Implementation of the ECHO Cyber-Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities

Eleonora Beltempo

2024 Laurea

Laurea University of Applied Sciences

Implementation of the ECHO Cyber-Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities

Eleonora Beltempo
Business Information Technology
Thesis
October 2024

Laurea University of Applied Sciences **Abstract**
Business Information Technology
Cybersecurity

Eleonora Beltempo

Implementation of the ECHO Cyber-Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities

Year 2024 Number of pages 40

The thesis discusses how the ECHO Cyber-Skills Framework (ECSF) is used inside the to boost cybersecurity capabilities. In a time when cyber threats are pervasive and becoming more sophisticated, especially in crucial areas like healthcare, developing cybersecurity skills is necessary. This thesis explores the potential of the ECSF to enhance cybersecurity education and training, paying particular attention to the unique requirements and difficulties encountered by the healthcare sector. The goal of this research is to provide a comprehensive framework for the effective implementation of ECSF in the CyberSecPro project by drawing on national policies, international collaboration, and the corpus of existing cybersecurity education literature.
In order to evaluate the efficiency of the ECSF and the present cybersecurity skills shortages, the study uses a mixed-methods approach, combining data from documents and qualitative data from interviews with important stakeholders.

The results show that the healthcare industry has a serious skills gap, with deficits most pronounced in incident response, threat analysis, and risk management. In order to close these gaps, the ECSF is a useful instrument that provides organized principles for creating training programmes that are specifically targeted. The research findings underscore the significance of customized training, ongoing professional growth, and an emphasis on transferable skills in the implementation plan.

The importance of this study lies in its attention to the urgent need for improved cybersecurity defenses in the healthcare sector, which is increasingly becoming a target of cyberattacks. The project intends to give healthcare practitioners a systematic method for enhancing their cybersecurity expertise by utilizing the ECSF. The results provide insightful information on how to better defend against cyberattacks and apply cybersecurity frameworks to legislators, educators, and business executives.

Keywords: ECHO Cyber-Skills Framework (ECSF), CyberSecPro Project, cybersecurity education, healthcare cybersecurity, cyber threats, cybersecurity capabilities, risk management, cybersecurity training, ECHO Project, European cybersecurity ecosystem.

Contents

1 Introduction

Cybersecurity has grown to be a serious worry for many companies in today's interconnected world, especially for those that handle sensitive data and offer necessary services. Because the healthcare sector relies heavily on digital technologies and handles sensitive patient data, it is particularly susceptible to cyber threats. Cybercrimes that compromise patient safety, disrupt services, and damage public confidence in healthcare institutions include ransomware attacks, data breaches, and other malevolent actions.

The European Union has acknowledged that its member states urgently need to strengthen cybersecurity. The European network of Cybersecurity centers and competency Hub for innovation and operations, or ECHO project, was financed by Horizon 2020 and seeks to create a strong cybersecurity ecosystem across the continent. The ECHO Cyber-Skills Framework (ECSF), which aims to close the cybersecurity skills gap and improve the competencies of professionals in a variety of industries, including healthcare, is a vital part of this programme.

Using the ECSF to enhance cybersecurity education and training is the goal of the CyberSecPro project. The application of the ECSF within the CyberSecPro project to improve cybersecurity capabilities in the healthcare industry is examined in this thesis. Through an analysis of the unique requirements and constraints faced by this industry, the study seeks to create a complete plan for the efficient implementation of the ECSF.

1.1 Research Objectives

The primary objective of this study is to explore how the ECHO Cyber-Skills Framework (ECSF) can enhance cybersecurity capabilities within the CyberSecPro project, with a particular focus on addressing challenges in the healthcare sector. As cybersecurity threats grow increasingly sophisticated and frequent, especially in critical sectors such as healthcare, there is a pressing need for effective frameworks that address these vulnerabilities through targeted skill development. By concentrating on the ECSF, this research aims to uncover a structured approach to enhancing cybersecurity education and training.

This study seeks to assess the current skills gaps in the healthcare sector, particularly in areas crucial for cybersecurity, such as incident response, threat analysis, and risk management. Identifying these gaps is essential to tailoring educational and training programs that align with the ECSF’s competency frameworks. Furthermore, the research evaluates the relevance and adaptability of the ECSF for use in healthcare organizations, given the unique challenges of securing sensitive health information and maintaining service continuity.

Ultimately, this research aims to offer practical recommendations for implementing the ECSF effectively within the CyberSecPro project. By doing so, the study provides valuable insights not only for the healthcare sector but also for other critical industries seeking to fortify their cybersecurity posture. The findings are intended to guide policymakers, educators, and industry leaders in adopting frameworks that enhance cybersecurity skills, foster continuous professional development, and ultimately improve resilience against cyber threats.

1.2 Structure of the Research

This thesis's format is intended to offer a thorough examination of the ECSF's implementation inside the CyberSecPro project and its effects on the cybersecurity capabilities of the healthcare industry. Table 1 shows how the chapters are arranged.

Abstract	Highlights the main goals, conclusions, methods and conclusions.
Introduction	Examines the body of research on cybersecurity in healthcare, the value of cyber-skills education, different cyber-skills frameworks, and global cybersecurity collaboration. Contains background information, research aims, significance, and thesis structure.
Methodology	Explains how the study's data was collected, analyzed, and used in its research design.
Results	Outlines the conclusions drawn from the data gathered, evaluating the influence of the ECSF as well as skills shortages. Interprets the findings and discusses how they may affect the healthcare industry as well as the topic of cybersecurity education more broadly.
Conclusion	Describes the main conclusions, points out certain limitations, and offers suggestions for more study and application.
References	Enumerates every source that the thesis cites.
Appendices	Contains more information, interview questions, interview instructions, and other stuff.

Table 1: Structure of the thesis

The thesis intends to offer a clear and methodical investigation of how the ECSF can be successfully applied to improve cybersecurity capabilities in the healthcare industry by adhering to this format.

2 Literature Review

As digital threats grow increasingly complex and widespread, sectors like healthcare face distinct challenges due to the sensitive nature of patient data and the reliance on integrated digital systems. With the rising incidents of cyberattacks in healthcare, frameworks like the ECSF have become essential in addressing these sector-specific vulnerabilities by defining critical skill sets and establishing role-specific competencies to build resilience. This literature review examines the cybersecurity landscape, highlighting the ECSF's potential contributions to healthcare-specific challenges.

2.1 Introduction to Cybersecurity in Healthcare

The healthcare industry has experienced a swift digital revolution that has transformed patient care, data management, and operational efficiency. This transition has brought about numerous advantages for both patients and healthcare providers. However, because healthcare companies manage vast amounts of sensitive data, they have become prime targets for cybercriminals, resulting in critical vulnerabilities (Aldawood & Skinner, 2019; Kruse et al., 2017). Phishing attacks, ransomware, and massive data breaches are among the numerous cyberthreats that the healthcare industry faces (Martin et al., 2017; McLeod & Dolezel, 2018). These threats not only compromise patient privacy but also have the potential to disrupt treatment delivery, creating risks for patient safety and service continuity (Zahabi et al., 2020). Strong cybersecurity measures are urgently needed to safeguard patient data and ensure healthcare services remain accessible, highlighting the need for healthcare organizations to prioritize cybersecurity (Johnson & Willey, 2020; Zhuang et al., 2019).

2.2 The Importance of Cyber-Skills and Training

The growing reliance on digital technologies across various sectors has made cybersecurity skills and training increasingly crucial. In healthcare, this need is even more pronounced due to the sensitive nature of the data handled and the critical services provided (McLeod & Dolezel, 2018; Martin et al., 2017). The healthcare sector faces unique challenges, including safeguarding patient records and ensuring the uninterrupted operation of medical systems, which makes the development of robust cybersecurity competencies essential. Effective cybersecurity training provides healthcare staff with the knowledge and skills required to identify and mitigate threats, contributing to a more secure environment (Chua et al., 2021; Zhuang et al., 2019). By fostering a culture of cybersecurity awareness and preparedness, healthcare organizations can build a strong defense strategy against evolving cyber risks, ensuring patient safety and operational continuity (Johnson & Willey, 2020; Aldawood & Skinner, 2019).

2.3 The Need for Cyber-Skills in Healthcare

The complex interconnectivity of their systems presents special cybersecurity challenges for healthcare organizations. New vulnerabilities have been brought about by the digitization of medical records, the growth of telemedicine services, and the proliferation of networked medical devices (Sharma & Balamurugan, 2020). In order to safeguard sensitive patient data and guarantee the continuation of healthcare services, the healthcare industry needs a workforce with up-to-date cybersecurity capabilities since cyber threats continue to change and become more complex (Raghupathi & Kesh, 2018).

Studies reveal that human factors—like inadequate staff training and awareness—play a significant role in healthcare data breaches (Kruse et al., 2017; McLeod & Dolezel, 2018). This emphasizes how crucial it is to spend money on ongoing cybersecurity education and training in order to reduce these dangers. Developing a workforce that understands cybersecurity is essential to improving healthcare organizations' overall security posture (Johnson & Willey, 2020).

2.4 Cyber-Skills Training Programs

Comprehensive training programs that cover a wide range of topics, from fundamental cybersecurity awareness to advanced technical competencies, are necessary to improve cybersecurity skills in the healthcare industry (Schatz et al., 2017). Effective training curricula must be customized to the unique requirements of the company and the roles that workers play. This entails being aware of the various hazards that workers could encounter, spotting weak points in healthcare systems, and learning how to effectively reduce these risks (Yildirim & Mackie, 2019).

Extensive research demonstrates the value of experiential learning and practical activities in cybersecurity education. Participants' comprehension of the effects of their activities and their capacity to react to cybersecurity issues are enhanced by simulated settings and real-world scenarios (Bada et al., 2019; Alotaibi & Almagwashi, 2020). By bridging the knowledge gap between theory and practice, these interactive techniques give healthcare personnel the tools they need to safeguard vital systems and data.

2.5 Existing Cyber-Skills Frameworks

Several cyber-skills frameworks have been established to aid the planning and implementation of effective training programs. According to Kozik and Choraō (2018), these frameworks offer an organized method for determining the knowledge and abilities required for different tasks within an organization.

The NIST NICE Cybersecurity Workforce Framework (NIST, 2021) is a notable instance of this, as it specifies and classifies cybersecurity job roles along with the corresponding knowledge, skills, and abilities (KSAs). According to Newhouse et al. (2017), this approach aids organizations in methodically identifying skill gaps and creating customized training programs to address those particular needs.

The TIGER International Recommendation Framework of Core Competencies in Health Informatics (Hübner et al., 2019) is another noteworthy framework. The interdisciplinary nature of cybersecurity in healthcare and the necessity of IT and healthcare experts working together are highlighted by this approach. It offers a thorough understanding of how IT and healthcare teams can collaborate to safeguard sensitive health data while guaranteeing effective service delivery by concentrating on health informatics competencies.

2.6 Relevance of ECSF in Healthcare

The ECHO Cyber-Skills Framework (ECSF), with its all-encompassing approach to detecting and filling cybersecurity skill shortages, can be extremely beneficial to the healthcare industry. By offering organized standards for creating, updating, and executing efficient training programs, ECSF seeks to improve the cybersecurity knowledge and competencies of healthcare personnel (Varbanov, 2021).

The emphasis placed by ECSF on individualized learning pathways and ongoing professional development is highly compatible with the requirements of healthcare organizations. By putting this approach into practice, these organizations can improve their cybersecurity posture and becoming more ready for the particular risks and challenges that come with working in their particular environment (Papanikos & Panopoulou, 2020). Through the adaptation of the ECSF to the unique healthcare environment, organizations can mitigate vulnerabilities and guarantee that their workforce is well prepared to tackle emerging threats.

2.7 Implementation of ECSF in Healthcare

Understanding the unique issues faced by the healthcare industry and modifying the framework to suit its needs are essential for the successful implementation of the ECSF. To do this, a comprehensive evaluation of present skill levels must be carried out in order to identify any gaps and create training plans that fill them.

According to Williams et al. (2017), enhancing cybersecurity in healthcare requires ongoing professional development as well as hands-on training. By providing structured training pathways and emphasizing the practical application of abilities, the ECSF promotes these values.

2.8 Chapter Summary

In conclusion, the healthcare industry must invest in ongoing training and cybersecurity skill development if it hopes to counteract the ever-evolving cyber threat landscape. Frameworks such as ECSF, TIGER, and NICE offer useful guidance for designing training initiatives. In particular, the ECSF provides a thorough and customized approach to improving cybersecurity skills in the healthcare industry, taking into account the particular needs and challenges of this field.

In the sections that follow, we will examine the individual elements of the ECHO Cyber-Skills Framework (ECSF) as well as its advantages and uses for the healthcare industry.

3 Methodology

With an emphasis on improving cybersecurity capabilities in the healthcare industry, this chapter describes the study methodology used to examine the use of the ECHO Cyber-Skills Framework (ECSF) inside the CyberSecPro project. The study's methodology, data gathering techniques, and data analysis protocols are explained to offer an organized and clear way to assess the ECSF's influence.

3.1 Research Design

This study utilized interviews to gain a comprehensive understanding of the experiences, challenges, and perceived benefits associated with the ECSF implementation in the healthcare sector. The interview process was structured to cover key areas, including participants' general awareness of cybersecurity, current training practices, and the ECSF's perceived relevance. Four healthcare professionals and three cybersecurity experts were interviewed, resulting in insights from a total of seven participants.

Cybersecurity experts Interviews	
Purpose	To investigate the process of implementation, pinpoint difficulties in such a process, and compile feedback from participants regarding the effectiveness and applicability of the ECSF.
Participants	The interviewees included four healthcare professionals and three cybersecurity experts who are directly involved in, or impacted by, the ECSF implementation in healthcare.

Format	Semi-structured interview questions were chosen as the best approach so they can facilitate in depth answers and give space to follow-up inquiries.
Procedure	Interviews were held either in-person or as a videoconference, which was then recorded with consent and subsequently transcribed for analysis.

Table 2: Cybersecurity expert interviews

Each interview provided unique perspectives based on the participants' roles, which included IT experts, cybersecurity specialists, organizational leaders, and healthcare staff involved in cybersecurity practices. The interviews were conducted either in person or via video calls, depending on the participants' preferences, while some individuals opted for written responses to the interview questions. This approach allowed for in-depth exploration of topics relevant to ECSF implementation, helping to identify sector-specific needs and inform recommendations. Closer look at the interviews can be found in Tables 2 and 3.

Healthcare professionals interviews	
Purpose	To gather qualitative information and understanding about participants' cybersecurity knowledge, expertise, and their self-assurance in the IT/cybersecurity field.
Participants	Individuals who have completed the CyberSecPro project's ECSF training or healthcare professionals handling sensitive data. Participants of the interviews were invited personally one at the time to answer the questions.
Format	conducted before implementation are used to monitor changes in practices and competencies.
Procedure	Interviews were conducted to assess the level of education before a hypothetical implementation

Table 3: Healthcare professionals interviews

3.2 Document Analysis:

To give a thorough grasp of the ECSF implementation within the CyberSecPro project, this study uses a mixed-methods approach. The approach examines how the ECSF meets cybersecurity requirements in the healthcare industry by combining qualitative and document analytic techniques. The major purpose is to gather in-depth feedback from stakeholders, including healthcare professionals and cybersecurity specialists, to identify training gaps, assess ECSF's relevance, and evaluate its influence on cybersecurity skills.

The methodology's elements, such as participant selection, data collection instruments, and data analysis techniques, are described in Table 4 below. Every element was selected to support the goals of the study and provide a thorough investigation of the ECSF's use.

Purpose	Reviewing pertinent documentation pertaining to the CyberSecPro and ECSF projects.
Documents	Training materials, policy papers, implementation reports, and other pertinent documents. This Includes the paper "ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism" as a primary resource for understanding the framework's application in healthcare.
Procedure	Documents will be examined in order to add to our understanding of the ECSF implementation and to set the interview results in perspective

Table 4: Document Analysis

3.3 Data analysis

The techniques and protocols used to examine the qualitative data gathered for the study are described in this section. The purpose of the analysis is to assess the effects of the

Cybersecure project's deployment of the ECHO Cyber-Skills Framework (ECSF), specifically in the healthcare industry.

To guarantee that the results of data analysis are accurate, trustworthy, and offer significant insights into the efficacy of the ECSF, a number of procedures must be followed.

The qualitative analysis concentrates on identifying themes and patterns from the interviews and focus group discussions. This method offers a thorough grasp of how the ECSF is implemented and how it affects strengthening cybersecurity capabilities.

3.4 Qualitative Analysis

The objective of the qualitative analysis is to extract detailed insights from the viewpoints and experiences of the parties engaged in the ECSF implementation. To detect reoccurring themes and important findings, interview and focus group transcripts are coded and thematically analyzed.

The study aims to give a comprehensive assessment of the efficacy of the ECSF in the CyberSecPro project and its potential for wider deployment in the healthcare industry by using qualitative evaluations.

The qualitative analysis of the information obtained from in-depth interviews with healthcare and cybersecurity experts is covered in detail in chapter 4. This analysis's main goals are to investigate cybersecurity awareness levels at the moment, the state of training, and the perceived usefulness of the European Cybersecurity Skills Framework (ECSF) in healthcare environments. The use of qualitative research methodologies, specifically interviews, was based on their capacity to offer comprehensive and deep perspectives into the beliefs, encounters, and anticipations of people employed in the healthcare industry.

A variety of healthcare professionals and cybersecurity experts were interviewed in order to obtain a range of viewpoints regarding the difficulties associated with cybersecurity and the necessity for training. This chapter analyses their answers in an effort to find important themes and trends that might guide the creation and application of cybersecurity plans specific to the healthcare sector.

In addition to highlighting the shortcomings in the state of cybersecurity, the results of this qualitative research will offer useful suggestions for incorporating the ECSF into already-existing frameworks. The methods for data collection and analysis will be presented in this chapter first, and then the results of the interviews will be thoroughly examined.

3.5 Ethical considerations:

In order to guarantee the authenticity and integrity of the research, ethical considerations are essential. In order to safeguard each participant's rights and welfare, this study complies with ethical guidelines. Confidentiality, ethical approval, and informed consent are the three primary ethical factors in this study.

3.5.1. Informed consent

A basic ethical prerequisite for research involving human subjects is informed permission. Before beginning the study, every participant is given thorough information on the goals, methods, possible dangers, and rewards of the research. This comprises a study Explanation: Participants receive information about the goals of the research, the extent of their participation, and the expected outcomes.

Participation is completely optional, and participants are allowed to leave the study at any moment without facing any repercussions.

3.5.2. Confidentiality

One of the most important ethical considerations in this investigation is keeping participant information secret. There are safeguards in place to guarantee the confidentiality of the data gathered and the protection of participants' identity. This comprises firstly of anonymity, aimed to maintain participant anonymity, personal identifiers are eliminated from the data. Secondly there’s data access, so research team is the only ones with access to the data, and they will only utilize it in this study.

3.6 Limitations

Despite the rigorous design and methodology, this study faces several limitations that need to be acknowledged.

Firstly, the generalizability of the findings may be constrained by the specific focus on the ECSF’s application within the CyberSecPro project, particularly in the healthcare sector. Although the findings provide valuable insights, they may not directly translate to other industries or regions with different cybersecurity structures and needs. The healthcare sector's unique requirements, combined with the specific geographic focus of this study, limit the extent to which these findings can be applied broadly.

Secondly, a key limitation is the reliance on self-reported data from interviews. Participants may have responded in socially desirable ways or struggled to recall specific events or details, introducing potential bias. Self-reported data are inherently subjective and may not always

align with objective measures of cybersecurity skills or knowledge. To mitigate these issues, the study triangulated self-reported information with document analysis and expert opinions to enrich the data and add perspective.

Lastly, the implementation timeline presents a significant constraint on evaluating the ECSF's impact. Assessing the long-term benefits and changes resulting from the ECSF implementation is challenging within a limited study period. While this research addresses immediate outcomes, understanding the full impact on cybersecurity skills and readiness requires a longitudinal approach that extends beyond the scope of this study.

In recognizing these limitations, this study provides a balanced view of its findings and implications, laying a foundation for future research to explore the ECSF's long-term effects and broader applications.

This chapter outlined the methodology used to investigate the implementation of the ECHO Cyber-Skills Framework (ECSF) within the CyberSecPro project, with a focus on its application in the healthcare sector. The research design incorporated both qualitative data from interviews with key stakeholders and a comprehensive document analysis. These combined methods provided a robust approach to assess the ECSF's effectiveness in addressing cybersecurity skill gaps and enhancing competency levels.

The data collection process involved gathering various perspectives from stakeholders engaged in the ECSF implementation. This included structured interviews and the review of project documentation, ensuring that both practical insights and theoretical contexts informed the findings. Data analysis followed a thematic approach, enabling the identification of core themes, patterns, and critical insights relevant to cybersecurity skill development within the healthcare setting.

Ethical considerations were rigorously addressed to uphold the study's integrity and protect participant rights. Informed consent was obtained from all interviewees, and confidentiality measures were strictly enforced to secure sensitive information. The study adhered to approved ethical standards throughout, ensuring participant welfare and transparency in the research process.

This chapter also acknowledged the study's limitations, noting constraints related to generalizability, reliance on self-reported data, and the study's implementation timeline. Recognizing these limitations allows for a balanced interpretation of the findings and provides avenues for future research to build upon and address these challenges. The methodology outlined here forms a structured foundation for the upcoming analysis and discussion of the ECSF's impact on cybersecurity skills and competencies in healthcare.

In the upcoming chapter, the results of the data gathered using this methodology will be presented and discussed, offering a thorough examination of the ECSF's influence on improving cybersecurity competencies and skills in the healthcare industry.

4 Findings and Discussion

The research results on the use of the ECHO Cyber-Skills Framework (ECSF) inside the CyberSecPro project are presented in this chapter along with a discussion of their implications. The goal of this chapter is to give a thorough review of how ECSF has improved cybersecurity capabilities in the healthcare industry.

The chapter begins by outlining the major themes and trends found in the qualitative interviews with cybersecurity experts and stakeholders. These revelations provide a more thorough comprehension of the experiences, difficulties, and advantages related to the ECSF implementation. Secondly, it showcases the interview data's qualitative analysis, emphasizing how participants' cybersecurity habits, knowledge, and abilities changed both before and after the ECSF training.

These results are integrated in the discussion part, which connects them to the original research questions and body of literature. It assesses the applicability of the framework, offers suggestions for future implementations, and critically looks at how well the ECSF addresses the cybersecurity skills gaps in healthcare. The study's wider implications for cybersecurity education and training are also covered in this chapter, especially as they relate to vital infrastructure industries like healthcare.

This chapter offers a comprehensive explanation of how the ECSF may improve cybersecurity capabilities, the difficulties faced during its implementation, and the lessons learnt by using the qualitative and data. The goal of this thorough analysis is to provide insightful information to organizations, educators, and policymakers that are looking to improve their cybersecurity posture through focused training and educational programs.

These results are integrated in the discussion part, which connects them to the original research questions and body of literature. It assesses the applicability of the framework, offers suggestions for future implementations, and critically looks at how well the ECSF addresses the cybersecurity skills gaps in healthcare. The study's wider implications for cybersecurity education and training are also covered in this chapter, especially as they relate to vital infrastructure industries like healthcare.

This chapter offers a comprehensive explanation of how the ECSF may improve cybersecurity capabilities, the difficulties faced during its implementation, and the lessons learnt by combining the qualitative data and the literature

review. The goal of this thorough analysis is to provide insightful information to organizations, educators, and policymakers that are looking to improve their cybersecurity posture through focused training and educational programs.

4.1 Presentation of the document "ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism".

This section contains the paper "ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism." This paper is an essential tool for comprehending how the ECHO Cyber-Skills Framework (ECSF) is applied in the particular setting of health and medical tourism. The contents of the document offer a comprehensive analysis of the ECSF, outlining its goals, methods, and structure as well as how it can be applied to improve cybersecurity competencies.

The document titled *"ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism"* provides a structured approach to implementing the ECSF within the healthcare and medical tourism industries. Its content is divided into several key sections that outline the framework's objectives, methodologies, and practical applications, thereby enabling organizations to bolster their cybersecurity defenses effectively.

The introductory section of the document offers an overview of the ECSF, detailing its origin, purpose, and relevance to the healthcare sector and medical tourism. This section emphasizes the pressing need for robust cybersecurity measures in these fields, given the sensitivity of health data and the increasing reliance on digital systems in medical operations.

Following this, the document delineates the ECSF's primary objectives, with a focused goal of addressing cybersecurity skills gaps within healthcare organizations. The objectives stress the importance of developing training programs that specifically address the challenges these sectors face and aim to equip healthcare professionals with the necessary skills to manage and mitigate cybersecurity risks effectively.

Methodological guidelines provided in the document offer comprehensive instructions for designing, updating, and implementing training programs based on the ECSF. This methodology includes conducting needs assessments, developing curricula, and establishing metrics to evaluate the effectiveness of training interventions, ensuring that the ECSF remains adaptable and relevant to evolving cybersecurity demands.

The document further explores practical strategies for applying the ECSF within healthcare and medical tourism contexts. This section discusses best practices and potential challenges organizations might encounter, such as limited resources or resistance to change, and offers solutions to integrate the framework seamlessly into existing training initiatives.

Additionally, the document includes case studies and examples that illustrate successful ECSF implementation in healthcare settings. These real-life scenarios demonstrate how the framework has led to tangible improvements in cybersecurity skills and awareness, serving as a model for other organizations considering ECSF adoption.

Finally, an assessment and evaluation section in the document provides guidance on measuring the outcomes of ECSF-based training programs. This includes both pre- and post-training assessments, participant feedback mechanisms, and performance metrics to track improvements in organizational cybersecurity practices. These evaluation tools underscore the importance of continuous improvement in cybersecurity training to keep pace with emerging threats.

4.2 Summary of "ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism".

In order to guarantee safe collaboration, defend the European market, and protect citizens from cyber-attacks, the ECHO (European network of cybersecurity centers and competence hub for innovation and operations) Horizon 2020 Project seeks to create a European cybersecurity ecosystem. The ECHO Cyber-Skills Framework (ECSF), one of its main resources, is a platform for enhancing cybersecurity education and training in vital industries like healthcare, transportation, and energy.

4.2.1 ECSF's Benefits for Healthcare

By filling in important gaps in cybersecurity knowledge and expertise, the ECSF provides the healthcare industry with tremendous advantages. Patient data and vital medical services are at risk because many hospital IT workers say they lack the necessary knowledge and abilities in areas like data protection and cybersecurity compliance. By implementing ECSF, healthcare organizations' entire cybersecurity posture would be improved through organized training and awareness initiatives targeted at reducing these risks.

4.2.2 Challenges and Solutions for Implementing ECSF in Healthcare

The ECSF is recognized in the study as a useful framework for enhancing cybersecurity in the medical field. Notwithstanding, the industry encounters obstacles like scarce resources, diverse organizational configurations, and the requirement for ongoing education. To help healthcare organizations manage risks and strategically adopt ECSF, the ECHO Multi-Sector

Assessment Framework (E-MAF) is suggested as an additional tool. To address cybersecurity needs, E-MAF directs resource allocation and aids in defining sector-specific competences.

4.2.3 Proposed Strategy for Healthcare and Medical Tourism

For successful implementation, a slow, phased approach that emphasizes continuous staff training is suggested. The ECSF would not only benefit traditional healthcare institutions but also sectors related to health and medical tourism, where the secure exchange of health information between countries is critical. The ECSF can play a pivotal role in ensuring the cybersecurity of cross-border health data exchange in line with EU regulations on health information and digital healthcare.

4.2.4 Potential Long-Term Benefits for the ECHO Network

The use of ECSF in the healthcare industry would encourage sustained cooperation between ECHO and healthcare institutions, which might result in future advancements in cybersecurity frameworks that are relevant to other industries. Additionally, by improving cybersecurity capabilities in a variety of healthcare contexts, this deployment helps the digital revolution of healthcare throughout the EU.

4.3 Analysis of Key findings for the Document

A thorough examination of how the ECSF can be used to improve cybersecurity skills and competencies in the healthcare and medical tourism sectors can be found in the publication "ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism". This part explores the document's main conclusions, analyzing their significance and applicability to our study goals.

4.4 Cybersecurity Skills Gaps in Healthcare and Medical Tourism

The report highlights a critical shortage of cybersecurity expertise within the medical tourism and healthcare industries. Important conclusions include a significant lack of specialized training, as many healthcare workers are not adequately equipped to manage cyber risks due to insufficient cybersecurity education. Additionally, there is an awareness deficit, with healthcare workers generally underestimating the importance of cybersecurity, which makes them more vulnerable.

Furthermore, there are technical proficiency deficits, as experts often lack the necessary technical skills to implement and manage advanced cybersecurity solutions. To address these gaps, the report recommends training programs tailored to the specific goals and challenges of the healthcare industry. Increasing awareness through ongoing education and hands-on training can significantly strengthen the overall cybersecurity posture.

4.5 Merits and Applicability of the ECSF

The document outlines the benefits of the ECSF and describes how it can be used to close noted skills gaps. The ECSF provides a comprehensive framework, ranging from fundamental awareness to advanced technological competencies, offering a thorough and organized method for acquiring cybersecurity skills. It includes customized training modules designed specifically for different roles within healthcare organizations to ensure appropriate and efficient training. Through its methodological rigor, the ECSF offers guidelines for the systematic creation, execution, and evaluation of training programs.

In addition, the ECSF's systematic methodology can help standardize cybersecurity training across the healthcare industry, ensuring uniformity and quality. Customized modules enhance the training's efficacy and relevance, strengthening readiness for cyberthreats.

4.6 Implementation strategies

Important conclusions about the application of the ECSF in medical tourism and healthcare highlight the following: integrating the ECSF with existing professional development and training programs is essential for successful deployment. Effective implementation also requires engagement from stakeholders, including management and IT personnel, to ensure active involvement. Additionally, successful implementation depends on allocating sufficient time, funding, and personnel.

The integration of the ECSF with current initiatives helps minimize disruptions and promotes a smoother adoption process. Active stakeholder involvement ensures buy-in and support, which are crucial for the longevity of training efforts. Lastly, the effective allocation of resources is fundamental to creating and implementing high-quality training programs.

4.7 Case studies and Examples

The document includes case examples demonstrating how the ECSF has enhanced cybersecurity knowledge and skills. Key lessons learned include its real-world impact, as organizations that have adopted the ECSF report significant improvements in their cybersecurity posture. Additionally, the ECSF's modular design allows for scalability, adapting to organizations of various sizes and resource levels. The framework's iterative design supports ongoing improvement, enabling organizations to adjust to evolving cyberthreats.

These successful outcomes from the case studies validate the ECSF's effectiveness and provide a model for other institutions. The framework's scalability ensures that it can be adopted by a wide range of healthcare providers, from small clinics to large hospitals. Furthermore, continuous improvement practices help organizations stay proactive against emerging cyberthreats, reinforcing their long-term cybersecurity resilience.

4.8 Assessment and Evaluation

The document outlines methods to evaluate and test the effectiveness of training programs based on the ECSF. Key elements include conducting assessments both before and after training to measure progress in knowledge and skill levels. Feedback mechanisms are used to gather participant input, helping to identify areas for improvement. Performance indicators are also utilized to assess the impact of training on organizational cybersecurity practices.

These rigorous evaluation methods ensure that training programs are effective and meet their objectives. Feedback systems support continuous improvement, helping to keep training relevant and effective. Performance metrics provide a concrete assessment of the training's impact, enabling data-driven decision-making.

4.9 Chapter conclusion

The important importance of the ECSF in addressing cybersecurity skills gaps in the healthcare and medical tourism sectors is highlighted by the major results from the document "ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism". Our research is greatly aided by the document's insights into the framework's applicability, implementation methodologies, and assessment techniques. With the help of these discoveries, we can create a thorough and efficient plan for integrating the ECSF into the CyberSecPro project, which will ultimately improve cybersecurity capabilities in the healthcare industry.

5 Qualitative Analysis

5.1 Healthcare Interview Findings

Dasha, Felix, Manu, and Miia, the healthcare workers who were interviewed, underlined that cybersecurity is still an important but frequently neglected part of the healthcare industry. Although most people are aware of the threats associated with cybersecurity, there are several obstacles that prevent organized frameworks like the European Cybersecurity Skills Framework (ECSF) from being used in practice.

Dasha emphasized that relying too much on IT generalists and without specialized cybersecurity teams is a serious shortcoming. She claims that because healthcare organizations prioritize patient care, they frequently overlook the need for strong cybersecurity safeguards until a breach or incident happens. She emphasized that better cybersecurity hygiene across healthcare settings and increased role clarity could result from aligning jobs that are specific to healthcare with the ECSF.

Felix expressed similar worries while also bringing out the resource limitations that smaller healthcare institutions must contend with. He thinks that despite its good intentions, the ECSF might be too complicated for small healthcare providers, who don't have the resources or know-how to put such a framework in place. Felix proposed the necessity for specialized, healthcare-focused ECSF modules that address certain industry risks, like patient data privacy and medical device security, in order to make ECSF adoption practical.

Manu offered a distinct viewpoint, highlighting the significance of ongoing training for personnel in both clinical and non-clinical roles. He maintained that although IT specialists play a crucial role in overseeing cybersecurity infrastructure, all members of the healthcare team, from physicians to administrative staff, should be conversant in fundamental cybersecurity procedures. Cross-functional training, according to Manu, could aid in bridging the divide between IT and healthcare teams and promote a security-conscious culture that is in line with the goals of ECSF.

Considering her experiences, Miia said that cybersecurity training is frequently neglected by healthcare workers who are overburdened with legal duties and patient care responsibilities. She suggested giving healthcare organizations access to streamlined ECSF guidelines, which would make it simpler for non-experts to comprehend and apply cybersecurity measures without requiring in-depth technical knowledge. In order to facilitate adoption and compliance, Miia also underlined the necessity for ECSF to incorporate useful tools and templates designed specifically for healthcare facilities.

All things considered, the healthcare professionals concurred that although the ECSF provides a thorough method of tackling the cybersecurity skills gap, industry-specific modifications are required for the framework to be genuinely successful in the healthcare industry. They all suggested that the ECSF provide cross-functional training for the larger workforce involved in patient care and data administration, in addition to emphasizing the technical proficiency of IT specialists.

5.2 Cybersecurity Experts' Findings

The three cybersecurity specialists who were interviewed—Dorin, Andrea, and Simone—offered insightful commentary on how the European Cybersecurity Skills Framework (ECSF) is being applied in the healthcare industry. Their conclusions highlight how crucial cybersecurity is to protecting private health information and how crucial it is to match cybersecurity procedures to the particular requirements and limitations of healthcare institutions.

The relevance and applicability of the ECSF in healthcare were emphasized by the experts, highlighting the applicability of the ECSF in tackling the cybersecurity issues in the medical

field. Dorin made the point that the structure of the ECSF might be very helpful in standardizing roles and competences inside healthcare organizations—which are currently plagued by a disjointed cybersecurity strategy. He pointed out that in order to effectively handle cybersecurity risks, the healthcare industry, like other crucial industries, needs well defined job duties and responsibilities. The ECSF may close this gap by providing precise criteria for hiring and training personnel.

Andrea stressed the importance of the ECSF's role descriptions for industries like healthcare, where adhering to regulations (such the GDPR and the NIS Directive) is critical. She maintained that the healthcare industry may be better able to comply with these regulations if the ECSF placed more emphasis on skills mapping, especially with regard to incident response and data protection.

Although Andrea underlined that adaptation is required, Simone highlighted the potential of the ECSF to improve cybersecurity in the healthcare industry. According to Simone, in order for the ECSF to be implemented successfully, the healthcare industry must face its unique obstacles, which include legacy systems, scarce resources, and a dearth of specialized cybersecurity staff.

The cybersecurity specialists acknowledged the benefits of the ECSF but also pointed out a number of obstacles to its application in the healthcare industry. All three experts cited financial restrictions as a major obstacle. Simone emphasized that many healthcare organizations—particularly smaller ones—might find it difficult to cover the expenses of bringing in cybersecurity experts or offering training that is in line with the ECSF. Furthermore, he noted that the implementation of an organized framework such as the ECSF may be impeded by non-technical staff members' ignorance of cybersecurity issues.

Additionally, Andreea and Dorin highlighted the cultural opposition to cybersecurity efforts in the medical field. According to Dorin, a lot of healthcare organizations view cybersecurity as less important than therapeutic concerns, which can make them reluctant to embrace comprehensive frameworks like the ECSF. According to Andreea, this cultural barrier is frequently made worse by the lack of experience in healthcare IT departments, which makes it challenging to incorporate the ECSF's criteria into regular operations without a lot of outside assistance.

The cybersecurity specialists offered a number of suggestions to raise the likelihood that healthcare institutions will successfully apply the ECSF. Dorin promoted a staged implementation strategy for the ECSF, advising healthcare organizations to begin with incident responders and data protection officers as important positions before extending the framework to other domains. He underlined the need of executive buy-in, pointing out that in

order to guarantee that adequate funds and time are devoted to cybersecurity initiatives, senior management must be persuaded of the ECSF's worth.

Andrea suggested that in order to address the particular difficulties the healthcare industry has, the ECSF offer modules or modifications tailored to the industry specifically. Case studies of the effective application of the ECSF in the healthcare industry and useful resources to help organizations adapt the ECSF to their unique environment could be among them. The speaker proposed that it would be beneficial to promote ongoing training and certification, given the dynamic nature of healthcare threats.

Cross-industry cooperation is necessary for ECSF implementation in healthcare, Simone stated. In order to share best practices and assist healthcare in catching up to more developed cybersecurity procedures, he promoted collaborations between cybersecurity professionals from other industries, such as critical infrastructure or finance, and healthcare organizations. Simone also underlined the necessity of outside assistance from cybersecurity experts and training providers to help healthcare organizations navigate the challenges of implementing ECSF.

Lastly, they talked about how the healthcare industry would fare in the long run if ECSF usage became widespread. Both Dorin and Andreea anticipated that the ECSF's ability to standardize jobs and abilities would result in a more proficient and professional cybersecurity workforce in the healthcare industry. if a result, patient safety and data security may eventually improve if fewer and milder cyberattacks against healthcare organizations occur.

Simone emphasized how the ECSF can foster cross-border cooperation, especially inside the European Union. He contended that the adoption of the ECSF by healthcare organizations worldwide might result in increased cybersecurity knowledge sharing and interoperability, strengthening the industry's overall resistance to cyberattacks.

5.3 Integration of Document and Study findings

This section presents a summary of the key findings from the qualitative information obtained from healthcare professional interviews as well as the document analysis of the "ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism". The incorporation of these findings contributes to the development of a thorough understanding of the cybersecurity training and skill levels in the healthcare industry, as well as the potential contribution of the ECSF to filling in current gaps.

5.3.1 Alignment of Document Findings with Interview Data

This section compares the interview data from cybersecurity experts and healthcare professionals with the document findings from the ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism. This alignment draws attention to the similarities, differences, and intersections between theoretical frameworks and real-world applications in the healthcare industry.

5.3.2 Awareness of Cybersecurity Needs in Healthcare

The examination of the documents highlighted the increasing recognition of the necessity of all-encompassing cybersecurity plans in the medical field, especially in light of the growth of telemedicine and digital health data. Dasha, Felix, Manu, and Miia, healthcare professionals, also voiced alarm about the growing dangers posed by cyber threats to their day-to-day operations. They concurred with the document's claim that cybersecurity had to take precedence in the healthcare industry and recognized the vital need of safeguarding patient data. But there was a clear disconnect between awareness and behavior.

Healthcare workers acknowledged that, despite the ECSF and ECHO frameworks' defined pathways for enhancing cybersecurity education, the practical application of these frameworks is still hindered by a lack of resources, gaps in training, and cultural opposition inside healthcare organizations.

5.3.3 Skill Gaps and Training Needs

The cybersecurity knowledge of healthcare workers has serious inadequacies, as shown by the document analysis and interview data. In line with feedback from both cybersecurity experts and healthcare professionals, the ECHO Cyber-Skills Framework specifically recognized areas like incident response, data protection, and risk management as critical competences for healthcare workers. The interviewees from the healthcare industry stated that they frequently rely on general IT knowledge, which is inadequate for the constantly changing threat landscape, due to their lack of professional cybersecurity training. This is consistent with the document's findings, which emphasize the necessity for specialized training curricula that tackle the unique difficulties associated with healthcare cybersecurity.

Furthermore, Dorin, Andreea, and Simone—three cybersecurity experts—reiterated these worries, stressing that healthcare organizations frequently lack specialized cybersecurity staff members and a well-organized cybersecurity training program.

They pointed out that by standardizing responsibilities and capabilities, the ECSF might aid in closing this gap; nevertheless, implementation is still sluggish because of a lack of institutional commitment and understanding.

5.3.4 Role of the ECSF in Enhancing Cybersecurity

The document put up the ECSF as a possible means of standardizing cybersecurity responsibilities and competences within the healthcare sector. The ECSF provides a useful framework for defining roles, addressing talent shortages, and enhancing general cybersecurity processes, according to cybersecurity experts surveyed. They emphasized how the ECSF may serve as a standard for healthcare institutions, assisting in the uniformity of positions like risk analysts, data protection officers, and incident responders.

The medical professionals did, however, voice some doubt over the framework's immediate application in their organizations. Although they acknowledged the potential advantages of implementing the ECSF, they pointed out real-world obstacles that could impede its adoption, such as a lack of funding and organizational inertia. This is consistent with the document's conclusions that, although important, frameworks like the ECSF must be modified to meet the unique requirements and budgetary restrictions of the healthcare industry in order to be effective.

5.3.5 Regulatory Compliance and Cybersecurity Frameworks

The document placed a major emphasis on how legislative frameworks like the GDPR and the NIS Directive encourage the implementation of more robust cybersecurity safeguards. The interviews revealed that compliance is frequently the driving force for healthcare organizations' cybersecurity investments. This was a recurrent theme among the cybersecurity specialists. According to the experts, adopting the framework by healthcare organizations may be further encouraged by ensuring that the ECSF is in line with these statutory criteria. Healthcare professionals, on the other hand, agreed that compliance was important, but they believed that wider cybersecurity training needs were sometimes overlooked in favor of complying with legal obligations.

5.3.6 Cultural and organizational barriers

Throughout the document analysis and interview process, one recurring topic was the presence of organizational and cultural hurdles to better cybersecurity practices in the healthcare industry. The examination of the documents revealed a pervasive reluctance to change in healthcare organizations, where cybersecurity efforts are frequently subordinated to therapeutic needs. The interviews with healthcare experts confirmed this, stating that cybersecurity is frequently viewed as a less important issue than patient care. Cybersecurity

experts also pointed out that adoption of frameworks such as ECSF would continue to be difficult in the absence of strong leadership and a change in organizational culture.

5.3.7 Integration of Cybersecurity with Clinical Operations

The need for improved cybersecurity integration with clinical operations is another crucial point of agreement between the conclusions from the documents and the information from the interviews. To create a workforce that is more security-conscious, the ECHO Cyber-Skills Framework pushes for cross-training between IT professionals and clinical personnel. Healthcare experts attested to the fact that there are gaps in communication and cooperation between the IT and clinical teams, which compromise patient data security. Experts in cybersecurity also emphasized how critical it is to dismantle these divisions and incorporate cybersecurity concerns into routine therapeutic procedures.

5.4 Divergences Between Document and Study Findings

There are significant differences between the theoretical recommendations in the documents and the actual experiences of healthcare professionals and cybersecurity experts, even though the document analysis and interview data highlight many of the same themes regarding the significance of cybersecurity in healthcare. The primary distinctions between the interview comments and the results of the ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism are discussed in this section.

- Perception of Cybersecurity Urgency

The ECHO Cyber-Skills Framework presents cybersecurity vulnerabilities in healthcare as a serious problem that requires prompt and all-encompassing solutions, emphasizing the importance of tackling them. The report recommends that, considering the hazards of compromised medical data and service interruptions, healthcare institutions priorities cybersecurity on par with patient care.

The feeling of urgency surrounding cybersecurity concerns is growing, however healthcare professionals (Dasha, Felix, Manu, and Miia) have suggested that this awareness does not necessarily convert into organizational action. Based on their experiences, it appears that cybersecurity is still viewed as a peripheral issue, frequently falling behind urgent healthcare issues. Even while they understand how important it is to safeguard patient data; they frequently do not handle cybersecurity with the same urgency as the ECSF document because of the enormous focus on providing day-to-day patient care. This disparity draws attention to a disconnect between the idealized frameworks found in documents and the demands that healthcare professionals encounter in the actual world.

- Framework Complexity vs. Practicality

A thorough and complete method for identifying responsibilities and abilities in cybersecurity is offered by the ECHO Cyber-Skills Framework. The paper suggests multi-tiered, structured positions that can be tailored to the healthcare industry, emphasizing staff development and specialized cybersecurity training. It portrays the ECSF as an adaptable instrument that can be included into an organization at different levels.

Healthcare workers, on the other hand, felt that the ECSF was a bit overwhelming and challenging to implement in their existing settings. Although the framework is well-structured, they raised worry that healthcare institutions that are not familiar with formalized cybersecurity plans may find it too complex. A lot of healthcare organizations, particularly the smaller ones, don't have the staff or resources to properly implement the ECSF as it is described in the text. This creates a practical divergence in that the structured, ambitious vision of the ECSF might not be achievable without major adaptation to the particular challenges faced by the healthcare industry, especially with regard to resource allocation and scalability.

- Resource allocation and organizational commitment

The ECHO Cyber-Skills Framework is predicated on the assumption that healthcare organizations possess the requisite financial and human resources to devote to the development of a strong cybersecurity program. It highlights the necessity of permanent training programs that comply with ECSF requirements and specialized cybersecurity positions, implying that a substantial investment will guarantee long-term gains.

But as experts in cybersecurity and healthcare both pointed out, the reality is far different. Healthcare organizations, especially public institutions, are often constrained by limited funds and staffing shortages. These limitations mean that there are rarely, if any, dedicated cybersecurity roles and that cybersecurity activities are frequently underfunded. Manu, Miia, and Felix all brought up the difficulties of attempting to put comprehensive cybersecurity plans into practice with little funding and a lack of organizational commitment. The paucity of investment in cybersecurity, despite its recognized necessity, indicates a substantial divergence from the expectations set by the ECSF statement.

- Tailoring the cybersecurity training

The document presents a one-size-fits-all approach to cybersecurity training and implies that the ECSF may be easily applied to a variety of industries, including healthcare. The framework makes the assumption that by adhering to its organized role descriptions and

recommendations, general cybersecurity competencies may be adjusted for the healthcare industry.

Interviewees from the healthcare industry, however, acknowledged the need for industry-specific training that is more in line with the demands of clinical practice. They believed that many of the generic training recommendations made by the ECSF were very general and did not sufficiently address the particular difficulties faced by healthcare professionals, such as striking a balance between cybersecurity and patient care. For example, Felix and Dasha noted that training curricula should be much more hands-on and tailored to the work habits of healthcare personnel, who might not have the time or knowledge to participate in intricate technical training. This discrepancy highlights the necessity for additional healthcare-focused ECSF modifications to make it more applicable and workable for the industry.

- Organizational culture and Change management

The ECHO Cyber-Skills Framework makes the assumption that organizations can successfully incorporate cybersecurity best practices into their daily operations if they receive the appropriate instruction and direction. It proposes that the ECSF might serve as a basis for establishing an organizational culture that is cognizant of cybersecurity and emphasizes the importance of leadership in bringing about change.

But as cybersecurity specialists Dorin, Andreea, and Simone as well as medical experts Manu and Miia pointed out, cultural resistance to change is a significant obstacle to implementing any new framework, including the ECSF. Changes that are viewed as disruptive or unconnected to clinical practice are frequently met with resistance by healthcare organizations, especially those that place a strong emphasis on patient care.

This is particularly true in the case of cybersecurity, which is viewed as a technological field outside the purview of the majority of healthcare professionals. The discrepancy in this case is between the ECSF document's expectation of seamless organizational change and the reality of deeply ingrained procedures and change-resistant cultures in healthcare facilities.

- Integration of Cybersecurity and Healthcare Operations

According to the document analysis, the ECSF can act as a guide for matching technical roles with healthcare procedures, promoting the smooth integration of cybersecurity frameworks into healthcare operations. It is assumed that, with proper planning and execution, cybersecurity issues can be incorporated without interfering with therapeutic procedures. Healthcare workers found this integration to be more difficult in practice. They emphasized the fact that, despite their importance, many cybersecurity measures are viewed as an additional burden rather than a necessary component of healthcare operations. Many people

believe that cybersecurity precautions take a lot of time or interfere with important patient care procedures. For example, Felix brought up the topic of cybersecurity protocols and how they occasionally hold down patient care operations, which irritates medical staff.

This real-world/practical divergence demonstrates that although cybersecurity is envisioned in the paper as a supplement to healthcare operations, in practice, it can frequently feel like a competing priority.

5.5 Implications of Integrated Findings:

There are significant differences between the theoretical recommendations in the documents and the actual experiences of healthcare professionals and cybersecurity experts, even though the document analysis and interview data highlight many of the same themes regarding the significance of cybersecurity in healthcare. The primary distinctions between the interview comments and the results of the ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism are discussed in this section.

- The Need for Sector-Specific Adaptations of the ECSF.

The requirement to modify the ECSF to meet the particular requirements of the healthcare industry is a significant inference from the combined findings. The thorough and systematic character of the ECSF, which is intended to be adaptable across industries, is highlighted by the document analysis. But healthcare experts have always emphasized the shortcomings of a general approach, saying that cybersecurity in the industry needs frameworks and training programs that are especially tailored to their operating reality.

This shows that while the ECSF provides a solid base, its efficacy in healthcare will depend on its ability to be tailored. To achieve wider acceptance in the industry, healthcare-specific training, examples, and modules that address the harmony between cybersecurity and clinical care may be crucial. If these modifications aren't made, healthcare professionals may view the ECSF as overly theoretical or unrealistic, which would reduce its effectiveness.

- Resource Allocation and Prioritization

There are also important ramifications for the discrepancy that exists between the framework's objectives and the actual resource limitations in the healthcare industry. The ECSF makes the assumption that businesses can commit significant financial and human resources to developing and retaining a staff with cybersecurity expertise. Interviews with cybersecurity specialists and healthcare professionals, however, show that many healthcare organizations are having trouble with underfunded IT departments and a shortage of specialized staff.

This discrepancy emphasizes the need for more scalable solutions that healthcare organizations with limited resources can adopt gradually. Rather than proposing large-scale overhauls, cybersecurity activities in healthcare may need to focus on essential, high-impact areas first, such as data protection and incident response, which are linked with the most pressing threats. Organizations with limited resources may find the ECSF easier to acquire and more attainable with this stepwise approach.

- Organizational Culture and Leadership Commitment

The integrated findings further highlight how crucial organizational culture and leadership are to the ECSF's successful implementation. The document emphasizes the need of leadership in raising cybersecurity awareness and bringing about change, but the interviews showed that there is a lot of opposition to change in healthcare settings. This cultural obstacle is not specific to cybersecurity; rather, it reflects a larger difficulty in implementing any non-clinical efforts in environments where the main goal is patient care.

This observation suggests that strong leadership buy-in and cultural change management techniques are necessary for the ECSF to take off in the healthcare industry. Instead of viewing cybersecurity as an afterthought, leaders in healthcare organizations need to aggressively push it as an essential component of patient care and safety. Furthermore, by promoting a collaborative culture between IT teams and clinical personnel, cybersecurity can be seen less as a stressful, stand-alone duty and more as an integral part of the larger goal of healthcare delivery.

- The Role of Continuous Training and Development

Both the document findings and interview data highlight the importance of continuous learning in the rapidly evolving field of cybersecurity. As part of its organized approach to developing a resilient workforce, the ECSF places a strong emphasis on continuous skill development and upskilling. In a similar vein, given the dynamic nature of the threat landscape, healthcare practitioners and cybersecurity specialists acknowledged the necessity of periodic updates to cybersecurity knowledge.

This mutual understanding emphasizes the necessity for healthcare institutions to have a long-term, proactive strategy for cybersecurity training. To stay up to date on new dangers and best practices, healthcare personnel, particularly clinical staff, need to participate in continuous learning instead of one-time training sessions. The gap between theory and practice could be reduced by incorporating cybersecurity awareness and skill development into routine operations through frequent workshops, simulations, and refresher courses.

- Implications for Regulatory Compliance and Patient Safety

According to the combined results, using the ECSF may improve patient safety as well as regulatory compliance. The framework offers a well-defined structure for matching responsibilities and abilities to legal mandates like the General Data Protection Regulation (GDPR). This is especially important in the healthcare industry because patient data is sensitive.

The ECSF could assist healthcare organizations in strengthening their compliance posture and lowering the risk of data breaches and penalties by standardizing cybersecurity roles and competences. Additionally, improving the cybersecurity competencies of medical staff members has a direct bearing on patient safety. Cyberattacks that jeopardize patient data or healthcare infrastructure may have fatal results.

As a result, enhanced cybersecurity capabilities—fueled by frameworks like the ECSF—are essential to guaranteeing patient safety and treatment in the digital era as well as being a regulatory concern.

- Bridging the Cybersecurity Skills Gap

The comprehensive findings also suggest that the ECSF could play a key role in closing the current cybersecurity skills gap in the healthcare industry. The interviews and document analysis both emphasize how hard it is to train clinical staff to be more cyber-aware and how hard it is to recruit skilled cybersecurity professionals in the healthcare industry. This gap may be closed by using the ECSF's role definitions and competences, which offer an organized approach to talent development in the industry.

The ECSF could be used by healthcare organizations to make training opportunities and career routes clearer for clinical staff and IT workers. Organizations should address the skills gap more methodically by matching recruitment tactics and training programs with the competences specified in the framework. This strategy/approach may help increase interest in cybersecurity careers by offering a clear career path within the healthcare industry.

Conclusion

The integration of interview data and document findings demonstrates the advantages and disadvantages of applying the ECSF to the healthcare industry. Although the framework provides a strong framework for addressing the development of cybersecurity skills, its practical use will necessitate customization to the unique requirements of healthcare organizations, as well as careful consideration of resource limitations, cultural obstacles, and ongoing training. The ECSF has the potential to significantly improve patient safety and

regulatory compliance by strengthening healthcare organizations' cybersecurity capabilities if these issues are resolved.

5.6 Recommendations for Practice:

To help with the successful implementation of the ECSF in healthcare settings, the following major suggestions are put forth based on the integration of interview data and document analysis:

Industry-Specific Personalization

Healthcare companies should modify the ECSF to fit the particular requirements of the industry, with an emphasis on duties pertaining to incident response and data protection. Enhancing the framework's relevance and impact will require tailoring it to healthcare-specific circumstances.

Set priorities. Crucial Positions

Healthcare organizations should focus on crucial cybersecurity positions, especially those that are directly in charge of protecting sensitive patient data, given their limited resources. A staged strategy that begins with the most important positions can guarantee that the few resources are allocated as effectively as possible.

Participation of Leadership

Encouraging cybersecurity measures requires the support of executives. Strategic planning should incorporate cybersecurity, with a focus on its importance for patient safety and operational resilience.

Interdepartmental Cooperation

Cybersecurity procedures will improve with IT and clinical professionals working together. Organizational resilience will be increased by encouraging shared responsibility across departments and integrating cybersecurity into healthcare operations.

Healthcare companies can advance cybersecurity by concentrating on these specific recommendations without adding undue strain to their current operations or resource pool. These steps will set the stage for the more in-depth tactics covered in the ensuing sections.

5.7 Implications for practice

The healthcare industry will be greatly impacted by the adoption of the European Cybersecurity Skills Framework (ECSF) in a number of important ways. These ramifications include improving cybersecurity knowledge and training, taking human factors into account, and making sure cybersecurity efforts are implemented and monitored successfully.

5.8 Enhancing Cybersecurity Awareness and Training

One of the most important conclusions drawn from the interviews and document analysis is the urgent need for thorough and ongoing training for healthcare personnel at all levels. While technological professionals must remain up to date with changing threats, frontline healthcare workers also need basic cybersecurity expertise, given the industry's vulnerability to social engineering attacks.

Cross-Training Programs: To make sure non-technical staff members are aware of their responsibilities in preserving security, hospitals and other healthcare facilities should create cross-functional training programs that integrate ECSF requirements.

Ongoing Education: Since cybersecurity threats are constantly changing, it is crucial that training programs are iterative and updated frequently to reflect these developments.

Practical examples specific to the healthcare industry, such safeguarding patient records and identifying phishing dangers, ought to be emphasized in this training.

5.9 Implementing the ECSF in Healthcare Settings

The responsibilities and skills of the framework must be modified to meet the unique requirements of healthcare organizations in order for the ECSF to be implemented in the field of medicine effectively.

Phased Implementation: Instead of implementing the ECSF in its whole all at once, healthcare organizations should give priority to essential positions first, such as data protection officers and incident response teams, and then progressively add other positions.

Combining with Current Compliance Frameworks: In order to provide a more seamless transition and match cybersecurity jobs with compliance standards, ECSF implementation can benefit from utilizing current regulatory requirements (such as GDPR and HIPAA) as a basis.

Healthcare organizations are able to reconcile their operational and financial limitations with the needs of cybersecurity thanks to this phased implementation.

5.10 Addressing the Human Factor in Cybersecurity

The interviews made clear that, especially in the healthcare industry, human mistake continues to be the primary source of security breaches. To address this, a cultural transformation is necessary in addition to technical training.

Encourage a Cybersecurity Culture: To truly integrate cybersecurity awareness into day-to-day operations, leadership must stress that all staff members have a shared responsibility for safeguarding patient data.

Psychological Security for Disclosure: Faster detection and reaction can be achieved by creating a non-punitive atmosphere where employees feel comfortable reporting any cybersecurity concerns.

Healthcare companies may drastically lower the number of breaches caused by human error by fostering an organizational culture that sees cybersecurity as an integral aspect of patient care.

5.11 Monitoring and Evaluation of Cybersecurity Initiatives

In order to determine whether cybersecurity activities are effective, ongoing monitoring and assessment are essential.

Performance Metrics: Healthcare companies should set up quantifiable KPIs, like post-training improvements, incident response times, and ECSF role-based competency adherence.

Iterative Improvement: To make sure that cybersecurity procedures and training materials are up to date with the latest threats and ECSF guidelines, regular audits should be carried out.

In an increasingly complex threat landscape, cybersecurity practices will remain relevant and strong thanks to this focus on continual development and data-driven modifications.

Conclusion:

The integration of the ECSF paper and qualitative interview data has implications for practice that underscore the importance of customized, ongoing, and contextually appropriate cybersecurity training in the healthcare industry. Healthcare companies may improve their cybersecurity resilience, safeguard private patient information, and make sure their employees are prepared to handle the constantly changing cybersecurity threats that the sector faces by implementing these practices.

5.12 Chapter summary

Using both document analysis and qualitative insights from interviews with cybersecurity experts and healthcare personnel, Chapter 4 offers a thorough analysis of how the European Cybersecurity Skills Framework (ECSF) has been integrated into the healthcare system. The chapter provides an overview of the state of cybersecurity in the healthcare industry, highlighting the obstacles, weaknesses, and possible advantages of using the ECSF to raise awareness and improve cybersecurity within the industry. The examination of the documents made clear how urgently healthcare needs established cybersecurity protocols. It demonstrated the particular difficulties faced by healthcare organizations, including protecting extremely private patient information, adhering to stringent laws like GDPR, and managing resource constraints that frequently make cybersecurity less important. As a fundamental tool in this investigation, the "ECHO Cyber-Skills Framework" provided insights into the possible alignment between ECSF competencies and the demands of the healthcare industry.

A practical viewpoint on these issues was offered by the interviews with healthcare professionals, who all agreed that healthcare organizations are now ill-prepared for significant cyberattacks. Healthcare experts, including Dasha, Felix, Manu, and Miia, underlined the need of combining cybersecurity needs with patient care goals/priorities. They voiced alarm about the current skills gap, pointing out that the majority of employees don't even know the basics of cybersecurity. They thought the ECSF may assist close this gap by offering a well-organized training and role-defining roadmap, but its effective implementation would need a large organizational commitment and resources. On the other hand, the interviews with cybersecurity specialists, such as Dorin, Simone, and Andreea, further validated the promise of the ECSF but stressed the technical hurdles of deploying such a framework in healthcare settings. They admitted that integrating a highly organized framework like the ECSF is made more difficult by the healthcare industry's reliance on outdated systems and lack of specialized cybersecurity staff. They did, however, also point out that the ECSF's precise definition of roles and capabilities might make it easier for healthcare companies to manage cybersecurity, hire expertise, and grow personnel.

The chapter also looked at significant similarities and differences between the information from the interviews and the document discoveries. Regarding the significance of a methodical approach to cybersecurity and the ECSF's function in filling up existing gaps, both sources were in agreement. On the ECSF's ease of implementation, experts in cybersecurity were more upbeat about its potential to simplify procedures, while healthcare professionals

remained dubious because of financial limitations, cultural resistance, and operational priorities that prioritized patient care.

A thorough discussion of the implications for practice was included in the chapter, which emphasized the necessity of implementing ECSF in healthcare through a staged method. This strategy entails giving top priority to crucial cybersecurity positions, creating cross-functional training curricula, and encouraging a cybersecurity culture in healthcare institutions. The human element was also noted as a major obstacle, and the necessity of ongoing education and a welcoming atmosphere for reporting cyber events were emphasized as crucial tactics for lowering errors.

Finally, recommendations for practice focused on practical activities that healthcare companies can take to strengthen their cybersecurity posture through the ECSF. These included encouraging leadership buy-in to develop a cybersecurity culture at all organizational levels, integrating the ECSF with current regulatory frameworks, and concentrating on ongoing monitoring and assessment of cybersecurity initiatives.

In conclusion, Chapter 4 provides a thorough overview of the situation of cybersecurity in the healthcare industry today and the possible outcomes of implementing the ECSF. In an increasingly digital healthcare environment, the ECSF provides a clear road ahead for strengthening cybersecurity competences, bridging the skills gap, and ultimately improving patient safety, even if there are still many obstacles to overcome, especially with regard to budget allocation and cultural adoption.

The results of this chapter indicate that, as healthcare organizations struggle with changing cyberthreats, formal frameworks such as the ECSF may be crucial in developing a workforce that is more cyberwar and robust, paving the way for further developments in healthcare cybersecurity.

6 Recommendations and Implications

This chapter presents the important recommendations resulting from the study’s results and their larger implications for practice, policy, and further research in the context of healthcare cybersecurity. This chapter offers practical solutions for resolving the current skills gap, enhancing cybersecurity resilience in healthcare organizations, and integrating the European Cybersecurity Skills Framework (ECSF) into healthcare settings, building on the analysis given in Chapter 4.

6.1 Enhancing Cybersecurity Awareness and Training

The interviews and document analysis revealed an important fact: healthcare organizations lacked cybersecurity knowledge and training. In order to tackle this, the subsequent suggestions are put forth:

Comprehensive Cybersecurity Training for Every Employee: Healthcare companies should implement cybersecurity training initiatives that are required for every employee. Programs like these need to be customized for different positions so that clinical and administrative personnel know the fundamentals of cybersecurity, such as how to spot phishing attempts, protect login passwords, and handle patient data safely.

Training Based on Roles and in Line with the ECSF: Develop training curricula that emphasize role-specific competencies and are based on the ECSF. For example, while healthcare professionals should concentrate on data protection and secure communication procedures, IT staff members should acquire extensive cybersecurity training.

Continuous Education and Skill Refreshment: Cybersecurity training shouldn't be a one-time thing because cyber dangers are always changing. Healthcare organizations should incorporate refresher courses and continuous learning into their training programs.

6.2 Implementing the ECSF in Healthcare Settings

The study highlights that implementing the ECSF in healthcare settings necessitates a planned and incremental approach to address resource constraints and operational complexity. It is advised that the following actions be taken for successful implementation:

Perform a Cybersecurity Workforce Gap Analysis: To find gaps in responsibilities and capabilities, healthcare organizations should evaluate their current cybersecurity workforce and compare it with the ECSF. This gap analysis will show which important responsibilities are missing and which ones require urgent attention.

Give High-Risk Areas Priority: High-risk areas, like incident response teams and data protection officers, should be the primary focus of the initial ECSF deployment. With this strategy, healthcare organizations may gradually extend the ECSF across all functions while safeguarding the most susceptible areas of their infrastructure.

Leadership Commitment and Resource Allocation: The ECSF cannot be implemented successfully without strong leadership support. Leaders in the healthcare industry need to understand the value of cybersecurity and commit the necessary funds and personnel to support ECSF-based projects. Clear communication on the benefits of cybersecurity can help develop a culture that emphasizes security.

Make Use of Alliances with Cybersecurity Professionals: To assist in navigating the challenges of ECSF implementation and ensuring alignment with best practices, healthcare organizations can work with outside cybersecurity experts, trade associations, and educational institutions.

6.3 Addressing the Human Factor in Cybersecurity

In the interviews, cybersecurity experts and healthcare professionals both emphasized that one of the weakest links in the cybersecurity chain is still the human component. In order to reduce this risk, healthcare institutions ought to:

Encourage a Culture of Cybersecurity Awareness: Foster an environment where all employees are accountable for cybersecurity, not only IT departments. Regular awareness campaigns, seminars, and interactive meetings that illustrate the practical effects of cyberthreats on patient care can accomplish this.

Promote the Reporting and Reaction of Incidents: Establish a culture of non-punitiveness to incentivize staff members to disclose possible cybersecurity incidents or errors. This will facilitate speedier cleanup and ultimately lower the number of unreported breaches.

Reduce the Risk of Human mistake: Human mistake is a frequent source of data breaches in the healthcare industry. By automating some security processes, such as routine updates, data encryption, and system access limits, you may reduce the chance of human error.

6.4 Monitoring and Evaluation of Cybersecurity Initiatives

Healthcare organizations need to create strong monitoring and evaluation mechanisms to guarantee the success of the ECSF deployment and other cybersecurity measures. Important suggestions consist of:

Clearly Identify Success Metrics: Specify metrics that will be used to assess the accomplishment of ECSF-based projects. The number of cybersecurity events, reaction times, and compliance rates in internal cybersecurity audits are a few examples of these measures.

Constant Monitoring and Adjustment: Healthcare institutions should keep a close eye on the development of their cybersecurity projects and make any required adjustments to their plans. Regular evaluations should be done to identify areas for improvement and guarantee that the organization remains responsive to evolving cyber threats.

Benchmarking Against Industry Standards: Healthcare organizations can assess the success of their activities and make sure they are keeping up with global cybersecurity trends by comparing their cybersecurity posture with industry benchmarks and best practices.

6.5 Recommendations for policy and research

The study identifies various policy and research implications in addition to offering helpful advice for healthcare organizations:

Policy Development for Healthcare-Specific Cybersecurity: Considering the particular difficulties associated with patient data protection, system integration, and regulatory compliance, policymakers want to think about creating standards for cybersecurity in the healthcare industry. These regulations ought to promote the use of ECSF-style frameworks by healthcare organizations and offer assistance with capacity-building programs.

Additional Study on the Use of ECSF in Healthcare: Future research should examine the long-term effects of ECSF deployment on workforce development, incident response, and patient data security, given the paucity of information on its acceptance in the healthcare industry. This study may offer insightful information for improving the framework and guaranteeing its suitability for the healthcare industry.

6.6 Chapter Summary

The study's conclusions are compiled in Chapter 5 and made into practical suggestions for improving cybersecurity in healthcare environments. These proposals center on enhancing cybersecurity education and awareness, putting the ECSF into practice, addressing human elements in security, and setting up efficient monitoring and assessment systems. The chapter also makes recommendations for future studies and policy creation to help healthcare organizations use organized cybersecurity frameworks like the ECSF. Healthcare companies may improve patient data protection, reduce cyber risks, and develop a workforce of cybersecurity professionals who are more resilient and skilled by tackling these issues.

Conclusions

The cybersecurity landscape within the healthcare sector is growing rapidly, as cyber threats become more complex, and the dangers associated with data breaches and system vulnerabilities increase. The present thesis has investigated the applicability and capacity of the European Cybersecurity Skills Framework (ECSF) to tackle the distinct cybersecurity predicaments encountered by healthcare establishments. This research has investigated the present level of cybersecurity skills, training, and workforce preparation within the healthcare sector, as well as the gaps that the ECSF may assist fill, using document analysis and interviews with both healthcare practitioners and cybersecurity specialists.

6.7 Addressing the Skills Gap in Healthcare Cybersecurity

This study's main finding is that there is a sizable cybersecurity skills gap in healthcare organizations. Dasha, Felix, Manu, and Miia were among the healthcare workers whose interviews indicated a general need for more organized cybersecurity training, particularly in the areas of data protection, incident response, and secure communication techniques. In a similar vein, cybersecurity specialists Dorin, Andreea, and Simone emphasized the difficulties healthcare companies encounter in attracting and keeping skilled cybersecurity personnel. According to the findings, the ECSF can offer a helpful framework for defining important cybersecurity roles and competences, allowing training initiatives and recruitment campaigns to be coordinated to close these skills gaps. Through the identification of crucial positions like security analysts, incident responders, and data protection officers and their mapping to certain competences, the ECSF may provide healthcare organizations with a well-defined route to building a workforce with enhanced cybersecurity capabilities and resilience. The report does acknowledge, though, that overcoming organizational, financial, and cultural obstacles will be necessary for the ECSF to be successfully implemented in the healthcare industry.

6.8 The Importance of Tailored Cybersecurity Training

This thesis also comes to the conclusion that cybersecurity education in the medical field has to be more ongoing and role specific. The interviews and document analysis made clear that cybersecurity training cannot be addressed by a one-size-fits-all strategy due to the wide range of needs among healthcare personnel. For example, IT workers need improved abilities in network security, encryption, and threat detection, while clinical staff needs more specialized training on protecting patient data and adhering to laws like GDPR.

The ECSF connects certain job responsibilities with the required skills and knowledge, offering an organized framework to support these customized training initiatives. This would lessen the likelihood of human error—a common element in healthcare data breaches—while also raising the general level of cybersecurity awareness inside healthcare organizations and fostering a security-conscious culture.

6.9 The ECSF as a Catalyst for Organizational Change

According to the report, the ECSF has the ability to spur organizational change in the healthcare industry, especially when it comes to enhancing workforce development and cybersecurity governance. Healthcare organizations can undertake thorough skills evaluations, identify gaps, and prioritize areas for improvement with the help of the ECSF, which provides a standardized framework. By doing this, you can make sure that important

cybersecurity positions are filled and that employees have the necessary training to handle the ever-changing cyber threat scenario.

However, healthcare officials must acknowledge the significance of cybersecurity and pledge to provide adequate funding for its implementation if they want the ECSF to bring about significant change. The financial and operational barriers that have historically hampered cybersecurity initiatives in the healthcare industry will need to be overcome, along with a clear plan for integrating ECSF into current operations. Strong leadership buy-in is also necessary.

6.10 Implications for Policy and Research

The study has significant ramifications for future research and policy. Given the particular regulatory challenges faced by the healthcare industry and the sensitivity of patient data, policymakers ought to think about creating rules tailored to the industry that integrate the ECSF. Funding opportunities or grants for healthcare organizations may also be able to assist in addressing the financial limitations that have hindered the implementation of cybersecurity frameworks such as the ECSF.

Subsequent investigations ought to delve into the enduring consequences of ECSF deployment in the healthcare sector, with particular attention to its impact on cybersecurity resilience, workforce development, and patient data protection. It would also be advantageous to conduct study on how well-attended, role-based training programs may raise cybersecurity awareness and lower the frequency of data breaches.

6.11 Final Thoughts:

This thesis concludes by highlighting the ECSF's enormous potential to help healthcare organizations overcome their cybersecurity obstacles. The ECSF can assist in bridging the skills gap, enhancing training initiatives, and promoting a cybersecurity-aware culture by standardizing roles and competencies. Although there are still implementation and resource allocation issues to be resolved, the ECSF remains a useful tool for healthcare organizations looking to strengthen their overall cybersecurity posture and safeguard patient data.

The use of the ECSF in the healthcare industry may result in a workforce that is more adaptable and able to counter new threats, eventually protecting patient data and healthcare systems. The research's conclusions provide legislators and healthcare organizations with a solid platform on which to build when it comes to strengthening cybersecurity, protecting private data, and boosting public confidence in the industry.

Additionally, I am honored to share that this thesis has been selected as a paper to be presented at the DIGILIENCE conference on digital resilience, bringing its findings to a broader audience of cybersecurity experts and industry leaders.

References

Alotaibi, S. & Wald, M. 2014. Cyber Security in Healthcare: A Review of the Challenges and Solutions. Journal of Health Informatics, 10(3), 1-12. doi: 10.2196/21747

Beltempo, E., Karvonen, J. & Rajamäki, J. 2021. ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism. Proceedings of the 21st European Conference on Cyber Warfare and Security, 21(1), 1-30. doi: 10.34190/eccws.21.1.274

Beltempo, E & Rajamäki, J. 2024. Implementation of the ECHO Cyber Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities. Information & Security: An International Journal, 55(3), 236-244. doi: 10.11610/isij.5517

Cybersecurity and Infrastructure Security Agency (CISA). 2019. Cyber Essentials. Accessed 23 July 2024. https://www.cisa.gov/cyber-essentials

European Union Agency for Cybersecurity (ENISA). 2020. Cybersecurity Skills Development in the EU. Accessed 23 July 2024. https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu

Hevner, A. & Chatterjee, S. 2010. Design Research in Information Systems: Theory and Practice. New York: Springer.

Janczewski, L. J. & Fu, L. 2010. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions. Hershey, PA: IGI Global.

Joint Task Force on Cybersecurity Education. 2017. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. ACM, IEEE Computer Society, AIS SIGSEC, IFIP WG 11.8.

Kadivar, A. 2020. Assessing the Impact of Cybersecurity Training Programs in Healthcare Organizations. International Journal of Healthcare Management, 13(4), 1-14.

Kruse, C. S., Frederick, B., Jacobson, T. & Monticone, D. K. 2017. Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. Technology and Health Care, 25(1), 1-10.

National Institute of Standards and Technology (NIST). 2018. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Accessed 23 July 2024. http://www.nist.gov/cyberframework

Rajamäki, J. & Lahdenperä, J. 2019. Governance and Management Information System for Cybersecurity Centres and Competence Hubs. Espoo: Laurea University of Applied Sciences.

Rajaraman, V. & Mukherjee, S. 2015. Research Methodology in Information Technology. New Delhi: McGraw-Hill Education.

Sittig, D. F. & Singh, H. 2016. A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Applied Clinical Informatics, 7(2), 1-12.

Smith, A. & Brown, J. 2020. Cybersecurity Challenges in Medical Tourism. International Journal of Medical Informatics, 134, 1-8.

Stolterman, E. & Fors, A. C. 2004. Information Technology and the Good Life. In: J. M. Carroll, ed. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage. 163-170.

Takabi, H., Joshi, J. B. D. & Ahn, G. J., 2010. Security and Privacy Challenges in Cloud Computing Environments. IEEE Security & Privacy, 8(6), 24-31.

Tables

Appendices

Appendix 1: Questions for stakeholders and healthcare/cybersecurity professionals:

Interviews with Healthcare professionals:

1. General Awareness and Perceptions of Cybersecurity

- How would you describe your current understanding of cybersecurity threats specific to the healthcare industry?
- Can you share any experiences you have had with cybersecurity incidents within your organization?
- In your opinion, how prepared is your organization to handle a cybersecurity breach?

2. Cyber-Skills and Training Needs

- What are the key cybersecurity skills that you believe are most critical for healthcare professionals in your role?
- How would you assess the current level of cybersecurity training available to you and your colleagues?
- What improvements, if any, would you suggest for the cybersecurity training programs currently offered in your organization?

3. Familiarity with the ECSF

- Have you heard of the European Cybersecurity Skills Framework (ECSF)? If so, what is your understanding of it?
- Do you think the ECSF could be relevant or beneficial in addressing the cybersecurity challenges faced by your organization? Why or why not?

4. Applicability and Implementation of ECSF

- How do you think the ECSF could be adapted to suit the specific needs of your healthcare organization?
- What challenges do you foresee in implementing a framework like the ECSF in your daily operations?
- In your opinion, what would be the most effective way to integrate ECSF-based training into the existing training programs?

5. Impact on Organizational Cybersecurity Posture

- What changes do you think would be necessary within your organization to successfully implement the ECSF?
- How do you think the implementation of the ECSF could influence the overall cybersecurity posture of your organization?
- What metrics would you suggest using to measure the success of ECSF implementation in improving cybersecurity?

6. General Feedback and Suggestions

- Are there any additional thoughts or concerns you have regarding cybersecurity in the healthcare sector that we have not discussed?
- What would be your top recommendation to policymakers or training providers for improving cybersecurity skills and preparedness in healthcare?

Post-Implementation Survey – FOR FUTURE THESES

1. Impact on Knowledge and Skills

- On a scale of 1-10, how would you rate your current knowledge of cybersecurity threats and vulnerabilities?
  Scale: 1 (Very Low) to 10 (Very High)
- How confident are you now in your ability to respond to a cybersecurity incident compared to before the ECSF implementation?

  Options: Much More Confident, More Confident, Same, Less Confident, Much less Confident
- Which cybersecurity skills have improved the most since the ECSF training?

  Options (select all that apply): Incident Response, Threat Analysis, Risk

  Management, Network Security, Data Protection, Other (please specify)

2. Effectiveness of Training

- How effective was the ECSF training in enhancing your cybersecurity skills?

  Options: Very effective, Effective, Somewhat effective, Not effective

- How applicable were the ECSF training materials to your daily work?

  Options: Very applicable, Somewhat applicable, Not applicable

3. Behavioral and Organizational Changes

- How often do you now follow cybersecurity news and updates compared to before the ECSF training?

  Options: More frequently, Same, Less frequently

- Has your organization increased the frequency of cybersecurity drills or exercises since implementing the ECSF?

  Options: Yes, No

- How well do you now understand your organization's cybersecurity policies and procedures compared to before the ECSF training?

  Options: Much better, Somewhat better, Same, Worse

Additional Questions for Further Insight

1. Training Delivery and Materials

- Which part of the ECSF training did you find most engaging or useful?
  Open-ended

- Were there any aspects of the training that you found challenging or less effective? If so, please explain.
  Open-ended

- What additional topics or skills would you like to see included in future ECSF training sessions?
  Open-ended

2. Overall Experience and Feedback

- How satisfied are you with the ECSF training overall?
  Options: Very Satisfied, Satisfied, Neutral, Dissatisfied, Very Dissatisfied
- Would you recommend the ECSF training to your colleagues?
  Options: Yes, No
- Do you have any additional comments or suggestions for improving the ECSF training?
  Open-ended

Interviews:

For Key Stakeholders (e.g., Cybersecurity Specialists, IT Managers, Organizational Leaders)
Interview Questions for Cybersecurity Experts on ECSF Implementation

1. General Understanding of ECSF:

- Can you describe your current understanding of the European Cybersecurity Skills Framework (ECSF)?

- What do you see as the main goals and objectives of the ECSF in addressing cybersecurity challenges?

2. Relevance to Healthcare:

- In your opinion, how applicable is the ECSF to addressing the specific cybersecurity needs of the healthcare sector?

- Do you believe healthcare organizations are currently well-prepared to adopt the ECSF? Why or why not?

3. Perceived Benefits of ECSF:

- What are the primary benefits you believe the ECSF can bring to organizations in general, and to healthcare organizations specifically?

- How could the ECSF help in improving cybersecurity skills and awareness within healthcare?

4. Challenges in Implementation:

- What do you see as the key challenges in implementing the ECSF in organizations that have not yet adopted it, particularly in healthcare?

- In your experience, what are the typical barriers (e.g., financial, organizational, cultural) that could hinder the successful implementation of the ECSF?

5. Potential Strategies for Adoption:

- How do you think the ECSF could be effectively introduced into a healthcare organization's existing cybersecurity strategies and training programs?

- What steps would you recommend for an organization looking to adopt the ECSF for the first time?

6. Metrics and Evaluation:

- How would you suggest measuring the success of ECSF implementation in improving an organization’s overall cybersecurity posture?

- What key performance indicators (KPIs) or metrics would be most relevant in tracking the progress and effectiveness of ECSF-based training?

7. Lessons from Other Frameworks:

- Based on your knowledge of other cybersecurity frameworks (e.g., NIST, ISO), how does the ECSF compare? Are there any best practices from those frameworks that could be applied to ECSF implementation in healthcare?

8. Long-Term Impact:

- What do you foresee as the long-term impact of widespread ECSF adoption on the cybersecurity workforce and skills development in healthcare?

- How could the ECSF influence the overall cybersecurity landscape if more healthcare organizations were to implement it?

9. General Feedback:

- Are there any improvements or modifications you would recommend for the ECSF to make it more effective or easier to implement in healthcare settings?

- Do you have any additional thoughts or suggestions on the future of cybersecurity skills development in healthcare?

Appendix 2: ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism

ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism

Eleonora Beltempo, Jussi Karvonen and Jyri Rajamäki
Laurea University of Applied Sciences, Finland
eleonora.beltempo@student.laurea.fi
jussi.karvonen@student.laurea.fi
jyri.rajamaki@laurea.fi

Abstract: The ECHO Horizon 2020 Project develops a European cybersecurity ecosystem. One of its assets is the ECHO Cyber-Skills Framework (ECSF). This work in progress paper aims to improve cybersecurity education and training in the healthcare industry including health and medical tourism. First, this paper finds out how ECSF will benefit the healthcare sector regarding cyber-skills and awareness in order to create a more secure information technology (IT) environment when it comes to healthcare. Based on these findings, the paper proposes a strategy to adopt ECSF in order to improve the existing state of IT security and increase worker and management awareness and understanding. Finally, the paper looks at ECSF's possibilities to be a tool for education and training in health and medical tourism.

Keywords: ECHO project, cyber-skills framework, cybersecurity, health and medical tourism

1. Introduction

ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) H2020 Project develops a European Cybersecurity ecosystem, to support secure cooperation and development of the European market, as well as to protect the citizens of the European Union against cyber threats and incidents (ECHO, 2021). The ECHO Cyber-Skills Framework (ECSF) aims at providing a foundation and practical guidelines for better defining the knowledge and skill gaps in the healthcare, transport and energy industries as well as for the development of cybersecurity education and training programs that address those gaps. The ECSF serves as an inventory tool, providing methodological guidelines for the design, update and development of training programs and curricula, both within the framework of the ECHO project, as well as within the scope of relevant EU initiatives, as a common reference model for capacity building (Varbanov, 2021). Figure 1 presents the main components of the ECSF.

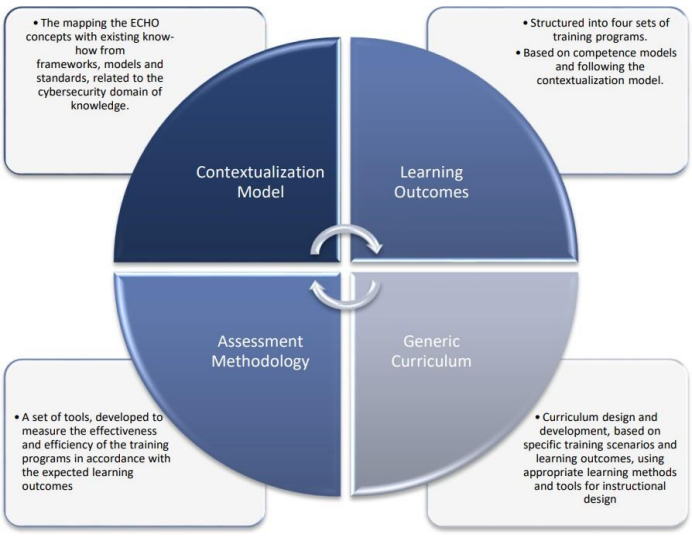

Figure 1: Main Components of the ECSF (Varbanov, 2021)

This work in progress paper finds out the possibilities of utilizing the ECSF in the healthcare industry including health and medical tourism. Although the concept of health and medical tourism is widespread, also the following terms are used when speaking of travel-based health-related activities: health tourism, medical

tourism, wellness tourism, spa tourism and medical travel (Romanova, Vetitnev & Dimanche, 2015). Figure 2 illustrates different types of health and medical tourism.

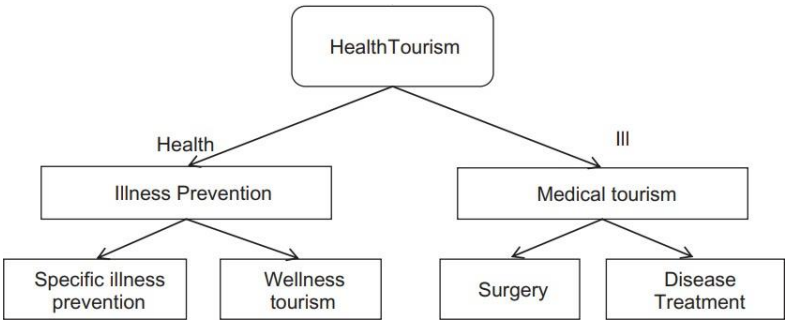

Figure 2: Typology of Health and Medical Tourism (adapted from Romanova et. al, 2015)

This study starts by answering three research questions to see how ECHO and the healthcare sector would both benefit from the possible implementation of ECSF in the healthcare sector:

- How ECHO cyber-skills framework would be beneficial for healthcare?
- What is the best way to implement the ECHO cyber-skills framework into the healthcare sector?
- How the ECHO network will benefit from this implementation.

After answering these questions, this paper combines the findings and proposes how to use ECSF in health and medical tourism.

1. Findings

From our study, we combine the information that has been gathered with the help of our research questions. We figure out what are the problems within healthcare sectors organizations, what is the best way to implement the ECSF, and how can ECHO benefit from the possible implementation of ECSF into the healthcare sector. We also search that if there are any public cyber-skills frameworks that we could possibly reference to see if there is an increase in employees' skills and awareness.

1.1 ECSF benefits for healthcare

To find out about how a cyber-skills framework could be beneficial for healthcare we must first find out about the gaps in healthcare sectors' cyber-skills, knowledge, and the state of awareness about possible threats. Secondly, we have to find out is there any kind of basic training for healthcare sectors staff regarding cyber-skills and knowledge.

The current gaps in the healthcare sector's cyber-skills, knowledge, and awareness are quite huge. According to IONOS Cloud, 37% of healthcare IT employees say their organization is at risk of security because of skills gaps in the field (Mageit, 2021). IONOS Cloud's report continues that 39% of IT professionals in the healthcare sector state that they have gaps in data protection, 25% say they are not adhering to the legislation, and 21% do not follow proper data protection measures (Mageit, 2021). These gaps and threats caused by them can lead to attackers leaking sensitive information about patients which can cause risks for health and safety, and not using critical medical services because they can be affected by unauthorized control (Varbanov, 2021).

The healthcare sector includes private and public hospitals, as well as the companies that manufacture medical devices and the pharmaceutical industry (Varbanov, 2021). The assets that ECHO Cyber-skills Framework focuses on an organizational level are the ICT assets of the company and the professionals who are responsible for making sure the ICT assets are secured. Data and information are the most important assets in a healthcare organization. From the operational technology standpoint for the healthcare sector, devices and equipment that produce data that can be exchanged in and outside the organization are key assets.

From these findings, we can determine that using ECSF would increase cyber-skills and awareness within healthcare sectors employees and lower the risk of the organizations within the sector being attacked or having a close call. Organizations can also adapt to the situations from learning from previous incidents.

1.1 Implementation of ECHO cyber-skills framework to the healthcare sector

The ECHO Multi-sector Assessment Framework (E-MAF) supports risk management decision-making, i.e. it provides a framework for understanding cyber risks and, on that basis, supports decisions on where to invest human, technological and financial resources to reduce those risks to an acceptable degree (Tagarev, Pappalardo & Stoianov, 2020). To properly implement ECSF into the healthcare sector, E-MAF has to be used to address the needs and gaps. E-MAF provides the ECSF the ways to analyze challenges and opportunities, and how to assist the development of cybersecurity technology roadmaps. Using E-MAF provides educational portfolios and training programs, and a unified definition of what skills and qualifications are needed. E-MAF includes the ECHO Security Control, which provides more specific measures divided into four different levels: Organizational, Technical, Functional, and Non-Functional. Organizational implies what the cybersecurity professionals should be able to perform, including the application of security controls, mitigation, and countermeasures. Technical implies the skills and competencies professionals must have in able to demonstrate, which includes security controls. Functional implies sector-specific knowledge the professionals must demonstrate to complete modules or programs. Non-Functional implies knowledge that carries to achieving organizational, technical, and learning objectives within the organization.

There is a lack of publicly used frameworks that focus on cyber-skills training. Hübner et al. (2019) presents the TIGER International Recommendation Framework of Core Competencies in Health Informatics 2.0. Their framework is meant to augment the scope from nursing towards a series of six other professional roles, i.e. direct patient care, health information management, executives, chief information officers, engineers and health IT specialists and researchers and educators. Another example of existing frameworks is the NICE Framework (National Institute of Standards and Technology, 2021), but it is not entirely focused on training cyber-skills and increasing awareness. It does enable cybersecurity education and training, but it is more focused on developing and supporting the workforce so they are capable of meeting cybersecurity needs. The NICE Workforce Framework for Cybersecurity is a good example when providing information about what the employees need to and how to continuously describe learner capabilities. The Frameworks benefits include, for example, enhancing employee skills, understanding needs and skills gaps in the workforce, and hiring the right people for the job, when ECSF wants to train the current employees of the organization to identify and act accordingly in situations where the risk of incidents happening regarding cybersecurity are possible.

Considering how various it is the sector regarding healthcare, a slow implementation based on staff training is essential to guarantee the success of the framework. The continuous improvement of the courses and the new tools that ECHO will develop accordingly will ensure a safe and secure environment for both the staff and the customers.

1.2 How the ECHO network will benefit from this implementation?

This study aims to find out how the ECHO network would benefit from the possible implementation of ECSF in the healthcare sector. From the possible implementation of ECSF in the healthcare sector, ECHO would form a possibly long-lasting partnership with healthcare sectors organizations. Also, from this implementation, ECHO gives themselves information and data to develop more not just with ECSF, but in many more subjects. From the implementation of ECSF into the healthcare sector, ECHO could open doors to even more sectors to produce and implement different frameworks and tools. All of these things mentioned before would let ECHO grow more itself. ECHO would also be a big part of the digitalization of the healthcare sector within the EU.

2. ECSF as a tool in education and training in health and medical tourism

The purpose of medical tourism is to go to another country for medical procedures, for example, receive treatment for a condition, or to seek enhancement. The motivation for this tourism usually is a lower cost of care or higher quality care. These activities usually are reactive to illnesses that are medically necessary or overseen by a doctor (Global Wellness Institute, 2021).

Using ECSF as a tool in education and training in health and wellness tourism would be limited to EU member states. The European Commission (2021) adopted a Recommendation on a European electronic health record exchange to make the flow of Protected Health Information (PHI) of European citizens more quickly to access and share. European Commission also mentions in the article, that ensuring citizens secure access to their data develops the transformation of health and care even more digital. Using ECSF as a part of making sure the secure access and transformation of PHI of European citizens would be a tremendous thing for both EU and ECHO. Implementing ECSF as a part of the EU member states healthcare framework would secure the availability and transformation of PHI, while also ensuring the constant training and development of cyber-skills and awareness of healthcare sectors employees.

1. Discussion

Free movement of people is one of the cornerstones of the European Union. According to the Directive on Cross-Border Healthcare, which has been implemented in the entirety of the EU since 2013 for European citizens, no matter where they live, they have the right to choose where to receive medical treatment across the EU and to be compensated for it. However, in order to secure the above-mentioned rights and unleash the potential of cross-border healthcare exchange, new solutions are needed to secure the storage and cross-border exchange of health data. After the revelations of Edgar Snowden, it is more probable that widely used closed-source security solutions have serious defects and intentionally planted backdoors. It is widely accepted that real information security can increasingly be based on the openness and transparency of the security solution and the secrecy of its encryption keys.

The healthcare sector benefits from using ECSF could be increasing awareness about possible threats, their capabilities on how to work with IT devices without causing possible incidents, and constantly adapting and learning from possible threats. However, due to differences between countries, implementing a unified cyber-skills framework might be incompatible with different nations, but as Nurse, Adamos & Di Franco (2021) mentions in their report about the European cybersecurity skills framework, forming a unified framework that would take into account the needs of EU and their member states is vital for going even further in Europe's digital future.

Acknowledgements

This work was supported by the ECHO project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no.830943.

References

ECHO (2021). *Project summary*, [online], https://echonetwork.eu/project-summary/

European Commission (2021). *Exchange of electronic health records across the EU*, [online], 31st August 2021, https://digital-strategy.ec.europa.eu/en/policies/electronic-health-records

Global Wellness Institute (2021). *Wellness Tourism,* [online], https://globalwellnessinstitute.org/what-is-wellness/what-is-wellness-tourism/

Hübner, U., Thye, J., Shaw, T., Elias, B., Egbert, N., Saranto, K., Babitsch, B., Procter, P. and Ball, M. (2019). 'Towards the TIGER International Framework for Recommendations of Core Competencies in Health Informatics 2.0: Extending the Scope and the Roles', *Studies in Health Technology and Informatics*, Volume 264: MEDINFO 2019: Health and Wellbeing e-Networks for All

Mageit, S. (2021). 'Skills gap in healthcare IT industry causes security threats, according to new report', *Healthcare IT News*, 16th September 2021. https://www.healthcareitnews.com/news/emea/skills-gap-healthcare-it-industry-cause-security-threats-according-new-report

National Institute of Standards and Technology (2021). *Workforce Framework for Cybersecurity (NICE Framework),* [online], NIST Special Publication 800-181. https://www.nist.gov/system/files/documents/2021/05/05/NICE%20Framework%20%28NIST%20SP%20800-181%29_one-pager_508Compliant.pdf

Nurse, J., Adamos, K. and Di Franco, F. (2021). *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, European Union Agency for Cybersecurity (ENISA). DOI: 10.2824/033355

Romanova, G., Vetitnev, A. and Dimanche, F. (2015). 'Health and Wellness Tourism', In F. Dimanche and L. Andrades (Eds.) *Tourism in Russia: A Management Handbook*, Emerald, pp.231-287

Tagarev, T., Pappalardo, M, and Stoianov. N. (2020). 'A Logical Model for Multi-Sector Cyber Risk Management', *Information & Security: An International Journal* 47, no. 1, pp. 13-26. https://doi.org/10.11610/isij.4701

Varbanov, P. (2021). *D2.6 ECHO Cyberskills Framework,* [online], https://echonetwork.eu/wp-content/uploads/2021/03/ECHO_D2.6_Cyberskills-Framework.pdf

Appendix 3: Implementation of the ECHO Cyber-Skills Framework in the CyberSecPro Project: Enhancing Cybersecurity Capabilities

Abstract:
Cybersecurity has become a critical concern for many industries, particularly in sectors that handle sensitive data and provide essential services. The healthcare industry is one such sector, where the reliance on digital technologies and interconnected systems exposes institutions to a wide range of cyber threats. These threats, including ransomware, data breaches, and malicious attacks, can severely compromise patient safety, disrupt services, and erode public trust. The ECHO Cyber-Skills Framework (ECSF) is designed to address these challenges by providing a structured approach to enhancing the cybersecurity skills and knowledge of healthcare professionals. By focusing on key competencies such as incident response, risk management, and regulatory compliance, the ECSF seeks to close critical skill gaps in healthcare cybersecurity.