Cybersecurity in Education – Developing and Testing New Teaching Practices

Ilkka Tikanmäki
Business, Data Processing and Service Sector Unit, Laurea University of Applied Sciences
Department of Warfare, National Defence University

Ilkka.tikanmaki@laurea.fi

Abstract: Recently, cybersecurity has taken on significant importance as a specialised field in both the social and healthcare sectors. The safety of customers and patients is directly linked to the handling of sensitive information and the security of digital operating environments. Despite this, systematic integration of cybersecurity into teaching remains fragmented in many places, and there is variability in teachers' preparedness to handle it pedagogically. This study investigates data gathered during the KyberSote pilot, aimed at enhancing cybersecurity competence among social and healthcare educators and facilitating the integration of the subject into their teaching practices. The research data is composed of qualitative data that was gathered during three workshops and a feedback survey (n = 17) that took place at the end of the pilot, with teachers from four Finnish Universities of Applied Sciences (UAS) participating. The data offers a diverse overview of teachers' starting points, perceived development needs, and the functioning of pedagogical solutions in various educational contexts. This study focuses on synthesising individual responses to identify key themes and development t rends i n c ybersecurity education. The KyberSote pilot's implementation was based on a working method that was both participative and reflective. Teachers evaluated their own abilities, experimented with various learning resources, and contemplated the significance of cybersecurity in teaching and the overall operating culture. The pilot utilised a variety of pedagogical methods, including videos, discussion tasks, and game-based approaches, with the goal of supporting practical learning and increasing student participation. The study aims to explore teachers' perceptions of their cybersecurity competence, the suitability of the provided learning materials and environments, and the barriers and opportunities related to integrating cybersecurity into teaching. The integration of cybersecurity into social and healthcare education is given special attention to organisational factors that enable or limit it. The study provides new insights into the pedagogic development of cybersecurity education in the social and healthcare sector and provides suggestions for the improvement of teaching and training systems. This approach contributes to the discussion about how cybersecurity can be understood and implemented as a key competence that is an essential part of the future professionals' competence profile.

Keywords: Cybersecurity Education, Social and healthcare Sector, Teacher Competence, Pedagogical Development, Higher Education (UAS), Cybersecurity Competence

1. Introduction

KyberSoTe – Cybersecurity in the everyday life of social services and healthcare – is a project to strengthen the cybersecurity competence of social services and healthcare professionals and to foster cooperation between different professional groups. The project implementation period is 12.2.2024 - 31.12.2026 and is funded by the Finnish National Agency for Supply Security Digital Security 2030 program. The project is implemented by Jyväskylä University of Applied Sciences, Laurea, Tampere University of Applied Sciences and Turku University of Applied Sciences. The partners are the welfare regions of Central Finland, Pirkanmaa, Päijät-Häme, Vantaa-Kerava, and Southwest Finland. (The National Emergency Supply Agency, 2023)

The main goal of the project is to promote preparedness, service continuity, and patient safety in social and healthcare organisations. This is objective is pursued from two perspectives: increasing the cybersecurity competence of social and healthcare professionals and strengthening cooperation between social and healthcare professionals and information management professionals regarding cybersecurity. In addition, the cybersecurity expertise of social and healthcare teachers at Universities of Applied Sciences (UAS) and of social and healthcare students will be enhanced. (The National Emergency Supply Agency, 2023)

The pilot for teachers was implemented in spring 2026. 3–5 teachers in the social and healthcare sector/University of Applied Sciences participated in it, and 10 hours of working time were allocated per person for implementation. The pilot was implemented in three two-hour meetings. The topics of the first meeting were information about the pilot and an introduction to the topic and materials. Between the 1st and 2nd meetings, the participants completed the online training on the Moodle Learning Management System (Moodle, 2026) independently. Two hours were allocated for this. In the second meeting, some additions were made to the workshop from the toolkit. In the third meeting, some additions were also made to the toolkit, and a feedback survey was conducted, as well as an open feedback event. Participants were encouraged to integrate the materials from the training environment to their own courses whenever feasible.

To achieve these objectives, the study is guided by the following research questions:

- How do social and healthcare teachers perceive the development of their cybersecurity competence?
- What pedagogical and organisational factors support its integration into teaching?

The article is organised as follows. First, a review is conducted on previous research concerning cybersecurity in the social and healthcare sectors, as well as its pedagogical aspects. This is followed by a presentation of the research methodology, including the research design, participants, data collection, and analysis methods. The results segment outlines important insights into teachers' initial standings, skill progression, and administrative and procedural elements that affect incorporating cybersecurity into their teaching. This section continues with a discussion where the outcomes are analysed in the context of previous studies, methodological viewpoints, and real-world applications. The final section includes conclusions, limitations, and suggestions for future research.

2. Literature

Due to digitalisation, cybersecurity has become a crucial skill in all industries. It is especially important in social and healthcare sectors, where confidential data is handled, and digital systems form a key component of service delivery. Customer and patient safety and the organisation's operational capacity can be jeopardised by cybersecurity-related risks, such as data breaches, phishing attacks, and system failures. The central role of education in risk management is highlighted by research that shows that a significant proportion of healthcare data security breaches are related to human factors and skills gaps. (Liu et al., 2025)

Digitalisation and the quick advancement in technology have significantly contributed to the benefits in the social and healthcare sectors. For instance, electronic health records and telehealth services contribute to operational efficiency and enhance the quality of care (Jerry-Egemba, 2024). There are downsides to digitalisation, as well; for instance, there has been an increase in cybersecurity threats (Jerry-Egemba, 2024; Nifakos et al., 2021). Interest from cybercriminals is drawn to social and healthcare environments and their vulnerabilities, which is why they target organisations and employees in these sectors (Haukilehto, 2024). Increasingly, social organisations, healthcare facilities, nursing homes, and care providers are becoming targets of cyberattacks (Alanazi, 2023; Aljuraid & Justinia, 2022). The unauthorised disclosure of personal and health information can lead to substantial risks and consequences, as noted by (Kotková, 2022).

The social and healthcare sectors consider personal and health information to be a valuable commodity. Its value is particularly high due to the difficulty in changing or replacing this information. Examples of how cybercriminals gain access to an organisation's information systems or devices on a network include data breaches, phishing, various ransomware attacks, and denial-of-service attacks. Cybercriminals gain access to systems via usernames and passwords, often obtained through phishing, and other methods, which is a prevalent type of information security breach (Blek & Solankallio-Vahteri, 2022). Maintaining a secure daily life in social and healthcare is essential for all professionals, and their activities are vital for ensuring the safety of both customers and patients in work environments. The Universities of Applied Sciences demand specific skills from teachers. Professionals graduating in social and healthcare have a thorough understanding of cybersecurity practices across various environments in the social and healthcare sectors.

Even though cybersecurity is becoming more important, its pedagogical treatment in higher education is still fragmented. Previous research has demonstrated that cybersecurity content is not consistently included in the curriculum, and teacher training is not always up to date with the rapidly changing threat environment (Blažič & Blažič, 2024). Moreover, notable discrepancies in cybersecurity expertise have been detected, particularly among students from non-technical backgrounds, thereby augmenting the organisational risk.

Cybersecurity research has primarily concentrated on technical solutions, though recent studies emphasise the importance of user-centred competence, cyber hygiene, and security culture (Maennel et al., 2018; Uchendu et al., 2021). Research has revealed that effective cybersecurity training necessitates pedagogical solutions that are both inclusive and contextualised, including case-based learning, simulations, and digital learning environments (Mukherjee et al., 2024). At the same time, notable gaps have been identified, particularly in teachers' pedagogical skills, curriculum integration, and the lasting effects of training solutions (Liu et al., 2025). The cybersecurity competence among social and healthcare practitioners is becoming more crucial nowadays to recognise and detect the possible cyber risks in these varied social and healthcare settings (Blek & Solankallio-Vahteri, 2022).

3. Method

This study employs a qualitative research method, designed to explore the development of teachers' cybersecurity competence and their encounters throughout the KyberSote pilot phase. The qualitative method allows for a thorough exploration of participants' experiences, interpretations, and insights (Creswell & Poth, 2018). The study is founded on a pilot conducted in spring 2026, involving teachers from four Finnish universities of applied sciences. The pilot implementation utilised a participatory and reflective development approach, in which participants played an active role in assessing their own competence and examining the integration of cybersecurity into their teaching (Boud et al., 1985/2013; Schön, 2017).

Three workshops, each about two hours long, comprised the pilot, with independent online studies in the Moodle environment serving as a supplement. The sessions covered essential cybersecurity topics, offered learning resources, and featured collaborative discussions and pedagogical reflections. After each workshop, participants independently studied the materials and incorporated them into their teaching, depending on the situation.

Seventeen (n = 17) social and healthcare educators took part in the research. Participants came from various educational backgrounds, with differing initial levels of cybersecurity knowledges, allowing for a comprehensive exploration of the issue. Participation in the study was voluntary. Figure 1 illustrates the structure of the pilot by phases and the points of data collection.

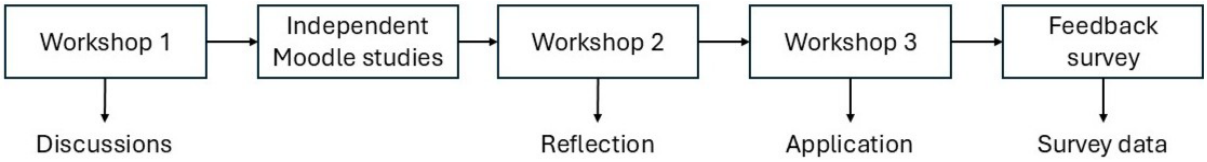

Figure 1: Pilot's structure in stages and data collection points.

The research data includes workshop data and the results of the feedback survey. Qualitative data generated during the workshops, which includes participants' discussions, reflections, and feedback on learning materials and competence development. Data collected for the pilot survey, conducted at its conclusion, encompassed both quantitative elements (using Likert scales) and open-ended queries delving into participants' experiences, learning outcomes, and developmental needs. Through multi-method data collection, the phenomenon could be studied from multiple viewpoints, thus boosting the research's reliability (Denzin, 2009). Data analysis was conducted through thematic analysis, a method effective for systematically organising qualitative data and uncovering meanings (Braun & Clarke, 2006). The structure of the data and analysis are presented in Table 1.

Table 1: Summary table of analysis.

Source of Data	Description	Analysis Method	Purpose
Workshops	Discussions and reflections	Thematic analysis	Development of competence
Moodle work	Independent learning	Reflective review	Learning process
Feedback survey	Likert + open-ended	Descriptive + thematic	Experiences and evaluation

The analysis employed inductive methods, without a predetermined theoretical framework, with themes emerging from the data serving as the basis for the analysis. The examination proceeded through the following phases:

1. Familiarisation with the data and preliminary coding
2. Determining the significant content sections (like pedagogy and implementation)
3. Organising codes into thematic groups
4. Investigating themes and their connection to the research questions

The table 2 shows the analytical process utilised in the research. It shows how survey responses and workshop discussions were initially coded, grouped into sub-themes, and then synthesised into broader themes, which served as the foundation for the findings.

Table 2: Progression from raw data to final themes.

Example Data Extract	Initial Code	Sub-Theme	Main Theme
"I learned how to teach cybersecurity and integrate it into different courses."	Increased teaching confidence	Pedagogical competence	Competence development
"The training made cybersecurity concrete through examples."	Practical relevance	Contextualised learning	Effectiveness of pedagogical methods
"The materials are versatile and suitable for many teaching situations."	Usable teaching resources	Teaching support	Organisational and pedagogical enablers
"Cybersecurity teaching depends too much on individual teachers."	Lack of systematic implementation	Structural challenges	Organisational barriers

The table highlights thematic analysis transparency, illustrating data from initial empirical sources to final themes. This allows readers to understand how the identified themes were based on participants' responses and how the collected data supported the interpretations of the study. The coding process resulted in multiple initial codes, which were subsequently grouped into sub-themes and four final themes.

The analysis gave particular focus to the teachers' initial level, their competence development, the practical effectiveness of pedagogical methods, and organisational elements that influence the incorporation of cybersecurity into teaching. The quantitative results of the questionnaire data were used descriptively to support the qualitative analysis, but they did not form the main analytical method of the study. Voluntary participation ensured confidential handling of the data. The anonymisation of all data was completed before the analysis, ensuring participant confidentiality. To strengthen reliability, the themes were consistently compared against the original data sources, which included workshop discussions and open-ended survey responses.

4. Results

Four main themes emerged from the analysis: (1) a varying initial cybersecurity competence, (2) perceived competence development during the pilot, (3) benefits of practical pedagogical methods, and (4) organisational factors influencing implementation. The same themes were consistently reflected in both the workshop discussions and the open-ended survey responses. According to the findings, in the initial situation, participants entered the pilot with varying levels of cybersecurity competence, and several competence gaps were identified.

Many participants were familiar with basic cybersecurity concepts but reported limitations in deeper understanding and in applying the topic within their teaching. Several competence challenges emerged, including the contextualisation of cybersecurity in social and healthcare sectors, the perceived ambiguity of terminology, and the uncertainty regarding the role of teachers as cybersecurity educators. Moreover, the inclusion of cybersecurity in education often seemed to lack a structured approach and was heavily reliant on individual teacher expertise.

The participants reported a more structured understanding of their cybersecurity competence following the pilot. Participants noted enhanced self-assurance and improved capability to recognise cyber-related occurrences and dangers within their own area. A significant adjustment was the integration of cybersecurity from a distinct and technical subject into everyday professional activities. Perceived competence development extended beyond knowledge acquisition and also included pedagogical skills. Teachers realised they had gained the ability to manage, instruct, and incorporate cybersecurity into various course components.

Participants emphasised that cybersecurity should be considered a fundamental competence for all social and healthcare professionals. Cybersecurity was closely tied to daily activities, including handling patient information, employing passwords, and leveraging digital tools. This fundamental skill approach reoriented the teaching perspective. The emphasis shifted from adhering to specific rules to incorporating safe practices. At the same time, this established a groundwork for incorporating cybersecurity into the curriculum without dedicated study modules.

Participants perceived practical and engaging teaching methods as supporting cybersecurity learning. Specifically, the increase in video presentations, case studies, interactive discussions, and game-based solutions boosted student engagement and provided a clearer understanding of abstract concepts. By integrating authentic work environments, these methods made cybersecurity courses more relevant. Interactivity and experientiality lowered the threshold for dealing with difficult topics and supported deeper understanding. Figure 2 below shows what kind of teaching or guidance situations participants utilised during the pilot.

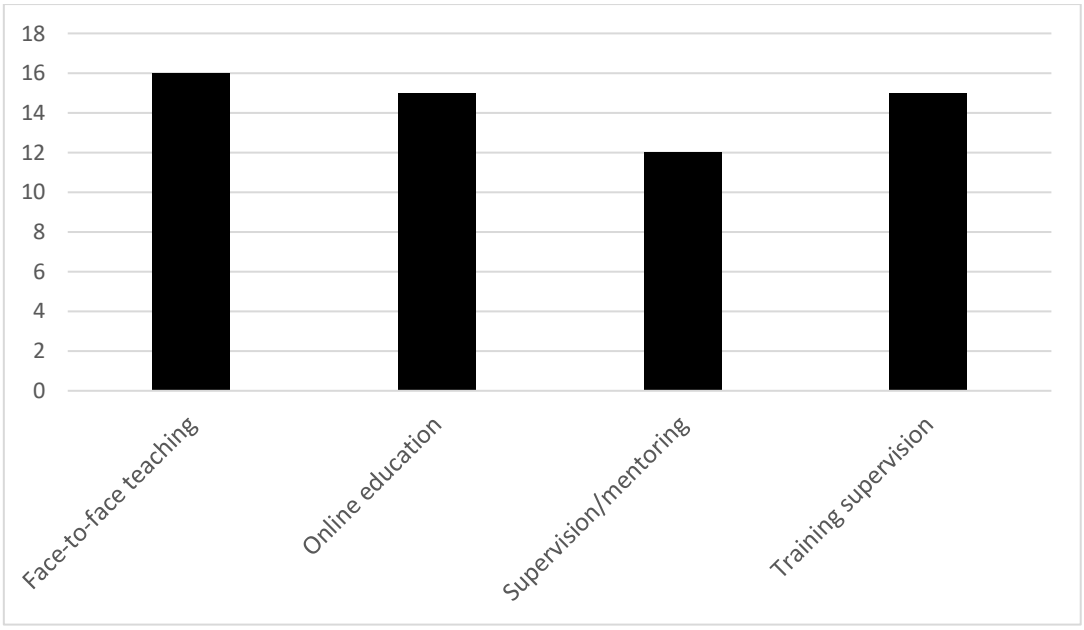

Figure 2: Teaching or guidance situations utilised in pilots.

The content of the training packet was used in face-to-face teaching, online training, internship supervision and supervision/mentoring situations, in some cases, also in tutor supervision and documentation teaching. The digital learning setting was primarily viewed as clear, pedagogically useful, and addressing the needs of teachers.

> *"The training made cybersecurity concrete through the use of examples and pedagogical approaches, which made the subject easier to understand*."

Specifically, the varied material and specific illustrations enhanced understanding and helped in the delivery of content during instruction. At the same time, the material highlighted the need for improvements in usability, structure clarity, and accessibility, including navigation and the availability of videos. The learning environment, even with its limitations, proved significant for cybersecurity teaching.

The results highlighted the lack of systematicity in cybersecurity teaching. Cybersecurity treatment largely depended on individual teacher competence and interest, resulting in varying student competencies. The integration needed time, planning, and pedagogical reflection, and its execution without standard guidelines was deemed challenging. Additionally, a rapidly shifting operating environment and an evolving cyber threat landscape put pressure on continuous competence updates.

> *"I learned how to teach cybersecurity and effectively integrate it into various courses."*

The outcomes reveal the significant influence of teachers on building a cybersecurity culture. The teacher functions as both a source of information and a model whose behaviour impacts students' views and behaviours. The teachers pointed out the necessity of pre-made resources, training, collaborative planning, and support at the organisational level. Systematic incorporation of cybersecurity into teaching was deemed to require ongoing competence development and well-defined operating models.

The training package was widely assessed as very useful for the work of the teachers. They felt that offering ready-made, usable materials would bolster their abilities and facilitate teaching development. Modular structures and concrete examples that facilitated the adaptable use of materials across various teaching scenarios were found to be particularly valuable.

> *"The materials are versatile and well-suited for use in face-to-face teaching, online training, guidance, mentoring, and the supervision of practical training."*

> *"Videos and practical exercises effectively support tutoring sessions, courses, and independent study."*

The training was also seen to strengthen the understanding of the importance of cybersecurity as part of working life skills. Table 2 presents a dataset that showcases quantitative representations of qualitative findings.

Table 3: Summary of quantitative feedback results from participants.

Scope	Result
Overall benefit	Participants reporting positive overall benefit: 100%
Increase in competence	Self-reported increase in competence: 100%
Direct usability in teaching	76% high
Widespread usability	> 80% in all contexts
Development needs	Focus on the social sector and visuality

Participants perceived the training as highly beneficial (100% positive responses), practical and widely usable, but requires development, especially in terms of the social sector context and the visuals of the materials. In total, the findings indicate that cybersecurity is acknowledged as an important area of expertise in the social and healthcare sectors, yet its systematic incorporation into education remains in an early stage of development. To ensure effective implementation, an integrated strategy, sound pedagogical methods, and support from both teachers and the organisation are essential.

5. Discussion

This investigation sought to explore the advancement of cybersecurity competence among social and healthcare teachers, along with the influence of pedagogical strategies in the KyberSote pilot. As a qualitative exploratory study, the findings reflect participants' experiences within a specific context and are not intended to be broadly generalisable (Creswell & Poth, 2018). Participants perceived that their cybersecurity competence had increased as a result of the pilot activities, particularly in conceptual knowledge, practical use, and confidence in teaching. Since the assessment relies on participants' own evaluations and reflections, it doesn't provide an objective measure of their competence. However, it offers a profound insight into the structure and development of competence in a professional setting (Braun & Clarke, 2006). The noted progression is closely tied to the participatory and reflective approach taken in the pilot, a method that reinforces prior studies highlighting the significance of reflective learning in fostering expertise (Schön, 2017).

A key finding is the shift in how participants viewed cybersecurity from a distinct technical subject to an essential aspect of regular professional duties. This indicates that cybersecurity should be recognised as a fundamental skill that needs to be seamlessly incorporated into education across different subjects (Uchendu et al., 2021). The thematic analysis's inductive nature enabled the identification of such deep meaning from the data without initial assumptions (Braun & Clarke, 2006). The findings highlight that competence isn't solely about having knowledge but is also linked to the organisation's culture and professional identity. Table 3, effectiveness of pedagogical methods, combines the results and pedagogical contribution.

Table 4: Effectiveness of pedagogical methods

Method	Perceived Benefit	Pedagogical Impact
Videos	High	Illustration
Case examples	High	Contextualisation
Discussions	High	Reflection
Gaming	Moderate/high	Engagement

Regarding pedagogical approaches, the findings endorse the conclusions concerning the efficacy of hands-on and interactive techniques, including case studies, multimedia presentations, and discussions (Mukherjee et al., 2024). These highlight the link between cybersecurity and realistic work environments, thereby enhancing the importance of training. As highlighted, the assessments rely on teachers' observations instead of students achieving the learning objectives. Combining workshop and survey data strengthened the credibility of the findings (Denzin, 2009), but it did not allow objective measurement of learning outcomes.

This outcome underscores a significant issue: the fragmentation of cybersecurity education, which relies heavily on individual teachers' skills. These findings supports the conclusion that individual competence development is not enough; a more comprehensive, organisational approach is necessary. The qualitative approach facilitated the detection of these structural and cultural elements.

The role of the teacher is emphasised as the builder of a cybersecurity culture. Simultaneously, the findings highlight the necessity of continued support, such as ready-made materials, training, and collaborative pedagogical growth. This aligns with the finding that enhancing cybersecurity necessitates both pedagogical approaches and organisational frameworks.

Some limitations of the study are the small sample size (n = 17), reliance on self-reported data, and the brief pilot period, neither of which permit evaluation of long-term outcomes. The short duration of the pilot project limited the assessment of long-term knowledge retention, sustained educational changes, or the adoption of cybersecurity teaching practices in educational institutions. Regardless, the study delivers an empirically based insight into the advancement of cybersecurity education. For future studies, attention should be directed towards longitudinal approaches, the assessment of learning results, and the evaluation of teaching methodologies.

Although the findings indicate positive perceptions regarding competence development and the usefulness of the training, these conclusions must be interpreted with care. The assessment was mainly conducted based on the participants' self-reported experiences, collected from surveys and dialogues in workshops. The study, therefore, cannot assess the level of improvement in actual cybersecurity expertise or pedagogical competence. Additionally, the results indicate participants' opinions on their own educational and professional progress. Further studies could enhance this self-reported data with objective evaluation methods, like pre- and post-training knowledge tests, observations of teaching, or frameworks based on skills and competencies.

To summarise, the findings substantiate the assertion that cybersecurity is essential for competence in social and healthcare sectors, and its enhancement necessitates a structured, pedagogically sound, and organisationally supported strategy.

6. Conclusions

Based on self-reported perceptions, participants experienced substantial improvements in their cybersecurity competence during the pilot. Participants reported improvements in conceptual understanding, practical application, and confidence in integrating cybersecurity into teaching. The findings indicate that a well-defined and user-friendly learning environment is essential for competence development. Concretely, examples and straightforward materials were effective in learning and quickly transformed theoretical knowledge into practical use.

The main finding is that cybersecurity should be viewed as a comprehensive capability, rather than a distinct subject area. Its incorporation into all forms of teaching - both theoretical, simulated, and real-world exercises - facilitates the systematic enhancement of students' skills throughout their educational journey. This methodology redirects attention from discrete information to a perpetual learning trajectory, embedding cybersecurity into routine tasks and conscientious operations.

Figure 3 visualises the thematic structure of the KyberSote project’s cybersecurity competence development. The figure shows the development path from the starting level through pedagogy and competence to the organisational factors.

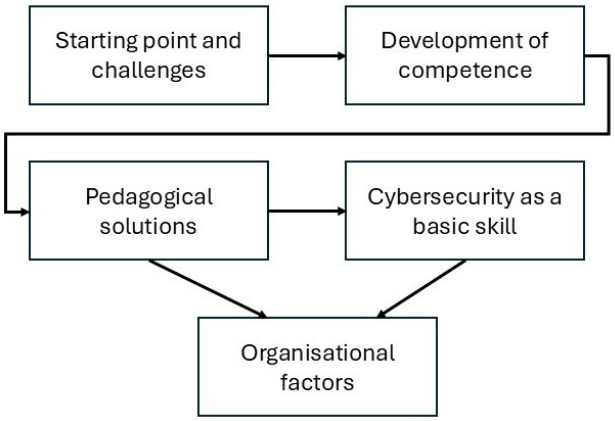

Figure 3: Thematic structure of cybersecurity competence development in the KyberSote pilot.

The results highlight the effectiveness of practical and participatory pedagogical methods. Participants perceived case examples, videos, simulations, and gamified approaches as particularly useful learning methods. The main advantage of these approaches lay in their capability to integrate cybersecurity into regular activities, thus enhancing learning retention and practical use.

The findings suggest that cybersecurity competence development is strongly influenced by the teacher's role. Furthermore, teachers serve as role models and influencers in cultivating an information security culture alongside being information transmitters. The study indicates that teachers' daily practices and pedagogical approaches significantly influence students' attitudes and learning behaviours. Cybersecurity is shown to be both an informational and cultural, as well as a functional competence.

The learning environment was seen as a key factor supporting success. Clear structure, diverse content, and practicality made it easy to incorporate cybersecurity themes into teaching. Similarly, targets for development were noted, including specifying navigation, enhancing material accessibility, diversifying content, particularly from various social and healthcare perspectives. The main challenge recognised was the absence of systematic instruction in cybersecurity. The handling of the topic frequently relies on individual teachers rather than following standard structures or curricula. Moreover, the swiftly altering threat landscape stresses the importance of continuous competence updates, which depend on teachers' support, relevant materials, and clear operating models.

6.1 Recommendations and Further Development

Based on the findings, the main recommendations concentrate on systematically incorporating cybersecurity into educational programs and organisational strategies. Table 4 presents barriers and enablers identified in the pilot.

Table 5: Barriers vs enablers.

Barriers	Enablers
Lack of time	Ready-made materials
Unclear role	Training
Variation of skills	Collaboration
Lack of structures	Organisational support

Cybersecurity should be integrated into curricula and study paths, and teachers should receive common initial training, with practical pedagogical methods being widely utilised. Learning environments should be improved by considering accessibility, usability, and organisational support structures, such as mentoring. Furthermore, a gradual approach is suggested, wherein cybersecurity competence is developed starting from the foundational level up to advanced proficiency throughout the learning journey.

Future research should combine qualitative observations with objective learning metrics. An integrated research design, incorporating competency assessments before and after the intervention, data on the implementation of the teaching sessions, and long-term follow-up, would provide more robust evidence regarding the effectiveness of teacher training programs in cybersecurity.

In summary, the findings indicate that cybersecurity is essential for competence in social and healthcare sectors, and its advancement necessitates a methodical, educationally grounded, and organisationally supported strategy. The key message of the pilot is that cybersecurity is not a separate theme, but a continuous process and part of the professional culture. By integrating expertise into teaching, supporting teachers, and utilising practical methods, a sustainable foundation for cybersecurity expertise in education and working life can be built.

Acknowledgements

This study has received funding from the Cybersecurity in Everyday Work in the Social and Healthcare Sector (KyberSoTe) project. The views expressed are those of the author only and do not necessarily reflect those of the granting authority.

Ethics Declaration

Participation in the study was voluntary, and all responses were treated confidentially. The data were anonymised before analysis, ensuring that individual participants could not be identified. The study followed good scientific practice and ethical guidelines for educational research.

AI Declaration

The paper's spelling was verified using the artificial intelligence tool.

References

Alanazi, A. T. (2023). Clinicians' Perspectives on Healthcare Cybersecurity and Cyber Threats. *Cureus*, *15*(10), e47026. https://doi.org/10.7759/cureus.47026

Aljuraid, R., & Justinia, T. (2022). Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review. *Advances in Informatics, Management and Technology in Healthcare*, *295*. https://doi.org/10.3233/SHTI220739

Blažič, A. J., & Blažič, B. J. (2024). Toward effective learning of cybersecurity: New curriculum agenda and learning methods. *Journal of Cybersecurity*, *10*(1), tyae018. https://doi.org/10.1093/cybsec/tyae018

Blek, T., & Solankallio-Vahteri, T. (2022). Information and cybersecurity competence of healthcare care personnel. *Finnish Journal of eHealth and eWelfare*, *14*(4), 352–363. https://doi.org/10.23996/fjhw.115829

Boud, D., Keogh, R., & Walker, D. (2013). *Reflection: Turning experience into learning*. Routledge. https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.4324/9781315059051&type=googlepdf (Original work published 1985, Routledge)

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Creswell, J. W., & Poth, C. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th edn). SAGE Publications. https://books.google.fi/books?hl=fi&lr=&id=DLbBDQAAQBAJ&oi=fnd&pg=PP1&dq=%E2%80%A2+Creswell,+J.+W.,+%26+Poth,+C.+N.+(2018).+Qualitative+inquiry+and+research+design.&ots=-iv06gEOWt&sig=AlbeVmKD3MdFX50Njy735R8iJYo&redir_esc=y#v=onepage&q&f=false

Denzin, N. K. (2009). *The research act: A theoretical introduction to sociological methods* (1st edn). Routledge.

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

Jerry-Egemba, N. (2024). Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs. *Healthcare Management Forum*, *37*(1), 21–25. https://doi.org/10.1177/08404704231194577

Kotková, B. (2022). *Cyber security in the healthcare sector—Current threats*. *22*(2.1), 11–18. https://doi.org/10.5593/sgem2022/2.1/s07.02

Liu, N., Long, S., & Martin, F. (2025). Systematic Review of Elementary Cybersecurity Education: Curriculum, Pedagogy, and Barriers. *Journal of Cybersecurity Education, Research and Practice*, *2025*(1), 178–181. https://doi.org/10.62915/2472-2707.1265

Maennel, K., Mäses, S., & Maennel, O. (2018). Cyber Hygiene: The Big Picture. In N. Gruschka (Ed.), *Secure IT Systems* (Vol. 11252, pp. 291–305). Springer International Publishing. https://doi.org/10.1007/978-3-030-03638-6_18

Moodle. (2026, May 22). *Learning tools*. Doodle. Welcome to the Moodle Community Forums. https://moodle.org/plugins/local_learningtools

Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information*, *15*(2), 117. https://doi.org/10.3390/info15020117

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

Schön, D. A. (2017). *The Reflective Practitioner: How Professionals Think in Action* (1st edn). Routledge. https://doi.org/10.4324/9781315237473

The National Emergency Supply Agency. (2023). *Cybersecurity in Everyday Life* [Project plan]. The National Emergency Supply Agency.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387