Received 1 December 2024
Revised 7 April 2025
20 June 2025
17 July 2025
Accepted 17 July 2025

Cybersecurity awareness and hygiene development in Finnish vocational education: staff perceptions, training gaps and diverse learning pathways

Anna-Liisa Ojala
School of Professional Teacher Education, Jamk University of Applied Sciences, Jyvaskyla, Finland, and

Tuomo Sipola and Karo Saharinen
Institute of Information Technology, Jamk University of Applied Sciences, Jyvaskyla, Finland

Abstract

Purpose – This study aims to examine cybersecurity awareness and hygiene development among staff in Finnish vocational education institutions. It explores perceived skill levels, training methods, gaps between awareness and action and diverse learning pathways. It also investigates how organisational learning influences cybersecurity practices.

Design/methodology/approach – A qualitative approach was used, involving thematic interviews with 27 staff members from three vocational institutions across Finland. The data, including limited observation notes, were analysed inductively using thematic analysis to identify patterns related to cybersecurity competence and training experiences.

Findings – The findings reveal significant variation in cybersecurity awareness, skills and practices among staff. While some demonstrate high competence, others rely on assumptions or outdated routines. Formal training is often generic learning, while more reflective and adaptive learning occurs through informal networks and peer collaboration. Gaps exist in preparing staff to manage real data in simulated and workplace learning environments.

Research limitations/implications – The study's qualitative scope limits generalisability. Broader samples and cross-sector comparisons are recommended.

Practical implications – Institutions should strengthen diverse learning pathways, align training with staff roles and responsibilities and support reflective learning practices that acknowledge the specific cybersecurity demands of vocational education's close connection to real-world workplaces.

Social implications – Improved cybersecurity hygiene in vocational education benefits not only institutions but also the industries they support through student placements.

Originality/value – This research addresses a gap in cybersecurity studies by focusing on vocational education, a sector with distinct responsibilities and risk surfaces. It highlights the importance of tailoring training and recognising informal learning.

Keywords Cyber hygiene, Cybersecurity, Vocational education, Schools, Qualitative study

Paper type Research paper

Funding: This research was fully supported by The Finnish Work Environment Fund under the grant number 230316. The authors would like to thank the participating educational institutions.

Information & Computer Security
Vol. 34 No. 1, 2026
pp. 66-85
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-12-2024-0311

1. Introduction

Cybersecurity has become a significant concern alongside traditional threats to the resilience of civil society. The education sector has also become a potential target for harassment, financial exploitation and intentional disruption of social stability. According to EdTech media (Viano, 2024), the education sector experienced its worst year yet for ransomware attacks in 2023. Research also indicates that improving information and cybersecurity capabilities is increasingly essential for educational institutions (e.g. Ulven and Wangen, 2021).

Because digital systems mainly serve as support functions in education, they may not be seen as lucrative targets. However, any system can be viewed as an attack vector by malicious actors (Mims, 2024). Additionally, any system is vulnerable to damage caused by potential negligence in the institution's own operations. Ensuring information and cybersecurity in an educational institution, as in any other organisation, is the responsibility of all its members (Anesone, 2024).

This study examines cybersecurity in the context of vocational education institutions, focusing on staff perceptions of their competencies and training. If research into cybersecurity within the higher education (HE) sector has gained popularity in recent years (e.g. Ugwu *et al.*, 2022), examining cybersecurity related capacities within vocational education and training (VET) is particularly important due to the differences between vocational schools and higher education institutions. Vocational education differs mainly through its practical focus and emphasis on job-specific skills. While higher education centres more on theoretical knowledge and widening of understanding, vocational studies are hands-on, with students often training directly at companies or environments simulating working life (Ferm, 2021). This means that their internships extend cybersecurity requirements from educational institutions to industries, especially in terms of supervising students. Furthermore, vocational teachers often bring industry experience into the classroom, creating learning environments similar to real workplaces. For example, vocational schools may operate car repair shops or hair salons serving real customers, with genuine customer data and industry-standard digital systems. This expands the institution's attack surface, which should be taken into account in staff training and competency development. Moreover, recent research has also identified a growing reliance on cloud-based services in educational institutions (Thavi *et al.*, 2024), which is also transforming how cybersecurity is managed and supported. As these systems become more deeply embedded in daily school operations, cybersecurity practices are increasingly shaped by the tools, protocols, and support mechanisms provided by external service providers. All these qualities make the VET sector an interesting subject for cybersecurity research.

This study is qualitative, with data collected through interviews ($n = 27$) with staff members from three vocational institutions across Finland. The methods of data collection and analysis are described in detail in the methods section, following the introduction of key concepts and the current state of research, including the specific research questions. After this, we present the findings, addressing each research question in turn.

1.1 Cybersecurity awareness and hygiene: key concepts

This section outlines how key terms related to cybersecurity are understood in the context of this study. While the definitions draw on established sources, they are adapted to reflect the educational and organisational focus of the research. Our approach builds on terminology developed by national and international cybersecurity bodies (Maurer and Morgus, 2014) as well as more recent academic work on the evolving definitions and frameworks of information and cybersecurity (e.g. Althonayan and Andronache, 2018). As previous

research has shown, these concepts are shaped by institutional, cultural and policy contexts, and their meanings often shift accordingly (Cains *et al.*, 2022).

Building on these earlier frameworks, in this study, *data protection* refers to the safeguarding of information relating to individuals, organisations and technologies. Such protection is typically grounded in legal frameworks or institutional policies and guidelines. Closely related is *information security*, which involves protecting such data across digital, paper-based or other physical formats, with particular attention to how it is processed, stored, and accessed in various operational settings. *Cybersecurity*, in turn, is not limited to technical systems or infrastructure. It also involves the capacity to act within the cyber domain, which is inherently digital but increasingly influences everyday activities. Consequently, we consider cybersecurity to mean "protective measures taken against cyber threats to communication and information systems and other electronic systems, to the data stored, processed or transferred in them, and to their users, appliers and other concerned parties" (Finland's Cyber Security Strategy, 2024/2035, p. 10). As digital systems are designed, operated and sometimes misused by people, cybersecurity cannot be separated from human behaviour. Incidents often result from both accidental and deliberate actions, making human agency a key factor in both threats and protection.

Two concepts of particular relevance to this study are *cybersecurity awareness* and *cybersecurity hygiene*. The former refers to an individual's understanding of cyber threats and their role in maintaining the security of systems, data and organisational processes (Shaw *et al.*, 2009). The latter, cybersecurity hygiene or simply cyber hygiene, has gained increasing prominence in recent policy discourse. For example, the European Public Policy Committee's position statement (IEEE, 2020) recommends that all citizens, organizations and businesses should be trained in cybersecurity hygiene. Previous studies have also observed that these policy programs often do not specify what this term means in practice. Thus, Vishwanath *et al.* (2020) composed a paper around defining cybersecurity hygiene, and their conclusion is the following: Cybersecurity hygiene means "the cybersecurity practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet-enabled devices from being compromised in a cyber-attack." They compare it to hygiene practices that keep environments clean and free from harmful elements. Similarly, Niegel *et al.* (2020) describe cyber hygiene as "the adaptive knowledge and behavior to mitigate risky online activities that put an individual's social, financial, and personal information at risk." In this study, we use a combined understanding of the two definitions, Vishwanath *et al.* (2020) emphasise regular cybersecurity practices to protect personal information, while Niegel *et al.* (2020) focus on the knowledge and behavior needed to avoid online risks. We apply this combined view in an organisational context and, thus, also take into account analogue data protection, as information management in educational institutions involves both digital and non-digital environments. Some information is still collected, stored and used in traditional, analogue ways and these operations also require protection, along with related skills and training.

Cybersecurity awareness and hygiene are related to Information and Communication Technology (ICT) system development, policies, laws and regulations. Thus, these concepts are dependent on the time and place where they are defined. In previous studies, it has been noted that the cloud service model is increasingly forming the foundation of current school ICT systems, although adoption has been somewhat slower in, for example, developing countries (Thavi *et al.*, 2024). Thus, it is only natural that cybersecurity hygiene is increasingly linked to cloud service models' development trends at educational institutions. Also, the European Union has many strong rules and aims to protect people's data, including schools, with the General Data Protection Regulation (GDPR, 2018) being one example of

the key protocols. Aiming for cybersecurity hygiene is a continuation of these other regulations and aims such as GDPR: important and sensitive information is aimed to be protected, but cybersecurity also considers the protection, safeguarding and recovery of critical operations.

1.2 State of the art and research questions

Research on cybersecurity awareness and hygiene in educational institutions has started to gain more attention in recent years. While many studies have concentrated on students (e.g. Baraković and Baraković Husić, 2022; Witsenboer *et al.*, 2022), a smaller number have focused on staff. For instance, Ugwu *et al.* (2022) examined staff and students' cyber hygiene at a Nigerian university, finding that age or education level had limited impact on cybersecurity knowledge or behaviour. Butler Lamar (2022) applied a maturity assessment framework to evaluate staff practices at Savannah State University, while Concepcion and Palaoag (2024) explored employee awareness in areas such as device and account security, emphasising the value of tailored, interactive training. These studies suggest growing interest in staff-focused cybersecurity within education, but empirical work remains limited in scope, particularly in vocational settings.

Several studies have also reviewed or tested the effectiveness of cybersecurity training methods. Prümmer *et al.* (2024) highlighted generally positive outcomes from training, though noted issues with small samples and lack of real-world application. Bada *et al.* (2019) and Dash and Ansari (2022) stressed that awareness alone is insufficient to change behaviour, calling for training approaches that are relevant, motivating and context-sensitive. However, many of these efforts focus on formalised formats, paying less attention to the informal and blended methods that often shape learning in practice. The present study builds on this by mapping the full range of training formats and development opportunities encountered in vocational institutions.

Despite the hands-on nature of vocational education, where staff regularly work with or oversee sensitive systems and real data, there is surprisingly little research into cybersecurity in this context. Educational institutions are not classified as essential or important entities under the NIS2 Directive (EU Directive 2022/2555), yet they remain fully accountable under the GDPR for safeguarding personal data. Moreover, vocational education and training (VET) institutions prepare professionals for critical sectors such as health, transport and digital services, meaning their cybersecurity responsibilities at least indirectly extend beyond their immediate institutional boundaries. There might be differences in how these matters are approached in different educational settings. Understanding the VET landscape helps building holistic awareness of all levels of educational institutions. However, previous research has not sufficiently addressed how well vocational education and training institutions are equipped to protect their own information environments while also meeting wider cybersecurity responsibilities in practice, particularly in terms of staff awareness, skills and training. This oversight may relate to the relatively marginal status of VET in many countries compared to academic education (Ferm, 2021). By examining both institutional conditions and professional competencies related to cybersecurity, the present study contributes to filling this gap.

The present study focuses on cybersecurity hygiene of the VET sector by asking:

RQ1. How do staff members of Finnish vocational education institutions perceive the awareness and skill level of the staff with respect to information and cyber security?

RQ2. What trainings and other tools or sources for skill development are identified by the staff members of Finnish vocational education institutions with respect to information and cyber security?

1.3 Theoretical framework

Organisational learning theory, and particularly the concepts of single-loop and double-loop learning introduced by Argyris and Schon (1978), offers a valuable lens for understanding how staff develop cybersecurity competence within organisations. In recent years, this theoretical approach has also been applied in cybersecurity research. For instance, Mahmood *et al.* (2024) used learning loops to analyse counterstrategies in the higher education and research sector during crises, while Maynard *et al.* (2022) proposed a conceptual framework illustrating how the integration of information security management and incident response enables organisational learning. Both studies highlight how organisational learning frameworks can explain not only behavioural change but also how organisations adapt their structures, routines and mental models in response to evolving security challenges.

In Argyris and Schön's (1978) framework, single-loop learning describes situations where individuals adjust their actions to meet rules or expectations without questioning the assumptions behind them. Cybersecurity training that focuses on procedural knowledge, such as identifying phishing emails or locking screens, typically supports this type of learning. It is useful for ensuring basic compliance, but it does not necessarily address deeper questions about why certain practices exist or whether they remain fit for purpose. Double-loop learning, by contrast, involves a more reflective process where individuals and organisations critically examine the beliefs and norms that shape current practices. In the context of cybersecurity, this means engaging with the reasons behind policies, reconsidering how risks are assessed, or adapting training to role-specific realities. This kind of learning is especially relevant in dynamic environments, where rigid adherence to existing routines may not be sufficient to respond to new or complex threats.

Argyris's later work (1982, 1990, 1999) further developed the idea that defensive routines in organisations often block double-loop learning. These routines may include an overreliance on standardised training, avoidance of critical discussion, or assumptions that staff needs are uniform. Such patterns limit an organisation's ability to question its own cybersecurity approach, even when gaps are evident. This is particularly relevant in our study, where several participants reported that available training felt too general or did not align with their actual responsibilities.

2. Methods

2.1 Data and collection

Given the nature of our research questions, thematic interviews together with thematic analysis is an enough flexible yet systematic approach for examining perceptions on awareness and skill level as well as identified trainings (Nowell *et al.*, 2017). It is important to note that although digital threats and security processes are seen and addressed differently in various roles within educational institutions, these issues still affect everyone in the organisation. All staff members must be aware of and engaged with digital safety, regardless of their specific job responsibilities. This is why our study includes staff members in varying roles at Finnish vocational schools, instead of focusing for example on teachers.

Our data set consists of 25 semi-structured interviews (Amis, 2005), conducted face-to-face during the spring of 2024 in three vocational schools across five different locations in Finland. Additionally, the data set includes some transcribed observation notes. The total

duration of the interviews is just under 22 h, with each interview averaging slightly over 50 min. Out of the 25 interviews, 24 were individual interviews, and one involved three participants who were part of a team focused on a specific area of expertise (that is, altogether 27 informants in the study). This group interview was conducted with a team that regularly works together and shares responsibilities in a specific digital service area, and there was no official hierarchy among this group. To minimise potential group bias, the interviewers paid attention to ensuring that each participant was given space to express their views. In the analysis phase, this group interview was treated the same way as individual ones, but we also noted where responses were clearly collective. We considered the data to be rich and valuable to the research questions. Each vocational school in the data set operates in multiple locations within Finland, and one of the schools is a vocational special education institution.

These interviews were conducted as part of a project investigating cybersecurity competences and risks in vocational schools. The interview questions were divided into three sets: one for digital experts and IT management, another for leadership and a third for academic administration. Depending on the question set, interviewees were asked about their views on the information and cybersecurity risks of the school, as well as the related organisational processes, training and response strategies for suspected data or cybersecurity incidents. Initally, separate observation was planned. The aim of the observations was to follow everyday practices. Although the intention was to closely observe the daily life of vocational school employees, this proved challenging due to the fast-paced nature of data collection. Schedules could not be properly coordinated, and the target schools did not fully understand the purpose of our observations, preventing us from integrating into the daily life of the schools as authentically as we had hoped. However, we did spend a few hours observing teaching, leadership activities and IT operations in the schools. Observation notes were produced accordingly.

We agreed on the data collection with the schools according to the practices of each educational institution before the start date of the research project. From each school, we interviewed the rectors or vice-rector and contacted potential interviewees they indicated. We informed the rectors and vice-rectors that we were interested in interviewing employees, especially from IT management, digital pedagogy, student offices, teaching staff and preferably a counsellor or nurse. We interviewed a diverse group of professionals, whose job titles included teacher, special education teacher, digital tutor, study secretary, data protection officer, IT manager, director of digital services, systems designer or counsellor. Despite the research agreement made with each school, we additionally asked for permission for data collection separately from each interviewee via email and at the beginning of the interview. We also emphasised that participation in the interview was voluntary and that the supervisor would not know if the interviewee decided not to give permission for data collection or later decided to withdraw their participation.

All interviews were conducted in Finnish, with one or two interviewers from the research team present. We followed a semi-structured interview approach, which gave us both structure and flexibility (Amis, 2005). A role-specific semi-structured interview guide was used in data collection. The full list of questions is included in Appendix. In the first school, the interview guide was followed quite strictly, and only one interviewer was present. In the second and third schools, a technical cybersecurity expert joined most of the interviews as a co-interviewer. In those cases, the guide worked more as a loose framework to support the conversation, rather than a fixed list of questions. This allowed us to explore the schools' specific risks and threat perceptions more deeply. While we made sure that all the main topics were covered, we also allowed space for follow-up questions and new directions when

something interesting came up. This fits with the idea of semi-structured interviews where the researcher has a list of topics, not necessarily a full script, and the conversation can develop naturally (Ruslin *et al.*, 2022). As the interviews went on, some new and important themes started to emerge. Because of this, the interviews in the second and third schools became a bit more conversational and flexible. This helped us collect richer and more detailed set of data.

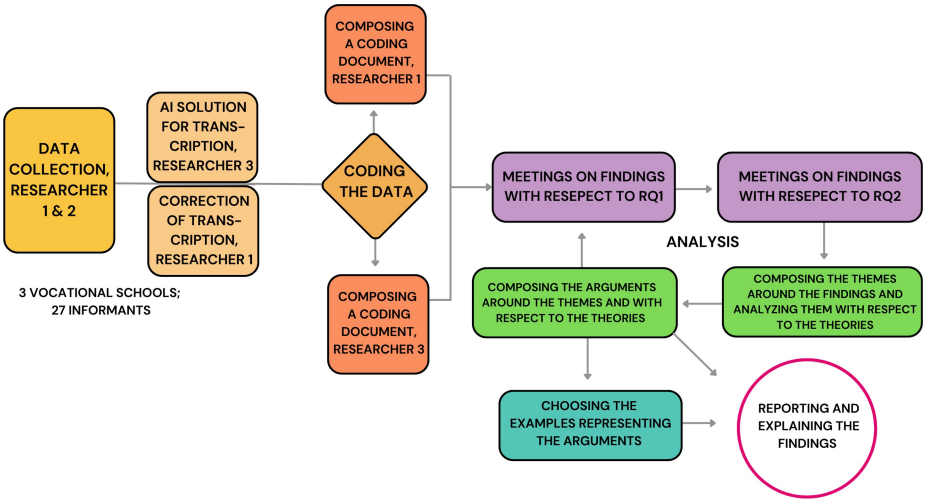
Due to time limitations in a couple of interviews, not every participant was asked every single question. We, however, paid close attention to make sure that the data was strong and deep enough to answer our research questions. We also wanted to keep the balance between sticking to our plan and being open to new topics as they came up. This is important in qualitative interviews, where we also see knowledge as being shaped by the situation and the context (Ruslin *et al.*, 2022). That's why we also made an effort to discuss the participants' roles, their typical tasks and the specific digital systems they use in their daily work. Understanding this context helped us interpret their views on cybersecurity more accurately.

Many informants had clearly prepared for the interviews and had also investigated their organisations' guidelines. Some had checked the staff pages, some used the organisation's guidelines during the interview, and one brought a newspaper clipping which she showed as an example of how she had oriented to the interview session. The interviews were fully transcribed using the largest multilingual model ("large") of the Whisper speech recognition system (OpenAI, 2023), and subsequently checked and edited by one of the authors. Whisper is an open-source automatic speech recognition system developed by OpenAI, which uses a deep learning model to transcribe spoken language into text. We used the system locally within our closed network, ensuring that no data left our internal infrastructure. The data has been anonymised, and speech patterns have been generalised to a degree that neither the individuals nor their schools can be identified from the transcribed material.

2.2 Analysis of the data

The data was analysed thematically using an inductive approach (Thomas, 2006; Braun and Clarke, 2006). In this study, the analysis began by using the research questions to guide the coding process, which is typical for inductive studies (Azungah, 2018). We examined the transcripts line by line and coded the segments of the text which were relevant to the research questions. In line with the inductive approach, neither the codes nor the themes were predetermined, but instead emerged from the data itself during this process, as patterns were identified and interpreted. Samples of different patterns were extracted into separate analysis documents by two researchers independently: one who conducted the interviews and one who did not take part in any of them. The coding was done one research question at a time, and after each coding phase, the researchers held meetings to discuss their findings. Gradually, the data-driven analysis of the identified patterns was developed through discussions between the researchers. The process is presented in a schematic form in Figure 1. For the first research question, the categories of "the good", "the bad", and "the ugly" emerged. For the second research question, it was decided to first expand the coding to include not only the training organised by the institution but also other forms of learning. This expansion was important because it allowed us to reach one of our key findings, which emerged through these discussions and this expansion: organisation's cybersecurity hygiene does not rely solely on the organisation's own training programs. Instead, organisations should systematically recognise, enable, and support all the various forms of skill development means that are highlighted in this study as employees' learning sources.

The figure illustrates the research process used in this study. On the left (orange), it shows data collection, transcription and initial coding, which two researchers conducted



Source: Created by authors

Figure 1. Overview of the analysis process

independently using shared coding documents. On the right (purple and green), the diagram outlines the analysis phase: purple marks collaborative meetings to discuss individual insights, while green highlights independent development of arguments and selection of illustrative examples. The loop-structure reflects the iterative nature of qualitative research, which is rarely as linear as research reports suggest (Marshall and Rossman, 2006, p. 23). This process involved repeated revisiting of data, themes and theory to deepen interpretation.

Rather than guiding the analysis from the outset, theoretical concepts were introduced at a later stage to help situate the findings within existing research. This is consistent with Thomas (2006), who argues that, in an inductive approach, insights should emerge directly from the raw data, with theory incorporated subsequently to contextualise the results. Given the limited amount of prior research on cybersecurity in vocational education, we allowed the data to shape both the structure and emphasis of the findings. In the latter stages of analysis, relevant literature was used to reflect on and interpret the emergent themes. In particular, Argyris and Schön's (1978) and Argyris' (1982, 1990, 1999) theories of organisational learning, and especially the distinction between single-loop and double-loop learning, proved useful in identifying whether staff adhered to established protocols or engaged in deeper reflection about the adequacy of existing cybersecurity practices. These concepts provided a framework for understanding how learning occurred within the institutions and why certain behavioural patterns persisted despite general awareness of cybersecurity risks.

In our findings, we highlight interview examples from all the different organisations and employees in various job roles. Some of the examples clearly represent a broader pattern found in the data, while others are examples with only few cases, which we also mention in connection with the examples. However, the number of cases in different categories is not as important in qualitative research as it is in quantitative research, due to the small sample size (Christou, 2022). Generally, as the sample size increases, more cases will appear in different categories. The aim of thematic qualitative research is more about identifying relevant

categories through rich data, rather than focusing on the number of cases (Christou, 2022). All examples have been translated into English and have been generalised where necessary, so that the interviewees cannot be identified, even by the representative organisations.

3. Results

3.1 The level of staff's cyber hygiene is perceived to be highly variable

Interviews reveal that there is a big variance in cyber hygiene skills, and this is stated directly in several interviews, for example in the following interview of a vice-rector of the vocational school:

> I: Well, the variation in levels is probably very large. It ranges from data protection officers and system experts to, at the other end, newly arrived teachers or substitutes, whose background might mean their levels are very low.

Some informants, however, were very aware, which can be noticed from how they considered various threat and risk factors to their organisation's information and cyber security and their own cyber hygiene practices related to it, as the following teacher reflects:

> I: In my opinion, the biggest risk is, of course, always the individual. If you think about it at a basic level, it's about being careless. I could be careless, or a colleague could be careless, leaving papers or computers open in the wrong places, and so on […]. But then there's also the risk of someone from outside wanting to harm us and gaining access to our systems to share some information […] But of course, how much one can influence this is quite small, as long as you follow the guidelines and don't neglect the basics.

However, we notice that even the more aware ones can face incidents, as seen in the same teacher's interview:

> I: For example, once during a lesson, I had a group of students from another field. I was teaching first aid, and I had my computer on. It wasn't connected to our student systems, but it had internet access. One student had opened a streaming channel on it. Luckily, I noticed it as soon as I entered the classroom, but it could have been streaming all day.

The teacher in the extract above was one of the more skilled ones, as was found out in other parts of the interview. However, this example shows that awareness does not always translate into cyber hygienic action in fast-paced educational contexts.

In addition to very aware and skilled staff-members, some employees were considered to be less so interested in or aware of information and cybersecurity themes, similar to society at large. We categorised the main findings under *The Good*, *The Bad*, and *The Ugly* based on whether employees perceived their organisation's awareness and skills good or bad, or if their experience was completely at odds with other assessments. The Good includes awareness and practices that were generally strong. The Bad includes skills that appeared uneven or insufficient. The Ugly captured more complex or conflicting situations, for example, where individuals were aware of risks but still failed to act accordingly. These labels are intended as practical tools to illustrate variation, not as value judgments about individuals or institutions. This classification helps identify not only levels of competence but also tensions and gaps in perception and behaviour, which are particularly relevant when designing training interventions. The categories can be seen in Table 1.

As illustrated in Table 1, the variation in cybersecurity awareness and skills among staff is not only technical but also attitudinal and perceptual. These findings suggest that effective development strategies must support both the content and relevance of training while also fostering active engagement. This ensures that perceived awareness translates into actual cyber hygiene practices. As Bada and colleagues (2019) point out, merely providing information is

Table 1. Categorised staff perceptions and notions of cybersecurity awareness and skills: Positive, negative and ambiguous themes ($n = 27$, from three organisations)

Category	Main findings of the perceptions and notions
The good	• Technical support staff often possess adequate cybersecurity skills and awareness • There is general improvement in awareness and practices over recent years • Cybersecurity training is available and, when aligned with job roles, strengthens both awareness and cyber hygiene practices • Some staff instinctively apply good cyber hygiene in their roles, such as avoiding identifiable data in student work or guiding students to manage sensitive material securely
The bad	• Awareness and skills are inconsistent, especially outside IT roles • Some staff show weak understanding of practical cyber hygiene measures, including safeguarding real customer data in school environments. There was also mentions that especially cyber incident or crisis readiness is at a low level • Basic good practices are sometimes bypassed for convenience in teaching settings
The ugly (discrepancy with reality)	• Some staff (especially non-technical personnel) perceive the organisation's overall cyber hygiene competence to be high, despite evidence to the contrary from peers and observations • Individuals with lower levels of skill and awareness often remain silent, which may be more concerning than visible uncertainty • Many staff assumed that external placement organisations train students in cybersecurity, but this was not confirmed or coordinated • Despite informants indicating the topic's importance during interviews, this attitude is not necessarily reflected in actions related to skill development nor day-to-day practices

Source(s): Created by authors

insufficient because attitudes, intentions and motivation are essential for turning awareness into secure everyday behaviour. Discrepancies in self-assessment and organisational perceptions (The Ugly) point to a need for more systematic and continuous organisational learning. Similarly, the uneven distribution of skills and low readiness outside technical roles (The Bad) emphasise the importance of tailored training approaches. Furthermore, the strong practices perceived in technical support and certain trained individuals (The Good) offer valuable models for peer learning and institutional benchmarking.

Generally, it can be said that although all informants in the interviews showed some interest in the topic and considered skills and training important as well as noticed cybersecurity hygiene being increased during past years, the subject is not necessarily the most interesting to the staff overall, as the information security manager demonstrates in his interview example:

> I: It somehow feels like what we want to communicate, educate and instruct from an information security perspective often falls on deaf ears. Last year's information security week, we offered two experts through our intranet for the entire week to help with the information security course or to generally discuss and provide guidance on information security issues. Not a single staff member visited, even though we had open doors.

Furthermore, some internal tests conducted in the vocational schools show that many slip up, as become apparent in the data. This indicates that not everyone is fully aware of cybersecurity hygiene or follows the recommended practice, as also the categories of *the Bad* and *the Ugly* highlight. For example, while some organisations have implemented embedded phishing exercises as part of awareness efforts, recent studies (Ho *et al.*, 2025; Lain *et al.*, 2022) suggest that these may have limited long-term impact, and highlight the greater effectiveness of ongoing, context-specific training programs, an observation that aligns with our interviewees' emphasis on continuous learning over isolated tests. The data also shows that those who are less familiar with or not responsible for creating information and cyber security processes are more likely to see competencies as good. Those more familiar or whose job includes monitoring information security, data protection, or cyber security, more easily mentioned that the skills in the institution are poor or variable, which is unsurprising due to the low level of cyber hygiene exhibited by a large part of the workforce (Pedley *et al.*, 2020).

3.2 Trainings and skill development methods

When we asked employees of educational institutions whether they receive any training on information and cybersecurity topics, we received a variety of responses on forms of training. The most common of the mentioned were basic course for all employees or short training sessions, as in the following example of a student affairs secretary:

> R: Do you remember if you had any kind of training or other sessions where you were introduced to these topics?
>
> I: Yes, we do have an online cybersecurity training. There's a basic level that everyone has to take, and then there's an additional level for us.
>
> R: Right. Are there aspects of it that fit well with your job?
>
> I: Well, yes, it's quite relevant to my current job. Data protection is a major focus for us, so it covers things like where documents are kept, where they're left out, whether they're locked up, and so on. And then, making sure the computer is in a locked area when you leave the room, that kind of thing; it's always present.

You can tell from the interview that the trainings provided have aligned well with the student affairs secretary's specific job role. However, some interviewees specifically pointed out that the training programs fail to address certain information and cybersecurity risks, as well as risk mitigating practices, that are particularly relevant to specific institutional roles, such as teaching. For example, one informant reflects the offered training: "But indeed, since it was generally about information security, there might be a need to specify it further to address teaching work, specifically, so that at some point we would have something tailored for our teachers".

Some of the interviewees did not mention any trainings organised by the employer at all when responding to our question, and some brought up other forms of skill development. Also, in different parts of the interviews, the respondents mentioned various formal and informal forms of training and skill development through which they learn about information and cybersecurity or maintain their skills. We have compiled all the different forms of training and skill development mentioned in the data into the table below, where we have also noted who organises or maintains the training in our educational institutions, as Table 2 showcases.

Some forms of skill development and training in the table are mentioned in several interviews, such as the basic course for all employees. Others are mentioned in one or two interviews, such as industry meetings or product webinars. Interestingly, as the table

Table 2. Formal and informal competence development types of staff cybersecurity skills in Finnish vocational education institutions

Category	Training/skill development method	Organised by
Formal trainings or methods for skill development provided by the employer	• Basic course for all employees	Employer
	• Continuous training with yearly or more interval	Employer
	• Testing of learned skills and information security tests (e.g. e-mails with links one should not open)	Employer
	• Information emails with related content	Employer
	• Recurring video content	Employer
	• Guidelines (no specific mention of the topic)	Employer
Formal trainings or methods for skill development provided by external parties	• Cyber exercise (mainly for directors and IT management personnel)	National digital and population data service agency
	• System administrator group meetings	Commercial service providers
	• Industry meetings for IT management	Commercial service providers
	• Product webinars	Commercial service providers
	• Networks between educational institutions	Other education institutions
	• Personal studies related to the topic alongside work	Other education institutions
Formal trainings or methods from unknown sources	• Gamified training	Provider unknown, but apparently not the employer
	• Training days [although dubious that such days are arranged.]	Provider unknown, but apparently the employer or the national administrative body
Informal trainings or means for skill development	• Colleagues within the institution	Personal networks
	• Personal networks between educational institutions	Personal networks

Source(s): Created by authors

indicates, a significant portion of staff competence development occurs outside of formal, employer-organised training. This includes informal peer learning, participation in external professional networks and webinars or exercises organised by national or commercial actors.

Furthermore, interestingly, four participants did not recognise any official training organised by the institution or recognises something which is not in line with their own thoughts on information or cybersecurity issues, although the rector or vice-rector of each institution stated that the basic course for all employees is required for every staff member. For example, one participant explained the following:

> R: Well, do you then train staff in these kinds of cybersecurity matters?
>
> I: No. Not really. I guess it's like, we don't exactly know in what way to approach it, or maybe [says a name] would instruct us on it, like everyone on the staff had to do that kind of security test, but it didn't cover threats like these.

However, all rectors or vice-rectors of the three organisations claimed them to have trainings regularly.

It was also notable that training and networks organised by external actors, such as service providers, educational institutions, or national bodies, played a clearly significant role, particularly in role-specific orientation and support. These structures were also assumed to contribute to maintaining and updating competencies related to cybersecurity awareness and hygiene, as illustrated in the following interview with an academic administration specialist:

> R: Well, do you recognise any collaboration groups or other networks where you can reflect on your work with others doing similar tasks, and discuss practices or seek support?
>
> I: Yes, we do have such a network, for example, a PKW network for student information and student management system users with administrative privileges. We meet once a month on Teams. It's really good. And we also collaborate between educational institutions, both officially and unofficially to some extent.
>
> R: The administrator group, isn't there a huge number of participants? […]
>
> I: Well, practically, there are always around a hundred, a bit over a hundred.
>
> […] R: Does it cover all of Finland from your perspective?
>
> I: Yes, it does.
>
> R: And who maintains it?
>
> I: Well, it started from one vocational institution […].

It has been running for several years now, and it's really good. It's called PKW morning coffee, once a month. An hour for that. Everyone can bring their own issues to it. Peer support. And discussions also happen outside of that:

> R: Are there any development days or external events you participate in?
>
> I: Yes, there are. First, there are the company days offered by the service provider. And then there are also some training sessions organised by Finnish National Agency for Education on current

> topics and such. But they are more in the form of webinars. But there are forums. And you can always ask colleagues from elsewhere.

Which aspects of cybersecurity hygiene are covered in these trainings or competence development occasions remained unclear in our data. However, it is evident that some awareness, understanding and knowledge on cybersecurity hygiene is offered via these networks and trainings.

We systematically asked interviewees how they are trained to support students during their work-based learning periods and how they are instructed to secure the school-based learning environments where real customer data is handled. None of the participants reported receiving any specific training or guidance from their employer regarding these responsibilities. Based on the responses, no one mentioned acquiring such knowledge through informal means either. Despite this, some staff members described taking these concerns into account instinctively when supervising students or planning and delivering their teaching. For example, one teacher working in healthcare education explained that they are particularly strict about ensuring no identifiable information about clients appears in students' written work, let alone in any submitted images. However, our observational data also highlighted notable shortcomings. For example, in one vocational school's automotive workshop, customer data was openly displayed on a large screen without a lock screen or user-specific login. In that case, the system was intentionally left unlocked throughout the lesson, as it was considered more practical for both teachers and students to avoid logging in repeatedly. In addition, many respondents said they assumed that the organisations hosting students for placements would provide cybersecurity and data protection training, but none reported that this had been verified or coordinated in any systematic way.

3.3 Organisational learning in vocational education cybersecurity

The findings of this study align closely with the concepts of single-loop and double-loop learning introduced by Argyris and Schön (1978) and further developed by Argyris (1982, 1990, 1999). Most participants described formal cybersecurity training in the form of mandatory basic courses or short refreshers. These support rule-based behavioural adjustments, such as document handling or workstation security, which reflect single-loop learning. While helpful for day-to-day operational compliance, these trainings generally lacked depth and role-specific adaptation, particularly for teaching staff. Thus, a need for training that addresses the unique risks associated with different institutional roles would be needed. This absence of reflective, tailored learning suggests a missed opportunity for double-loop learning, where individuals would question the adequacy of existing policies in light of emerging threats such as phishing or hybrid work vulnerabilities. As Argyris (1990) noted, such deeper learning is often constrained by organisational cultures that prioritise conformity over critical inquiry and fail to create space for open reflection.

At the same time, the data revealed informal learning environments, such as peer networks, administrator groups and monthly collaborative meetings, that may offer better conditions for double-loop learning. These settings encourage shared reflection, questioning of everyday practices and the creation of new ways of working, which Argyris and Schön (1978) saw as key to moving beyond surface-level learning and supporting real change within organisations.

This reflective capacity is particularly important in the VET sector, where institutions not only maintain their own cybersecurity posture but are also involved with critical fields under NIS2 through the training of professionals and cooperation with industry partners. The ability of staff to engage in adaptive, context-aware learning directly influences how cybersecurity values and practices are passed on to future professionals. Students may, for example, submit learning assignments that include photos or videos taken in hospitals or energy companies, which makes it essential that teachers understand the cybersecurity risks

involved and are able to guide students on how to share such material in ways that do not compromise the data or systems of partner organisations. This requires not only awareness of basic rules but also a capacity for double-loop learning, where teachers critically reflect on the adequacy of existing guidelines and adapt their instructions based on the specific contexts and evolving risks related to each learning environment.

4. Discussion

This study reveals wide variation in cybersecurity awareness and skills among staff in Finnish vocational education institutions. While some were highly competent, others had limited knowledge, particularly those not directly involved in cybersecurity tasks. Those with greater responsibility tended to assess organisational competence more critically, indicating a gap between perceived and actual capability. Although all three institutions had mandatory training protocols, implementation and monitoring were inconsistent. Some staff completed formal courses, others recalled only general email instructions or nothing at all. This supports earlier findings that awareness alone does not ensure behavioural change (Bada *et al.*, 2019; Dash and Ansari, 2022). Much learning occurred informally through peer networks, professional webinars and practical experience, which proved essential in developing real-world competencies.

The findings align with Argyris and Schön's (1978) organisational learning theory. Most formal training matched single-loop learning, focused on compliance and routine behaviour. These programmes help staff follow procedures, such as locking workstations or handling documents securely, but rarely prompt reflection on the adequacy of current policies or practices. Double-loop learning, further elaborated by Argyris (1982, 1990, 1999), involves questioning underlying norms and adapting behaviour accordingly. In this study, such deeper reflection emerged mainly in informal settings like peer support networks or national administrator meetings. These allowed for shared experiences, collaborative problem-solving and critical discussion which are all essential features to adaptive learning. Reflective capacity is particularly crucial in vocational education, where institutions do not only maintain internal cybersecurity but also train professionals for NIS2-relevant sectors like healthcare and digital infrastructure. Staff often supervise students using real systems or working with sensitive data, highlighting the need for teachers to understand cybersecurity risks and guide safe practices.

The study also supports prior research pointing to the limitations of generalised training models. Many staff noted the lack of role-specific content, echoing calls for tailored training (Abrahams *et al.*, 2024; Prümmer *et al.*, 2024). Continuous and context-aware programmes are more effective than one-off initiatives (Concepcion and Palaoag, 2024; Asker and Tamtam, 2020). External service providers play an increasing role in training and daily problem-solving, especially as institutions move toward cloud-based solutions (Thavi *et al.*, 2024).

These findings highlight the complex responsibilities faced by vocational education staff in maintaining cybersecurity. Staff are required to protect their institution's critical data and digital processes, which vary depending on their role. This includes systems for awarding qualifications and managing academic records, handling learning evidence, using classroom technologies and maintaining cloud-based services and simulated workplace environments that may involve real customer data. At the same time, staff are responsible for guiding students who regularly take part in work-based learning in sectors such as health care, energy and transport. During these placements, students may be exposed to or manage sensitive information and might also submit assignments containing photos or descriptions derived from real-world contexts. It is therefore essential that staff not only understand the associated risks but are also able to instruct students on how to manage and share such material securely. However, we found no evidence that the handling of real data in workplace or simulated settings is addressed

systematically in training or policy. The control and protection of such data is largely left to staff discretion, which creates uneven practices and potential vulnerabilities.

This dual responsibility demands training that moves beyond basic procedural awareness and takes into account the specific contexts in which both staff and students operate. It also highlights the value of reflective learning approaches, which enable staff to critically evaluate and adjust their cybersecurity practices. While such strategies help build organisational resilience and support safer learning environments, it is important to recognise that even well-informed individuals can still make errors (Triplett, 2022; Evans *et al.*, 2016), reinforcing the need for ongoing institutional support and continuous learning.

References

Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O. (2024), "Cybersecurity awareness and education programs: a review of employee engagement and accountability", *Computer Science and IT Research Journal*, Vol. 5 No. 1, pp. 100-119.

Althonayan, A. and Andronache, A. (2018), "Shifting from information security towards a cybersecurity paradigm", in *ICIME 2018: Information Management and Engineering*, *Association for Computing Machinery*, New York, NY, pp. 68-79.

Amis, J. (2005), "Interviewing for case study research", in Andrews, D.L., Mason, D.S. and Silk, M.L. (Eds), *Qualitative Methods in Sports Studies*, New York, NY, Berg, pp. 104-138.

Anesone, A.R. (2024), "Cybersecurity within organizations: who should be responsible for ensuring that the organization is protected against cybercrime?", *International Journal of Advances in Computer Science and Technology*, Vol. 13 No. 9, pp. 107-110, doi: 10.30534/ijacst/2024/011392024.

Argyris, C. (1982), *Reasoning, Learning and Action: Individual and Organizational*, Jossey-Bass, San Francisco, CA.

Argyris, C. (1990), *Overcoming Organizational Defenses: Facilitating Organizational Learning*, Prentice Hall, Upper Saddle River, NJ.

Argyris, C., and Schon, D. (1978), *Organizational Learning: A Theory of Action Perspective*, Addison-Wesley, Reading, MA.

Asker, H. and Tamtam, A. (2020), "An investigation of the information security awareness and practices among third level education staff, case study in Nalut libya", *European Scientific Journal, ESJ*, Vol. 16 No. 15, pp. 20-32, doi: 10.19044/esj.2020.v16n15p20.

Azungah, T. (2018), "Qualitative research: deductive and inductive approaches to data analysis", *Qualitative Research Journal*, Vol. 18 No. 4, pp. 383-400.

Bada, M., Sasse, A.M. and Nurse, J.R. (2019), "Cyber security awareness campaigns: Why do they fail to change behaviour?", arXiv preprint arXiv:1901.02672.

Baraković, S. and Baraković Husić, J. (2022), "Cyber hygiene knowledge, awareness, and behavioral practices of university students", *Information Security Journal: A Global Perspective*, Vol. 32 No. 5, pp. 347-370, doi: 10.1080/19393555.2022.2088428.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101.

Butler Lamar, S. (2022), "Managing cyber hygiene at a higher education institution in the United States", SAIS 2022, Association for Information Systems, pp. 1-6, available at: https://aisel.aisnet.org/sais2022/5

Cains, M.G., Flora, L., Taber, D., King, Z. and Henshel, D.S. (2022), "Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation", *Risk Analysis*, Vol. 42 No. 8, pp. 1643-1669.

Christou, P.A. (2022), "How to use thematic analysis in qualitative research", *Journal of Qualitative Research in Tourism*, Vol. 3 No. 2, pp. 79-95.

Concepcion, J.D. and Palaoag, T.D. (2024), "An assessment of cybersecurity awareness among academic employees at Quirino state university: promoting cyber hygiene", *Journal of Electrical Systems*, Vol. 20 No. 7, pp. 769-775.

Dash, B. and Ansari, M.F. (2022), "An effective cybersecurity awareness training model: first defense of an organizational security strategy", *International Research Journal of Engineering and Technology*, Vol. 9 No. 4.

Evans, M., Maglaras, L.A., He, Y. and Janicke, H. (2016), "Human behaviour as an aspect of cybersecurity assurance", *Security and Communication Networks*, Vol. 9 No. 17, pp. 4667-4679, doi: 10.1002/sec.1657.

Ferm, L. (2021), "Vocational students' ways of handling the academic/vocational divide", *International Journal for Research in Vocational Education and Training*, Vol. 8 No. 1, doi: 10.13152/ijrvet.8.1.1.

Finland's Cyber Security Strategy (2024/2035), "Prime minister's office helsinki 2024", VN/36693/2023: 978-952-383-462-0, Helsinki, available at: https://urn.fi/URN:ISBN:978-952-383-462-0 (accessed 13 June 2025).

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Liu, L., Longhurst, A.A., Dameff, C., Savage, S. and Voelker, G.M. (2025), "Understanding the efficacy of phishing training in practice", *Paper presented at the 2025 IEEE Symposium on Security and Privacy (SP), May 2025, San Francisco, CA, USA*, doi: 10.1109/SP61157.2025.00076 (accessed 1 April 2025).

IEEE (2020), "Cybersecurity for a stronger and more resilient digital Europe. An IEEE european public policy committee position statement", available at: www.ieee.org/content/dam/ieee-org/ieee/web/org/about/european-public-policy/cybersecurity-position-statement-dec-2020.pdf (accessed 21 November 2024).

Lain, D., Kostiainen, K. and Čapkun, S. (2022), "Phishing in organizations: Findings from a large-scale and long-term study", *Paper presented at the 2022 IEEE Symposium on Security and Privacy (SP), May 2022, San Francisco, CA, USA*, doi: 10.1109/SP46214.2022.9833766 (accessed 1 April 2025).

Mahmood, S., Chadhar, M. and Firmin, S. (2024), "Countermeasure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: an organisational learning perspective", *Information*, Vol. 15 No. 2, p. 106.

Marshall, C. and Rossman, G.B. (2006), *Designing Qualitative Research*, 4th ed., Sage, Thousand Oaks.

Maurer, T. and Morgus, R. (2014), *Compilation of Existing Cybersecurity and Information Security Related Definitions, Report*, New America, Washington, DC.

Mims, N.A. (2024), "Cyber attack process", in Vacca, J. R. (Ed.), *Computer and Information Security Handbook*, 4th ed., Elsevier, London, pp. 1381-1393, doi: 10.1016/b978-0-443-13223-0.00088-6.

Nowell, L.S., Norris, J.M., White, D.E. and Moules, N.J. (2017), "Thematic analysis: Striving to meet the trustworthiness criteria", *International Journal of Qualitative Methods*, Vol. 16 No. 1, doi: 10.1177/1609406917733847.

OpenAI (2023), "Whisper large-v3 (version large-v3), OpenAI", available at: https://github.com/openai/whisper

Pedley, D., Borges, T., Bollen, A., Shah, J.N., Donaldson, S., Furnell, S., and Crozier, D. (2020), *Cyber Security Skills in the UK Labour Market 2020*, Department for Digital, Culture, Media and Sport.

Prümmer, J., van Steen, T. and van den Berg, B. (2024), "A systematic review of current cybersecurity training methods", *Computers and Security*, Vol. 136, doi: 10.1016/j.cose.2023.103585.

Ruslin, R., Mashuri, S., Rasak, M.S.A., Alhabsyi, F. and Syam, H. (2022), "Semi-structured interview: a methodological reflection on the development of a qualitative research instrument in educational studies", *IOSR Journal of Research and Method in Education*, Vol. 12 No. 1, pp. 22-29.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.-J. (2009), "The impact of information richness on information security awareness training effectiveness", *Computers and Education*, Vol. 52 No. 1, pp. 92-100.

Thavi, R., Jhaveri, R., Narwane, V., Gardas, B. and Jafari Navimipour, N. (2024), "Role of cloud computing technology in the education sector", *Journal of Engineering, Design and Technology*, Vol. 22 No. 1, pp. 182-213.

Thomas, D.R. (2006), "A general inductive approach for analysing qualitative evaluation data", *American Journal of Evaluation*, Vol. 27 No. 2, pp. 237-246.

Triplett, W.J. (2022), "Addressing human factors in cybersecurity leadership", *Journal of Cybersecurity and Privacy*, Vol. 2 No. 3, pp. 573-586. available at: www.mdpi.com/2624-800X/2/3/29/pdf

Ugwu, C., Ani, C., Ezema, M., Asogwa, C., Ome, U., Obayi, A., Ebem, D., Atanda, M. and Ukwandu, E. (2022), "Towards determining the effect of age and educational level on cyber-hygiene", *IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Institute of Electrical and Electronics Engineers*, pp. 1-5.

Ulven, J.B. and Wangen, G. (2021), "A systematic review of cybersecurity risks in higher education", *Future Internet*, Vol. 13 No. 2, p. 39, doi: 10.3390/fi13020039.

Viano, A. (2024), "Cyberattacks on higher ed rose dramatically last year, report shows. EdTech", available at: https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows (accessed 14 November 2024).

Vishwanath, A., Neo, L.S., Goh, P., Lee, S., Khader, M., Ong, G. and Chin, J. (2020), "Cyber hygiene: the concept, its measure, and its initial tests", *Decision Support Systems*, Vol. 128, pp. 113-160.

Witsenboer, J., Sijtsma, K. and Scheele, F. (2022), "Measuring cyber secure behavior of elementary and high school students in The Netherlands", *Computers and Education*, Vol. 186, doi: 10.1016/j.compedu.2022.104536.

Further reading

Agyris, C. (1999), *On Organizational Learning*, 2nd ed., Blackwell Publishing, Oxford.

Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H. and Baskerville, R.L. (2020), "How integration of cyber security management and incident response enables organizational learning", *Journal of the Association for Information Science and Technology*, Vol. 71 No. 8, pp. 939-953.

Borrego, M., Amelink, C.T. and Douglas, E.P. (2009), "Quantitative, qualitative, and mixed research methods in engineering education", *Journal of Engineering Education*, Vol. 98 No. 1, pp. 53-66, doi: 10.1002/j.2168-9830.2009.tb01005.x.

Neigel, A.R., Claypoole, V.L., Waldfogle, G.E., Acharya, S. and Hancock, G.M. (2020), "Holistic cyber hygiene education: accounting for the human factors", *Computers and Security*, Vol. 92, p. 101731, doi: 10.1016/j.cose.2020.101731.

Sabato, S. and Scarlett, J. (Eds) (2025), *Proceedings of the 40th International Conference on Machine Learning*, JMLR, Cambridge MA, pp. 28492-28518.

Appendix 1. Interview Guide (English Translation)

This study used semi-structured interviews tailored to different professional roles in vocational education institutions. While certain warm-up and general cybersecurity questions were asked of all participants, role-specific sets of questions were used to ensure relevance, and follow-up questions were often applied. Below is the complete English translation of the interview guide, grouped by role.

1. Warm-up questions (asked to all participants)
   - What is your name?
   - What is your job title and what does it involve?
   - To which unit or department do you belong in your organisation?

- How did you come into your current role?

2. Conceptual framing (shared with all participants)

Definitions for terms used during the interview will be the following, please ask for more information whenever you need any:

- *Information security*: Refers here to protection to data handled in digital, paper or other physical environments.
- *Data protection*: Refers here to information protected by legislation or organisational policies.
- *Cybersecurity*: Refers here to preparedness for threats targeting digital systems, with consequences often extending to everyday offline contexts.

3. Role-specific question sets (also follow-up questions are allowed whenever needed)

A. Leadership and Management Roles

- In this project, we are studying information and cybersecurity risks and response capabilities in vocational institutions Can you describe what happens in your organisation when an information or cybersecurity incident is detected?
- Does your organisation use a systematic system (e.g. ticketing platform) for reporting incidents?
- Is there a system that records or quantifies incident data or reports?
- Who receives incident reports and how does the process continue?
- Are incidents categorised in more detail than just "security incident"?
- Do you recognise any external groups that support you in resolving security incidents?
- Which cybersecurity functions are managed internally and which are outsourced (e.g. because of other service providers)?
- What cybersecurity-related procedures come from external authorities (e.g. ownership organisations or vendors)?
- How have new technologies (e.g. AI or XR) been considered in your cybersecurity planning?
- What kinds of cybersecurity or data protection incidents have affected your organisation in the past?
- What do you consider to be the most significant cybersecurity threats in or to your organisation?
- Does your organisation have a crisis communication strategy related to cybersecurity?
- Whom would you inform if you noticed a cybersecurity incident?

B. On staff awareness and preparedness:

- Who do you consider that could pose a cybersecurity threat to your organisation?
- What do you consider to be the most likely, probable and severe consequences of a cybersecurity incident for your organisation?
- How do you perceive your staff's awareness level regarding information security incidents or their detection?
- How is your staff trained to handle these information and cybersecurity incidents? Their detection and response?
- Are students or other stakeholders, such as employers providing student internships, trained or guided in cybersecurity or data protection?
- How is digital safety supported or instructed in your simulated workplace learning environments?

C. IT and Digital services professionals

(Includes all questions listed for leadership and management, plus:)

- Are critical admin credentials and passwords (e.g., root/admin accounts or executive access) managed with backup or recovery procedures?

D. Teaching, student services and administrative staff
(e.g., teachers, secretaries, counsellors)

- What kinds of data protection or cybersecurity incidents do you know that have affected your organisation in the past?
- What do you consider to be the most significant threats to information or cybersecurity in your organisation?
- Whom would you inform if you noticed something that you think could be an information or cybersecurity incident?
- Who do you consider, that could pose a cybersecurity threat to your organisation?
- What do you consider to be the most likely, probable and severe consequences of a cybersecurity incident for your organization?
- How do you perceive your staff's awareness level regarding information security incidents or their detection?
- Are you trained in cybersecurity, data protection or information security?
- Are students or other stakeholders, such as employers providing student internships, trained or guided in cybersecurity or data protection?
- How is digital safety supported or instructed in your simulated workplace learning environments?

E. Incident reporting and data practices:

- Can you describe what happens in your organisation when an information or cybersecurity incident is detected?
- Can you mention three ways you could report a cybersecurity incident.
- What types of personal data do you acknowledge to handle in your daily work?
- Do you consider handling any particularly sensitive personal data?
- Do you consider having sufficient access to the data you need? Do you experience encountering data you should not have access to?
- Do you consider processing sensitive data concerning other organisations or third parties?

F. Work tools and practices:

- What tools do you use to process the data mentioned above?
- Do you use only organisation-provided devices, or also your own (e.g. laptop, phone)?
- Do you use only official systems, or also informal communication platforms (e.g. WhatsApp, Snapchat, Signal)?
- Do you use any unofficial meeting or presentation tools (e.g. Zoom, Canva, Google Meet)?
- Do you use any unofficial cloud storage services (e.g. Google Drive, Dropbox, OneDrive)?

Source: Created by authors

Corresponding author
Anna-Liisa Ojala can be contacted at: Anna-Liisa.Ojala@jamk.fi