Information & Security

E. Beltempo & J. Rajamäki
vol. 55, no. 3 (2024): 236-244
https://doi.org/10.11610/isij.5517

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

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

*Eleonore Beltempo* (✉) *and Jyri Rajamäki*

*Laurea University of Applied Sciences, Espoo, Finland*
*http://laurea.fi*

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 (ECHO CSF) 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 ECHO CSF seeks to close critical skill gaps in healthcare cybersecurity.

ARTICLE INFO:

RECEIVED: 04 SEP 2024
REVISED: 26 OCT 2024
ONLINE: 01 NOV 2024

KEYWORDS:

ECHO Cyber Skills Framework, ECSF, CyberSecPro project, cybersecurity education, healthcare cyber-security



## Introduction

Cybersecurity has become a critical concern for sectors dealing with sensitive data, particularly in healthcare, which is increasingly targeted by cyberattacks due to its reliance on digital systems. Healthcare organizations handle sensitive patient data, making them vulnerable to cyber threats such as data breaches and ransomware attacks. The ECHO Cyber Skills Framework (ECHO CSF) aims to

✉ E-mail: Eleonora.Beltempo@student.laurea.fi

address the significant cybersecurity skills gap in industries like healthcare by providing structured guidelines for training and skill development. This paper investigates the ECHO CSF's application within the CyberSecPro project, focusing on its potential to enhance cybersecurity capabilities in the healthcare sector.

The CyberSecPro project's effective use of the ECHO CSF could serve as a model for other industries, highlighting the significance of a flexible and cooperative approach to cybersecurity education and training.

## Methods

This study followed a structured qualitative methodology, guided by the ECHO CSF, to assess cybersecurity capabilities in the healthcare sector. The data collection methods included semi-structured interviews with healthcare professionals and a comprehensive document analysis of the ECHO project's cybersecurity frameworks. The ECHO CSF was used as a framework to structure the interview questions, focusing on competencies such as incident response, threat detection, and risk management. Data from the interviews was coded and thematically analyzed to identify key challenges and areas for improvement.

*Study Explanation:* Participants were thoroughly informed about the research goals, methods, potential risks, and benefits. This included detailed information on the objectives of the study, the extent of their participation, and the expected outcomes.

*Data Collection:* Data was gathered through a combination of literature review, interviews, and analysis of existing cybersecurity frameworks within healthcare organizations. This multi-faceted approach ensured a robust and comprehensive dataset.

*Data Analysis:* The collected data was systematically analyzed to identify key trends, challenges, and opportunities in enhancing cybersecurity skills and practices in healthcare. Statistical tools and qualitative analysis methods were employed to ensure the reliability and validity of the findings.

*Ethical Considerations:* All research involving human subjects adhered to strict ethical guidelines. Participants provided informed consent, and their privacy and confidentiality were maintained throughout the study.

*Methodological Rigor:* The study followed the guidelines of the European cybersecurity skills framework to ensure methodological rigor. Training programs were designed, implemented, and evaluated systematically to assess their effectiveness in improving cybersecurity skills.

## Literature review

### *Introduction to Cybersecurity in Healthcare*

Cybersecurity threats in healthcare are well-documented in the literature, with phishing scams, ransomware attacks, and data breaches identified as the most common risks. These threats not only endanger patient safety but also compromise data integrity and disrupt the continuity of healthcare services. According

to Kruse et al. (2017),[1] human error is the leading cause of cybersecurity incidents in healthcare, with a majority of data breaches caused by insufficient staff training and awareness.

The *National Institute of Standards and Technology's (NIST) Cybersecurity Framework*[2] provides a foundational guide for improving critical infrastructure cybersecurity, including healthcare. The *European Cybersecurity Skills Framework (ECSF)*[3] developed by ENISA, emphasizes a similar approach, specifically addressing the skills required to manage cybersecurity threats in industries like healthcare. Other notable frameworks include the *TIGER International Framework*,[4] which focuses on cybersecurity skills development in health informatics. These frameworks aim to standardize the training and development of cybersecurity professionals to address the specific risks faced by healthcare organizations.

The ECHO CSF, as applied in this study, builds on these existing frameworks by focusing on sector-specific competencies, such as data security, incident response, and threat intelligence. This structured approach to cybersecurity education is essential for improving the overall security posture of healthcare organizations.[5]

### *Introduction to Cybersecurity in Healthcare*

The significance of cybersecurity skills and training has increased due to the growing dependence of numerous sectors on digital technologies. This is especially necessary in the healthcare industry because of the sensitive data and vital services that are offered. A strong defense plan against changing cyber threats must include cybersecurity expertise and training.[6]

### *The Need for Cyber-Skills in Healthcare*

Healthcare companies have cybersecurity challenges because of their intricately linked systems. New risks have been brought about by the digitization of medical records, telemedicine services, and networked medical devices. The healthcare industry needs workers with the most recent cybersecurity skills to safeguard patient data and guarantee the availability of healthcare services as cyber threats grow more complex. Studies show that human factors, such as inadequate staff training and awareness, account for most healthcare data breaches.[7] To reduce these risks, it is essential to invest in ongoing cybersecurity education and training.

### *Cyber-Skills Training Programs*

Comprehensive training programs spanning a wide variety of topics, from basic awareness to sophisticated technical abilities, are necessary for improving cybersecurity skills. Training curricula that are effective should be customized to the unique requirements of the company and the roles that its workers play. This entails being aware of the various dangers they could encounter, the weaknesses in their systems, and the most effective ways to reduce the risks. The value of practical exercises and hands-on training in cybersecurity education has

been emphasized by numerous research. Participants' comprehension of the consequences of their actions and their capacity to react to real-world occurrences are enhanced by simulated surroundings and real-world scenarios.[8]

### *Existing Cyber-Skills Frameworks*

Several cyber-skills frameworks have been established to guide the development and execution of effective training programs across various industries. These frameworks offer structured methods for identifying the required knowledge and competencies needed for different roles within organizations, including healthcare.

The *NICE Cybersecurity Workforce Framework*[9] is a leading example of such a framework. It systematically classifies and characterizes cybersecurity job roles, aligning them with the necessary skills and competencies. The relevance of NICE to healthcare lies in its ability to provide clear role definitions, which are critical in an industry where data protection and incident response are paramount. Healthcare organizations can utilize the NICE framework to identify existing gaps in their cybersecurity workforce, particularly in areas such as risk management and compliance, and develop tailored training programs to address these needs.

The TIGER International Recommendation Framework of Core Competencies in Health Informatics[10] is another significant framework, particularly in the healthcare sector. It emphasizes the interdisciplinary nature of cybersecurity in healthcare, focusing on the need for collaboration between IT professionals and healthcare providers TIGER's approach to health informatics competencies is especially relevant when implementing ECHO CSF, as it bridges the gap between clinical knowledge and cybersecurity expertise. By integrating TIGER into the ECHO CSF, healthcare organizations can ensure that both technical and non-technical staff are equipped to handle the complex cybersecurity challenges they face.

By highlighting NICE and TIGER, this paper underscores the importance of adopting frameworks that address the sector-specific needs of healthcare. Both frameworks provide valuable lessons that complement the ECHO CSF's focus on building targeted, role-based cybersecurity skills and enhancing collaboration between IT and healthcare professionals.

### *Relevance of ECHO CSF in Healthcare*

The healthcare industry can benefit greatly from the ECHO Cyber-Skills Framework because of its all-encompassing approach to detecting and filling skill gaps. The ECHO CSF seeks to improve healthcare professionals' cybersecurity knowledge and skills by offering methodological guidelines for creating, updating, and executing training programs.[7]

The ECHO CSF's emphasis on individualized instruction and ongoing professional growth is a good fit for the demands of the healthcare industry. By putting it into practice, healthcare organizations may strengthen their cybersecurity

posture and become more equipped to deal with the particular challenges and risks that exist in their setting.

### *Implementation of ECHO CSF 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 ECHO CSF. To do this, a comprehensive evaluation of present skill levels must be carried out to identify any gaps and create training plans that fill them. According to Williams et al.,[11] 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 ECHO CSF promotes these values.

### *Literature Review Summary*

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 ECHO CSF, TIGER, and NICE offer useful guidance for designing training initiatives. In particular, the ECHO CSF provides a thorough and customised approach to improving cybersecurity skills in the healthcare industry, taking into account the particular needs and challenges of this field.

## Interview Findings

Four healthcare professionals were interviewed: 'Felix,' 'Dasha,' 'Miia,' and 'Antti.' The interviews were designed to cover several key areas, including cybersecurity awareness, training practices, and the applicability of the ECHO CSF.

- Felix noted that while his organization provides a basic introductory course for new employees, it lacks ongoing, specialized training. This reflects a gap in addressing advanced cybersecurity threats such as phishing and ransomware, which are key areas covered under the ECHO CSF's competencies in threat intelligence and incident response.
- Miia expressed concerns about the limited scope of data protection training, particularly around patient data security, which aligns with the ECHO CSF's focus on data security and privacy competencies. She highlighted the need for more comprehensive training in these areas to protect sensitive patient information.
- Dasha highlighted that her organization offers no specialized cybersecurity training, leaving the staff unprepared for specific threats. This indicates a clear gap in the implementation of the ECHO CSF's role-based training modules, which are designed to ensure that healthcare professionals, regardless of their technical role, are equipped to handle sector-specific cybersecurity challenges.
- Antti emphasized the importance of cross-functional training, where both clinical and non-clinical staff are educated on cybersecurity risks. This aligns

with the ECHO CSF's focus on developing comprehensive skills across different roles, ensuring that all staff members are aware of and capable of mitigating cybersecurity risks in their daily tasks, which reflects the ECHO CSF's emphasis on security awareness and collaboration.

### *General Awareness and Perceptions of Cybersecurity*

Given the possible hazards involved in handling sensitive patient data, all three interviewees recognized the significance of cybersecurity in the healthcare sector. Felix and Miia emphasized the risks of losing patient data access and the sensitive nature of the information, which could result in extortion or other nefarious behaviour. Dasha underlined the harm that disclosures of private data pose overall.

The individuals' level of awareness of the risks varied, notwithstanding their broad awareness. Felix said he was only vaguely aware of cybersecurity, but Miia pointed out specific dangers, including program crashes and data theft. This shows that although healthcare workers view cybersecurity as a crucial problem, their knowledge of particular risks and the readiness of their organization may be incomplete.

### *Cyber Skills and Training Needs*

The responses indicated that cybersecurity training in healthcare organizations is either minimal or non-existent. Felix mentioned a brief introductory course that all new employees must take but noted that the training was infrequent and lacked depth. Dasha reported that no formal cybersecurity training was available in her organization, and Miia mentioned that while some information security training is provided, it is limited.

All interviewees expressed a need for more robust and regular cybersecurity training. Felix and Dasha emphasized the importance of awareness and the ability to identify phishing threats, while Miia highlighted the need for proper handling of patient data. The lack of consistent training suggests a significant gap in the current cybersecurity preparedness of healthcare professionals.

### *Familiarity with the ECSF*

Before the interview, none of the interviewees had ever heard of the European Cybersecurity Skills Framework (ECSF). But after learning about the idea, they were all able to see its possible value and applicability. While Dasha believed that the ECSF provided crucial recommendations for handling sensitive material, Felix and Miia were amenable to the idea of utilizing a standardized framework.

The ECSF needs to be more widely known in the healthcare industry, as evidenced by the overall lack of understanding of the framework. This could promote the use of ECSF-based procedures and strengthen cybersecurity defenses all around.

### *Applicability and Implementation of ECHO CSF*

The interviewees provided a range of viewpoints regarding how their organizations could modify the ECHO CSF. Felix claimed that mandatory training sessions on a regular basis could facilitate the integration of the ECHO CSF into current programs. Dasha countered that management support would be necessary, particularly in smaller organizations. Miia stressed how crucial it is to translate the framework into Swedish and Finnish so that local medical experts can use it more easily.

Dasha and Miia both highlighted the necessity for localisation and the possibility of resistance to change as the two primary obstacles to the ECHO CSF's implementation. These answers emphasise how crucial it is to customise new frameworks for healthcare settings while also considering cultural nuances.

### *Impact on Organizational Cybersecurity Posture*

Every interviewee thought that putting the ECHO CSF into practice may improve the cybersecurity posture of their company. Felix and Miia expressed optimism over the possible enhancements. However, Dasha proposed that the success of the framework would hinge on its necessity and its seamless integration into day-to-day activities.

The interviewees had few recommendations for gauging the effectiveness of ECHO CSF adoption. Dasha proposed employee input as a potential success indicator, but Felix and Miia were not sure what the right measurements would be. This indicates that in order to evaluate the success of ECHO CSF adoption in healthcare organisations, specific, quantifiable results are required.

## Discussion

The implementation of the ECHO Cyber-Skills Framework within the CyberSecPro project has demonstrated significant potential in enhancing cybersecurity capabilities in the healthcare sector. The findings from this study highlight several key areas of impact and provide insights into the practical application of the ECHO CSF.

The study identified critical skill gaps in incident response, threat analysis, and risk management within the healthcare industry. The ECHO CSF has proven to be an effective tool in addressing these gaps by providing structured training programs tailored to the specific needs of healthcare professionals. The emphasis on customized training ensures that the unique challenges faced by the healthcare sector are adequately met.

The research underscores the necessity of ongoing professional development in maintaining and enhancing cybersecurity skills. The ECHO CSF's focus on continuous learning and skill enhancement aligns well with the dynamic nature of cyber threats. Regular updates and refresher courses are essential to keep healthcare professionals abreast of the latest developments in cybersecurity.

Despite the positive outcomes, the study also highlights several challenges in implementing the ECHO CSF. These include resistance to change, the need for localization of training materials, and the necessity of management support. To

overcome these challenges, the study recommends a phased implementation approach, active stakeholder engagement, and the translation of training materials into local languages.

## Conclusions

The findings of this study highlight the critical need for a structured and phased approach to implementing the ECHO CSF in the healthcare sector. To achieve this goal, it is recommended that healthcare organizations begin by conducting a skills gap analysis to identify the most urgent training needs. Based on the ECHO CSF's guidelines, tailored training programs should be developed, with a focus on incident response, threat analysis, and risk management. Ongoing professional development and regular assessments should be incorporated to ensure that healthcare staff remain up-to-date on evolving cyber threats. These strategies will enhance the sector's overall cybersecurity posture and align with the ECHO CSF's objectives.

## Acknowledgements

Acknowledgement is paid to the CyberSecPro Project. This project has received funding from the European Union's DIGITAL-2021-SKILLS-01 Programme under grant agreement no. 101083594. The sole responsibility for the content of this paper lies with the authors. It does not necessarily reflect the opinion of the European Commission or of the full project. The European Commission is not responsible for any use that may be made of the information contained therein.

## References

[1] Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson, and D. Kyle Monticone, "Cybersecurity inHealthcare: A Systematic Review of Modern Threats and Trends," *Technology and Health Care* 25, no. 1 (2017): 1-10.

[2] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, 2018, https://www.nist.gov/cyberframework.

[3] ENISA, "The European Cybersecurity Skills Framework (ECSF)," 2017.

[4] Toria Shaw, Rachelle Blake, Ursula Hübner, Christel Anderson, Victoria Wangia-Anderson, and Beth Elias, "The evolution of TIGER competencies and informatics resources," Executive Supplemental Report, 2017.

[5] Kruse, et al., "Cybersecurity in Healthcare," 2017.

[6] Eleonora Beltempo, Jussi Karvonen, and Jyri Rajamäki, "ECHO Cyber-Skills Framework as a Cyber-Skills Education and Training Tool in Health and Medical Tourism," ECHO Project,2021, pp. 1-30.

[7] Kruse, et al., "Cybersecurity in Healthcare," 2017.

[8] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse, "Cyber security awareness campaigns:Why do they fail to change behaviour?" arXiv preprint arXiv:1901.02672, 2019.

[9] NICCS, "Workforce Framework for Cybersecurity (NICE Framework)," March 2024, https://niccs.cisa.gov/workforce-development/nice-framework.

[10] Shaw, et al., "The evolution of TIGER competencies and informatics resources," 2017.

[11] Matthew L Williams, Pete Burnap, and Luke Sloan, "Towards an Ethical Framework for Publishing Twitter Data in Social Research: Taking into Account Users' Views, OnlineContext and Algorithmic Estimation," *Sociology* 51, no.6 (2017): 1149-1168.

## About the Authors

Eleonore **Beltempo** is a student at the Laurea University of Applied Sciences, Espoo, Finland, contributing as a researcher to some of Laurea's cybersecurity projects.

Dr. Jyri **Rajamäki** – see the CV on p. 78 of this volume, https://doi.org/10.11610/isij.5523. https://orcid.org/0000-0003-4798-2462