, awareness, and training programs. Common challenges include a lack of specialised courses, outdated content, and insufficient hands-on training opportunities.

According to the CyberSecPro Project's market demand analysis [16], the healthcare sector respondents identified Cybersecurity Principles (10%) as the most important area, followed by Cybersecurity Management (9%) and Cybersecurity Tools (7%). Ethical Hacking, Cybersecurity Education and Training, Communications and Network Security, and Cybersecurity Technologies were each mentioned by 4% of respondents. Ethical Hacking, Cybersecurity Education and Training, Communications and Network Security, and Cybersecurity Technologies were each mentioned by 4% of respondents. Other areas receiving between 3% and 4% of mentions included Embedded Systems, Emerging Digital Technologies, Risk Management, Incident Response, and Vulnerability Assessment [17].

III. The ManagiDiTH Master's Degree Programme

The need to adapt to rapid technological change and take advantage of the digitalisation of services has led to the development of the Managing Digital Transformation in the Health Sector (ManagiDiTH) master programme to facilitate the learning of specialised digital skills for the health sector. The Joint master's programme Managing the Digital Transformation in the Health Sector is designed to manage the digitalisation of health services, to promote the adoption of

data science and information system resources to innovate clinical approach, services and to reorganise processes. The master's programme will be based on a modular set of Curricular Units including a compulsory base as well as optional, flexible components giving the students the freedom to customise their educational journey and focus on two particular areas of specialisation.

ManagiDiTH Master includes 3 main components: Health sector skills, Societal skills and Digital skills. Among the Digital skills component, the students may choose between two possible branches: Data Science and Interoperability according to their interest and background profile.

The curriculum organisation comprises a total of 90 ECTS corresponding to three semesters of training. The diploma will be jointly issued by the four universities: ISCTE – University Institute of Lisbon, Laurea University of Applied Sciences, Aristotle University of Thessaloniki and Gustave Eiffel University. The scope of the degree is 90 credits of which the thesis forms 30 credits. The degree takes on average 1.5-2.5 years to complete. In line with the international ECTS standard, one credit corresponds with 26.7 hours of work for an average student. The degree level corresponds with level 7 of the European Qualifications Framework (EQF).

A. Curriculum Development

The curriculum is developed by using evaluation, monitoring, and feedback data. Feedback is received from students, personnel, and workplaces for the development of the curriculum. In addition, the curriculum is regularly assessed using predefined assessment criteria. The development of the curriculum also takes into consideration the changing needs of society. Changes may occur in the study units and implementation modes. Especially the offering of the complementary competence study units are constantly under development to match the requirements of the working life and thus the offering may change during the studies.

B. Competencies - Interdisciplinary approach

The need to adapt to rapid technological change and take advantage of digitalisation of services has led to the development of a master's programme to facilitate Interdisciplinary skills for the health sector. This degree program has been designed and delivered by a consortium consisting of four EU countries. The programme's goal is that the graduated students will be qualified to plan and support the digitalisation of health and social care services and to promote the implementation of new procedures and services, supported by ICT. ManagiDiTH will contribute to excellence and innovation in the health and social care sector in higher education.

The education is targeted towards individuals interested in the development of working life in the context of healthcare and social services. The student's background in working life can be from the private, public, or third sectors in the health and social care sector or any other field. The expertise from work or prior studies of potential students may vary from the health sector, management, ICT or other areas. The common factor among the participants in the education is an interest in the development and learning about health and social care services. Among the Digital skills component, the students may choose between two possible branches: Data Science and Interoperability according to their interest and background profile.

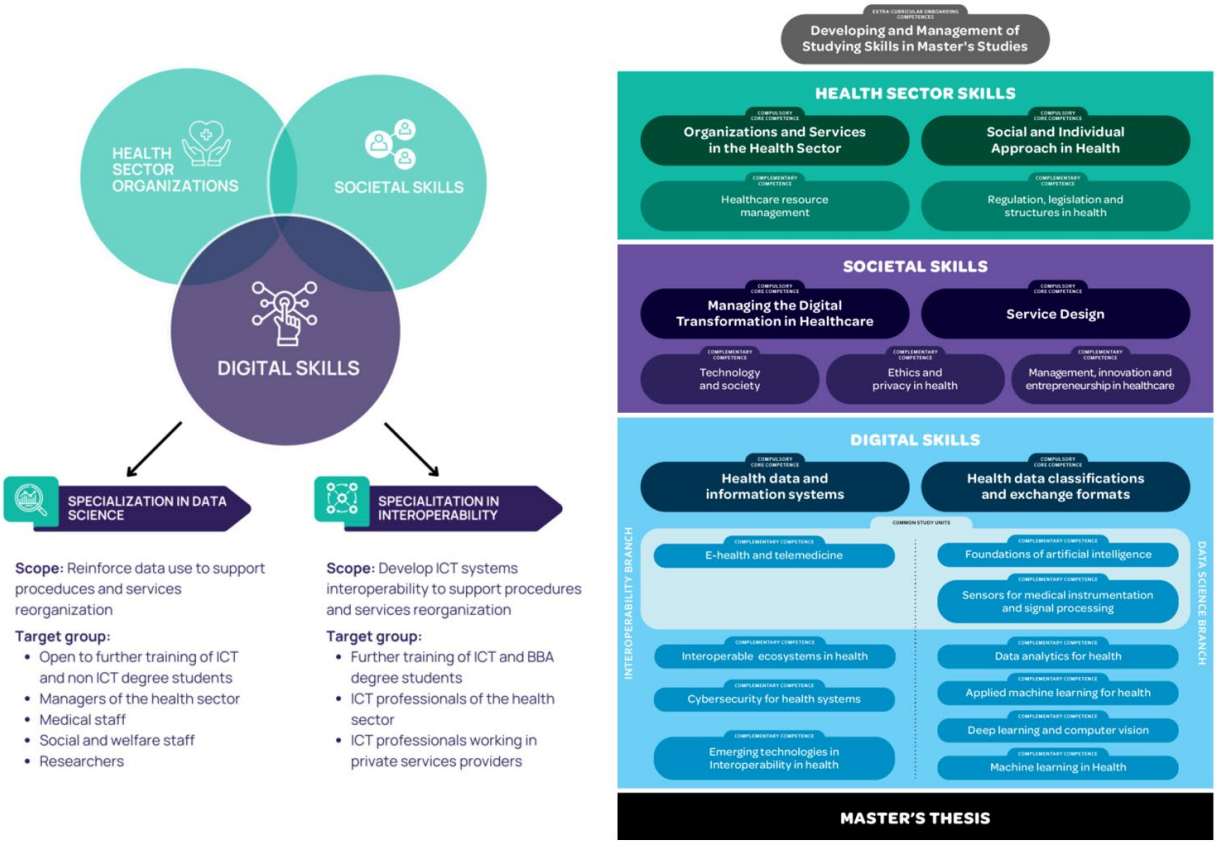


Fig. 1: Managing Digital Transformation in the Health Sector (ManagiDiTH): Programme Focus Areas and Curriculum

Figure 1 shows the ManagiDiTH focus areas and planned curriculum of the programme, which consists of three main competence areas: Health sector, societal and digital skills. It is composed of 10 study units of 6 ECTS each (10 Units * 6 ECTS = 60 ECTS) and the dissertation (30 ECTS). In total, the Master program accounts for 90 ECTS.

IV. Framework for Cybersecurity Education in ManagiDiTH Programme

A. Core Competencies

People's behaviour is known to be the weakest link in cybersecurity. On the other hand, human-centered cyber security is an area that is an intangible concept that is challenging to define and understand, not only by the lay end user but also by cyberspace experts [18]. Determining the knowledge and skills necessary for healthcare professionals to effectively mitigate cyber security risks includes understanding the regulatory environment, medical device security, and implementing incident response protocols. Grobler et al.[19] define human-centric cybersecurity, as encompassing all facets of cybersecurity while placing a specific emphasis on human involvement in systems and processes. They advocate for the development, execution, and evaluation of comprehensive human-centric cybersecurity systems, identifying three key components referred to as the 3U's: User, Usage, and Usability. Each of these components comprises additional subsections, as detailed in Table 1.

TABLE I. Design, implementation and assessment of holistic human-centric cyber security systems [19].

Component	Description
User	• Demography and Culture • Situational Awareness • Psychology and Behaviour • Cognitive Factors
Usage	• Functional Measures • Technical Measures • Legislation, Regulations and Policies
Usability	• Experience Factors • Interaction Factors

B. Specialised Courses

The ManagiDiTH curriculum integrates specialised learning units tailored to the healthcare sector. One of these study units is specially devoted to cybersecurity aspects. In addition, the curriculum also provides different perspective on cybersecurity issues as explained below:

1) ***Cybersecurity for Health Systems study unit:*** The study unit titled 'Cybersecurity for Health Systems' (6 ECTS) will allow students to be able to:

- Develop an understanding of the unique cybersecurity challenges in healthcare and the importance of protecting sensitive patient data
- Develop the knowledge and skills to assess and manage cybersecurity risks in health systems.
- Implement security measures to safeguard network infrastructure, applications, and medical devices.
- Ensure compliance with data privacy regulations and employ techniques to protect patient confidentiality.
- Develop effective incident response and disaster recovery plans to mitigate and recover from cybersecurity incidents.
- Identify how to stay updated on emerging trends and technologies in healthcare cybersecurity, while considering ethical considerations and sector best practices.

2) ***Other study units dealing with cybersecurity issues:*** *In the course curriculum, there are other study units that also approach cybersecurity aspects in their syllabus. The* following list offer an overview of the topics covered in each of them:

- Managing the Digital Transformation in Healthcare (6 ECTS): Develop strategies for effectively engaging patients in their healthcare through digital tools and platforms considering the ethical and privacy related to the use of digital technologies in healthcare.
- Health data and information systems (6 ECTS): (i) Identify the principles of health data collection, management, and analysis; (ii) Analyse the role of health information systems in healthcare delivery; (iii) Discover data standards, data sources, and data analytics tools used in healthcare; (iv) Develop an understanding of the ethical and legal considerations related to health data and information systems.
- Regulation, legislation and structures in health (6 ECTS): (i) Compare the differences in the national and EU-level regarding the structures of EU policy making and regulations in order to understand EU-Health and Wellbeing digitalisation regulatory framework; (ii) Examine the EU-Health and Wellbeing digitalisation regulatory framework´s from the perspectives of the public and private health and wellbeing services providers, third sector and health technology companies in order to get knowledge on how to make change together in digital transformation.
- Ethics and Privacy in Health (6 ECTS): Understand and apply regulatory frameworks for privacy and data protection in the health field, particularly the GDPR.
- E-Health and Telemedicine (6 ECTS): Critically evaluate privacy and security issues, as well as ethical dilemmas that arise in the use of digital technologies for healthcare.
- Interoperable ecosystems in health (6 ECTS): Design, develop, and implement interoperable healthcare systems, including system architecture, data exchange protocols, and security and privacy features.
- Emerging Technologies in Interoperability in Health (6 ECTS): Discover security and privacy considerations.

V. Cybersecurity for Health Systems

Cybersecurity threats to healthcare organisations and patient safety are real. Health information technology provides critical life-saving functions and consists of connected, networked systems that leverages wireless technologies, which in turn leave such systems more vulnerable to cyber-attacks. It is necessary to understand the cybersecurity threats that impact health systems and patients

and also learn which are the required cybersecurity measures to enable secure and resilient health systems.

On the design of this module a special focus was placed on the alignment of its content with international cybersecurity recommendations, namely the NIST Cybersecurity Framework [20] and European Cybersecurity Skills Framework (ECSF) [23], where a set of core cybersecurity activities are identified: IDENTIFY (ID), PROTECT (PR), DETECT (DE), RESPOND (RS) and RECOVER (RC).

The general objective of this module is to prepare students to identify the specific cybersecurity threats and risks health systems need to face (ID), learn about the appropriate mitigations that need to be implemented to protect them (PR), learn the techniques and mechanisms that can detect menaces (DE), identify how to handle the appropriate measures to face attacks to health systems (RS), and recover health systems to regular operation after attacks (RC).

This specific cybersecurity focused study units are composed by the following topics:

- Introduction to Cybersecurity in Healthcare (ID)
- Security Fundamentals for Health Systems (ID)
- Risk Assessment and Management in Health Systems (ID)
- Network Security in Health Systems (PR, DE)
- Application Security in Health Systems (PR, DE)
- Data Privacy and Confidentiality in Health Systems (ID, PR)
- Incident Response and Disaster Recovery in Health Systems (PR, DE, RS, RC)
- Threat Detection and Prevention in Health Systems (ID, PR, DE)
- Secure Cloud Computing in Health Systems (PR, DE)
- Medical Device Security (PR; DE)
- Security Governance and Compliance in Health Systems (ID)
- Emerging Trends and Future Directions in Healthcare Cybersecurity (PR, DE, RS, RC)

From the syllabus content, this module will provide a widespread overview of the most critical aspects of cybersecurity for healthcare professionals and managers, approaching topics addressing the technology, processes and people pillars of cybersecurity [24].

VI. Discussion

In today's interconnected and data-driven healthcare environment, cybersecurity is paramount to protecting sensitive patient information and ensuring the continuity of care. Especially, the cyber threats become increasingly sophisticated, therefore, it is crucial to provide comprehensive cybersecurity education to healthcare professionals and organisations. This paper proposes a comprehensive framework for cybersecurity education in healthcare that addresses the unique challenges and requirements of the sector. Further different aspect of the best practices explained in the following subsections.

A. Collaboration and Partnerships:

Cooperation between educational institutions, healthcare organisations, and experts in the field of cyber security enables the creation of a comprehensive approach to cyber security training. Creating partnerships can ensure that training programs remain relevant and in line with sector best practices. According to Kioskli et al.[18], a human-centric, co-produced approach enables:

(a) Education is tailored to the demographics and needs of the audience with regularly updated messages to avoid desensitisation of the audience.

(b) Automation, whereby users would not need to proactively undertake cyber practices, reducing their workload and resulting in increased engagement and adherence to regulations.

B. Best Practices for Cyber-hygiene

The baseline for cyber hygiene encompasses essential steps crucial for cyber security, primarily rooted in frameworks such as the European Cybersecurity Skills Framework (ECSF) [23] and NIST cybersecurity framework [18]. These frameworks offer organisations, including the healthcare supply chain, a comprehensive and transparent set of best practices to demonstrate and consistently adapt cybersecurity practices. While standardised best practices for healthcare may be lacking, the literature has presented a fundamental set of methods for maintaining cyber hygiene in business [21][22].

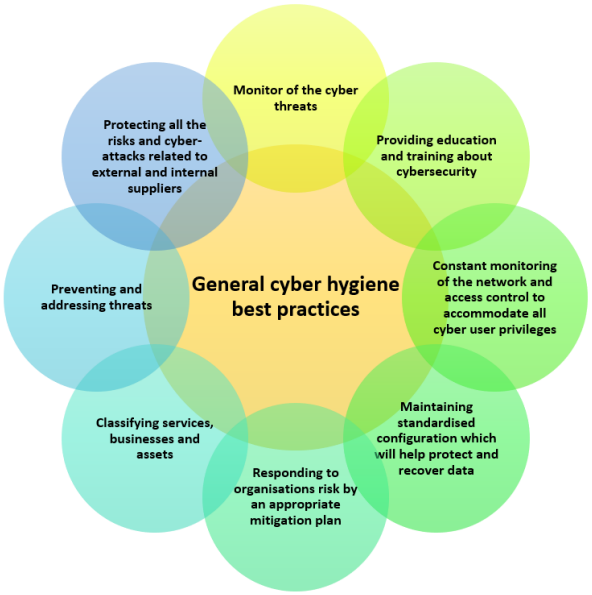


Fig. 2: General cyber hygiene best practices [18]

All organisations and cyber users must shoulder the responsibility for their browsing activities in both personal and professional realms. Individuals must proactively maintain adequate cyber hygiene and safeguard against cyberattacks by adhering to best practices [18]. Figure 2 illustrates these best practices gathered from the literature as recommended by Kioskli et al.[18].

C. Implementation Strategies

Provide guidance on implementing the proposed cybersecurity education framework within healthcare organisations and academic institutions. Discuss strategies for overcoming potential barriers, such as resource constraints and resistance to change, and emphasise the long-term benefits of investing in cybersecurity education.

D. Continuous Professional Development:

Recognise the dynamic nature of cybersecurity threats and the need for continuous professional development. Propose ongoing training programs, certifications, and resources to ensure that healthcare professionals stay updated on the latest cybersecurity trends and technologies.

E. Measuring the Effectiveness:

Establish metrics and key performance indicators (KPIs) to assess the effectiveness of cybersecurity education programs in the healthcare sector. Evaluate the impact on reducing security incidents, improving incident response times, and enhancing overall cybersecurity posture.

F. Future Directions and Emerging Trends:

Anticipate future challenges and emerging trends in healthcare cybersecurity. Discuss how the education framework can adapt to address evolving threats, technologies, and regulatory changes, ensuring its relevance in the years to come. The cybersecurity landscape in healthcare is constantly evolving, with new threats, technologies, and regulatory changes emerging regularly. The proposed education framework must adapt to these changes to remain relevant and effective in the years to come. This may involve incorporating emerging technologies such as artificial intelligence and machine learning into cybersecurity education programs [25].

G. Ethical Considerations:

Explore ethical considerations associated with cybersecurity education in healthcare, such as privacy concerns, responsible disclosure, and the ethical use of cybersecurity skills. Emphasise the importance of instilling ethical values in cybersecurity professionals to promote responsible and secure practices. Cybersecurity education in healthcare raises ethical considerations related to privacy concerns, responsible disclosure, and the ethical use of cybersecurity skills [26, 27]. It is essential to instil ethical values in cybersecurity professionals to promote responsible and secure practices.

VII. Conclusion

This paper emphasises the critical importance of developing specific cybersecurity education tailored to the healthcare sector. As the healthcare sector undergoes a digital transformation, integrating electronic health records, connected medical devices, and telehealth solutions, the associated increase in cybersecurity threats necessitates equipping professionals with the knowledge and skills to safeguard sensitive patient information and maintain healthcare system integrity. The discussion delves into the current landscape of cybersecurity education in healthcare, highlighting the existing gaps and challenges, including the prevalence of cybersecurity incidents and the identified needs of healthcare professionals. Notable cyber-attacks on healthcare organisations underscore the urgency for robust cybersecurity education programs.

The paper introduces the "ManagiDiTH" program, a master's program designed to address the Interdisciplinary skills required for the health sector's digital transformation. It involves a consortium of universities from four EU countries, offering a curriculum structured around the health sector, societal, and digital skills. The framework for cybersecurity education within the ManagiDiTH program is outlined, emphasizing core competencies and specialised courses. The incorporation of courses such as "Cybersecurity for Health Systems" is highlighted, addressing the unique challenges of healthcare cybersecurity. The discussion includes the importance of addressing human factors in cybersecurity, aligning with the 3U's framework (User, Usage, and Usability) proposed by Grobler et al.

In conclusion, the paper suggests collaborative efforts between educational institutions, healthcare organisations, and cybersecurity experts to tailor education to audience demographics and needs. Best practices for cyber hygiene are emphasised and rooted in established frameworks. Implementation strategies, continuous professional development, measuring effectiveness, case studies, and ethical considerations are also discussed, providing a comprehensive overview. The paper also advocates for a holistic and tailored approach to cybersecurity education in the healthcare sector, acknowledging the dynamic nature of cybersecurity threats and the need for ongoing adaptation to emerging trends. The proposed "ManagiDiTH" approach serves as a model for addressing the specific challenges and requirements of cybersecurity education in the evolving landscape of healthcare.

Acknowledgment

This research was conducted within the framework of two European Union (EU) research, development, and innovation (R&D&I) activities: Master of Managing Digital Transformation in the Health Sector Project and was supported by funding from the European Health and Digital Executive Agency (HADEA) EU executive agency, under the powers delegated by the European Commission. The project number is 101083896. And CyberSecPro project, funded by the European Union's Digital Europe Programme (DEP) under grant agreement No 101083594. The views and opinions expressed in this paper are the sole responsibility of the authors and do not necessarily reflect the official positions of the European Union or the European Commission

Special acknowledgements go to the project partners for their collaboration and partnership in the development work of the ManagiDiTH project.

References

[1] K. E. Aasmundtveit, C. Wang, M. Rencz, M. P. Y. Desmulliez, F. Ender and K. Imenes, "Joint international master in smart systems integration: University collaboration for improved education," 2018 IEEE Global Engineering Education Conference (EDUCON), Santa Cruz de Tenerife, Spain, 2018, pp. 624-629, doi: 10.1109/EDUCON.2018.8363288.

[2] R. N. Sindhwani, H. A. Abbasi, and A. M. Khan, "Cybersecurity in healthcare: A comprehensive survey of emerging trends, challenges, and solutions," IEEE Access, vol. 9, pp. 102213-102237, 2021. https://ieeexplore.ieee.org/document/9972597

[3] E. H. H. Chan, S. Y. S. Foo, and C. L. Tan, "Cybersecurity challenges in healthcare: A systematic review and thematic analysis," Journal of Medical Internet Research, vol. 23, no. 10, p. e26508, 2021. https://www.jmir.org/2021/4/e21747/

[4] Y. Wang, T. Yu, P. Zhou, W. Wang, and C. Wang, "Cybersecurity for medical devices: A survey," IEEE Access, vol. 6, pp. 47757-47778, 2018. https://ieeexplore.ieee.org/iel7/6287639/6514899/09119369.pdf

[5] A. A. Kaafarani, H. V. Poor, M. J. Mirsky, and S. H. Islam, "Vulnerability assessment and mitigation for medical devices in cybersecurity: A survey," IEEE Access, vol. 7, pp. 123343-123367, 2019. https://ieeexplore.ieee.org/document/8992922

[6] M. P. Brown, "Insider threat and data security in healthcare," Journal of Healthcare Management, vol. 61, no. 6, pp. 35-41, 2016. https://www.hhs.gov/sites/default/files/insider-threats-in-healthcare.pdf

[7] K. M. Goswami and N. N. Singh, "Supply chain security challenges and risk mitigation strategies in healthcare industry," Journal of Network and Computer Applications, vol. 156, p. 102644, 2020. https://pubmed.ncbi.nlm.nih.gov/36300412/

[8] R. N. Sindhwani, J. H. Kim, D.-H. Kim, and A. M. Khan, "Cybersecurity challenges in healthcare: A focus on legacy systems and outdated software," IEEE Access, vol. 8, pp. 156042-156053, 2020. http://ieeexplore.ieee.org/document/9020632/

[9] W. L. Miller, "Cybersecurity challenges in healthcare: A focus on human error and phishing attacks," JMIR mHealth and uHealth, vol. 9, no. 4, p. e17095, 2021. https://www.jmir.org/2021/4/e21747/

[10] S. A. Khan, M. Y. Lee, and S. Y. Chae, "Cybersecurity challenges in healthcare: A focus on interconnected healthcare ecosystem and its vulnerabilities," IEEE Access, vol. 8, pp. 155428-155442, 2020. http://ieeexplore.ieee.org/document/9020632/

[11] M. Allen and W. A. S. Smith, "Regulatory compliance challenges in cybersecurity: A focus on HIPAA," JMIR mHealth and uHealth, vol. 9, no. 3, p. e17080, 2021. https://thejournalofbusiness.org/index.php/site/article/view/714

[12] A. A. Kaafarani, N. A. Kaafarani, H. V. Poor, S. H. Islam, and H. A. Abbasi, "Limited resources for cybersecurity

[13] Stoianov, N., and Bozhilova, M. (2019). D2.1 Sector scenarios and use case analysis. ECHO.

[14] Imprivata. (2021, June 30). Hackers, breaches, and the value of healthcare data. [online] Available at: https://www.imprivata.com/blog/healthcare-data-new-prize-hackers

[15] Alder, S. (2023, November 2). Editorial: Why Do Criminals Target Medical Records. The HIPAA Journal. [online] Available at: https://www.hipaajournal.com/why-do-criminals-target-medical-records/ [Accessed 18 December 2023].

[16] Rathod, P., et al. (2023). D2.1 Cybersecurity Practical Skills Gaps in Europe: Market Demand and Analyse. CyberSecPro project.

[17] Rajamäki, J., Rathod, P., & Kioskli, K. (2023). Demand Analysis of the Cybersecurity Knowledge Areas and Skills for the Nurses: Preliminary Findings. Proceedings of the 22nd European Conference on Cyber Warfare and Security, 22(1), 711-716.

[18] Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Applied Sciences, 13(3410), 1-16.

[19] Grobler, M., Gaire, R., & Nepal, S. (2021). Usage and Usability: Redefining Human Centric Cyber Security. Front. Big Data, 4, 344–452.

[20] National Institute of Standards and Technology (NIST). (2018, April 16). Framework for Improving Critical Infrastructure Cybersecurity - version 1.1. [online] Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 18 December 2023].

[21] Trevors, M., & Wallen, C. (2017). Cyber Hygiene: A Baseline Set of Practices. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA.

[22] Ncubukezi, T., & Mwansa, L. (2021). Best practices used by businesses to maintain good cyber hygiene during COVID-19 pandemic. J. Internet Technol. Secur. Trans., 9, 714–721.

[23] European Cybersecurity Agency ENISA (2022), "European Cybersecurity Skills Framework (ECSF), https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework [Accessed 18 December 2023].

[24] Rathod, P., Kämppi, P. (2020). Applying LEAN Principles to Improve Introductory Cybersecurity Online Subject: Findings from the Pilot Study. In SITE 2020 10th International Conference on Society for Information Technology & Teacher Education. USA, Association for the Advancement of Computing in Education (AACE).

[25] Rathod, P., & Hämäläinen, T. (2020). Leveraging the benefits of big data with fast data for effective and efficient cybersecurity analytics systems: A robust optimisation approach. In International Conference on Cyber Warfare and Security (pp. 411-XVII). Academic Conferences International Limited.

[26] Aldewereld, H., & Pottinger, D. J. (2021). Ethical Considerations in Healthcare Data Sharing. Journal of Biomedical Research, 35(5), 702-711.

[27] Grobler, M., Gaire, R., & Nepal, S. (2021). Usage and Usability: Redefining Human Centric Cyber Security. Frontiers in Big Data, 4, 344–452.