SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Cybersecurity and incident response processes for maintaining operational security and continuity at vocational education institutions

Anna-Liisa Ojala[1], Tuomo Sipola[2], Karo Saharinen[3]

[1]Anna-Liisa.Ojala@jamk.fi

[1]https://orcid.org/0000-0002-5363-8425

[1]School of Professional Teacher Education, Jamk University of Applied Sciences, Rajakatu 35, 40600, Jyväskylä, Finland

[2]https://orcid.org/0000-0002-2354-0400

[3]https://orcid.org/0000-0002-8214-1426

[2,3]Institute of Information Technology, Jamk University of Applied Sciences, Rajakatu 35, 40600, Jyväskylä, Finland

Abstract

The presence of cybersecurity in educational institutions, including vocational education and training (VET), plays a vital role in ensuring the overall societal security in an increasing digital world. This study explores how staff of VET institutions respond to suspected cybersecurity incidents, focusing on reporting channels and methods used. The objective is to better understand incident response practices in the under-researched VET context, with special attention given to the human and organisational aspects of cybersecurity. VET institutions operate digital systems that mirror real workplace environments and often handle authentic customer data, exposing them to risks that differ from those of general education settings. A qualitative methodology was employed, consisting of thematic interviews with twenty-seven staff members across three Finnish vocational schools. The analysis was guided by the Situation Awareness in Cybersecurity Incident Response model and the Zone of Proximal Development framework, allowing for a deeper exploration of how staff perceive and act upon potential threats. Although formal reporting procedures exist, staff frequently rely on informal networks and direct contact with IT support. Urgent cases are often communicated via phone, a method perceived as efficient but lacking in documentation and structure, which can hinder post-incident analysis and learning. Improving cybersecurity incident response in VET institutions requires the integration of formal digital tools with flexible, human-centred communication methods. Strengthening these systems is essential, not only for protecting sensitive data, ensuring continuity, and creating safer learning environments, but also for reinforcing the digital resilience of society as a whole.

Keywords:

cybersecurity, human factors, societal security, educational institutions, incident response

Article info
Received: 11 April 2025
Revised: 19 September 2025
Accepted: 26 September 2025
Available online: 25 November 2025

Ojala, A.-L., Sipola, T. and Saharinen, K. (2025) 'Cybersecurity and incident response processes for maintaining operational security and continuity at vocational education institutions', *Security and Defence Quarterly*, 52(4), pp. 78–94. doi: 10.35467/sdq/211414.

Introduction

Vocational education and training (VET) focuses on instilling practical skills for specific jobs, along with general abilities that support personal growth and success in the workplace. As highlighted in the European Council recommendation of 24 November 2020, VET plays a key role in Europe in promoting sustainable competitiveness, social fairness, and resilience as well as in preparing young people to enter the workforce confidently and helping adults learn new skills or improve the existing ones. In 2022, a great number of upper-secondary students in the European Union (EU) chose a VET study pathway (Cedefop, 2025). In VET education, workplace training periods are part of both daily school activities and information systems (Organization for Economic Cooperation and Development [OECD], 2023). Through workplace training, students are involved in knowledge exchange between schools and workplaces, making the security practices at VET institutions influential on broader societal cybersecurity.

It is crucial for educational institutions to enhance cybersecurity maturity in order to safeguard their sensitive data, maintain their operational continuity, uphold brand and reputation, and promote a safe and secure educational and working environment and society. Academic studies have underscored the importance of developing robust cybersecurity frameworks within education institutions (Aliyu *et al.,* 2020). Recent discussions and research on cybersecurity have increasingly emphasised the importance of safeguarding societies through organisational operations and integrity, alongside traditional concerns like data protection and threat mitigation (Abrahams *et al.,* 2024). This more holistic approach considers not only digital activities within IT systems but also human actions across various operational processes.

Incident response is a vital element of cybersecurity, which helps to protect data, maintain continuity, and ensure a secure learning environment through timely detection, containment, and recovery from cybersecurity incidents (Cichonski *et al.,* 2012). However, the concept remains understudied in the educational sector. Sonhera *et al.* (2021) and Sonhera (2022) highlighted unclear procedures in South African schools and proposed structured reporting and response frameworks. Villegas-Ch *et al.* (2021) demonstrated how computer security incident response teams in universities can mitigate threats by following international standards. Yet, these studies do not address everyday practices and the development of situational awareness, often assuming that all staff can recognise incidents regardless of their role. This highlights the need for research on practical implementation and awareness-building. Our study addresses this gap by focusing on two early-stage aspects of incident response:

> **RQ1**: Who do the staff of vocational schools report to or rely on if they suspect cybersecurity incidents in information systems or data-handling?
>
> **RQ2**: What communication methods do the staff use when they report suspected cybersecurity incidents?

The rationale for examining these research questions stems from cybersecurity situation reports highlighted in the media and findings from the existing studies: Firstly, the occurrence of cyber incidents is more likely than unlikely in today's organisations (see, e.g. Celeny *et al.,* 2024). Secondly, the number of cyber incidents has increased within the educational sector (Viano, 2023), which has broad implications for societal security as educational institutions are integral to social infrastructure. Therefore, managing cyber incident response in the educational sector is crucial, as it helps to save time and resources, and prevents the situation from escalating further (Nelson *et al.,* 2025).

Our research draws on Endsley's (1995) situation awareness model, further developed by Ahmad *et al.* (2021) into the Situation Awareness in Cybersecurity Incident Response (SA-CIR) model. This framework helped us to examine how incident response unfolds in vocational education institutions—from frontline observations to the roles of IT support, security management, school leadership, and, when needed, external authorities and service providers. We also applied Vygotsky's (1978) concept of the Zone of Proximal Development (ZPD) to understand how school staff collaborate with more experienced colleagues to interpret digital practices, including distinguishing between normal system behaviour and events requiring reporting. Finally, we explored the tools that staff use for reporting, how they form perceptions, and how they build situational awareness in response to incidents.

Conceptual and theoretical background

Situation awareness and cyber incident response

Several previous studies demonstrated the applicability of Endsley's (1995) situation awareness model in enhancing cybersecurity practices across different organisational contexts (cf. Ofte and Katsikas, 2023). Endsley (1995) considers situation awareness, in general, as a process related to human decision-making. The background of this thinking can be traced back to aircraft, air traffic control, large-systems operations as well as tactical and strategic systems. Endsley's model consists of a feedback loop, having the situation awareness–decision–performance of actions pipeline as its core.

Ahmad *et al.* (2021) observed an excessive focus on the technological perspective of incident response. In contrast, they presented a process model based on real-world experience as a case study, leading to a model called Situation Awareness in Cybersecurity Incident Response (SA-CIR). The model includes three states of knowledge as defined by Endsley (1995): perception, comprehension, and projection. Perception is the first stage where raw information about the environment is collected. In incident response, this means gathering alerts and details about potential cybersecurity incidents from different sources. Comprehension involves understanding the collected data by combining key elements to see their importance. Projection is the highest level of situational awareness, where the current understanding is used to predict future events.

It is well known that the formulation of the SA-CIR model is an important phase in mitigating the risks of cybersecurity incidents. However, this issue has received very little attention from researchers overall (Ahmad *et al.*, 2021), especially in the educational sector. The present study focuses especially on the first two states of SA-CIR, perception and comprehension of cybersecurity incidents in VET institutions, although projection is also referred to in findings related to VET institutions' IT management and incident escalation. Building upon the conceptions of Ahmad *et al.* (2021) and Endsley (1995), we examined how staff members create understanding and how they analyse the nature of a potential incident, the need to respond to it, and the methods or tools through which the response is carried out.

Recent international frameworks and standards set the expectations for how organisations should approach incident response. The ISO/IEC 27035–1:2023 series by International Organisation for Standardisation & International Electrotechnical Commission, for instance, outlines a structured model for planning and managing security incidents, while the forthcoming revision of National Institute of Standards and Technology (NIST) SP 800-61 (Nelson *et al.*, 2025) updates earlier guidance to reflect current practices. In the

European context, the NIS2 directive (European Union [EU], 2023), together with the recommendations of the European Union Agency for Cybersecurity (ENISA), places strong emphasis on reporting duties, cooperation between organisations, and developing institutional capacities. Across these approaches, the recurring themes are the importance of clear escalation levels, systematic documentation, and the principle of continuous improvement. These benchmarks provide useful points of comparison for evaluating and strengthening incident response practices in VET institutions.

Previous studies also highlight that collecting meaningful and useful information about cybersecurity is referred to as cyber threat intelligence (CTI). This process requires proper standardisation to effectively relay information and support security incident response (Schlette *et al.*, 2021). Collecting such information demonstrates organisational maturity, and using standard methods to document cyber incident findings can help achieve it. Furthermore, the staff member that reports an incident, and how it is reported, directly influences the type and quality of information an organisation gathers about the incident as the process unfolds.

Zone of proximal development

Vygotsky's (1978) concept of ZPD builds upon the idea of a difference between the actual development level (ADL) and the learning potential of learners. Vygotsky asserted that there is a gap between what learners can achieve independently and what they can accomplish with guidance from a facilitator or peers, the latter being the ZPD. This idea emphasises learning as a collaborative process where support and interaction help learners to accomplish tasks and activities they would not have accomplished without external support. While Vygotsky's conception is often discussed in the context of children, it is apt also for explaining learning processes of adult learners, as the context of the present study shows.

Learning within the ZPD involves internal reflection and external interaction. Learners begin by internally processing challenges, often aided by speech and signs, and then turn to tools, resources, facilitators, or peers for help when they encounter problems they cannot solve alone (Clapper, 2015). Facilitators can use various methods, such as demonstrations, discussions, and case studies, to assist learners in overcoming these obstacles. Also, reflection and imitation are key aspects of this process. The gap between a learner's current ability to solve problems independently and their potential ability to solve problems with the help of a more experienced guide or capable peer gradually decreases as the learner successfully completes tasks and develops new skills (Vygotsky, 1978).

Vygotsky (1962, 1987) explained that development happens within social and cultural contexts, and learning is shaped by interacting with cultural artefacts. In his time, these artefacts included items like toys, different tools, language, art, and traditions. Today, we can see IT devices, software, and networks as modern cultural artefacts, also present in educational institutions (cf. OECD, 2023).

It is also important to highlight that ZPD is related to scaffolding but not identical to it (Clapper, 2015). Scaffolding refers to specific support strategies within the ZPD but is not always required. Learners may also progress through other means, such as imitation or cooperative learning, which encourage problem-solving and developmental growth by working together and learning from others. In other words, scaffolding is a teaching method where temporary support is provided to help learners accomplish tasks they cannot do alone, with the goal of gradually removing the support as they gain independence.

In the context of using ICT systems and incident response, the difference between ZPD and scaffolding could mean, for example, that in the ZPD, an employee informally asks a colleague or IT support for help and is able to act on that guidance, while in scaffolding, incident response is purposefully taught to employees by simulating situations and enabling them to perform proper analyses with assistance. In this study, ZPD became the key theoretical concept due to observations related to everyday incident response and analysis that emerged from the empirical data.

Methods

Data and collection

In incident response management, it is generally accepted that preventing incidents entirely is impossible (Cichonski *et al.*, 2012). However, their impact can be reduced with a systematic and effective incident response process, involving all employees in the organisation with different roles. Therefore, in this study, we engaged a wide range of staff members with various job roles in vocational colleges. The research method is qualitative, with the data consisting of semi-structured interviews and thematic analysis (Amis, 2005; Braun and Clarke, 2006). Through the interviews, we gained insights into everyday practices of employees that might not have been captured using other methods, such as quantitative methods or more structured questions.

Our dataset consists of 25 semi-structured interviews (Amis, 2005) conducted face-to-face in spring 2024 at three Finnish vocational schools operating across seven locations. One interview included a team of three, resulting in 27 informants in total. Additionally, the dataset includes transcribed observation notes. The interviews lasted just under 22 hours altogether, averaging slightly over 50 minutes each. One of the schools is a vocational special education institution.

The interviews are part of a project examining cybersecurity competences and risks in VET. Questions were tailored for three groups: IT and digital experts, school leadership, and academic administration. Topics included cybersecurity risks, organisational processes, training, and incident response practices. Data collection was agreed upon with each school in line with the restricting party's procedures. Participants were recruited through rector/vice-rector nominations, ensuring coverage of administrative, pedagogical, and technical staff. This purposive sampling aimed to capture a full range of perspectives on incident response. We specifically intended to include IT management, digital pedagogy, student services, teaching staff, and preferably a counsellor or nurse. The participants held various roles, such as teacher, special education teacher, digital tutor, study secretary, data protection officer, IT manager, director of digital services, systems designer, and counsellor. Despite formal agreements, informed consent was also obtained individually via email and at the start of each interview.

The interviews addressed topics related to incident response, particularly when participants were asked directly who they would report to if they noticed something suspicious, encountered a security breach, or if a computer or program failed to open upon arriving at work. Additionally, participants were asked how they would report such issues. IT management staff were asked more specific questions, such as how the process should work and what the threshold is for employees to report incidents. After the first few interviews, we began to also ask who employees would report to the incidents occurring outside office hours and how. This additional question was deemed necessary because an informant raised concerns about the effectiveness of their incident management processes outside regular office hours.

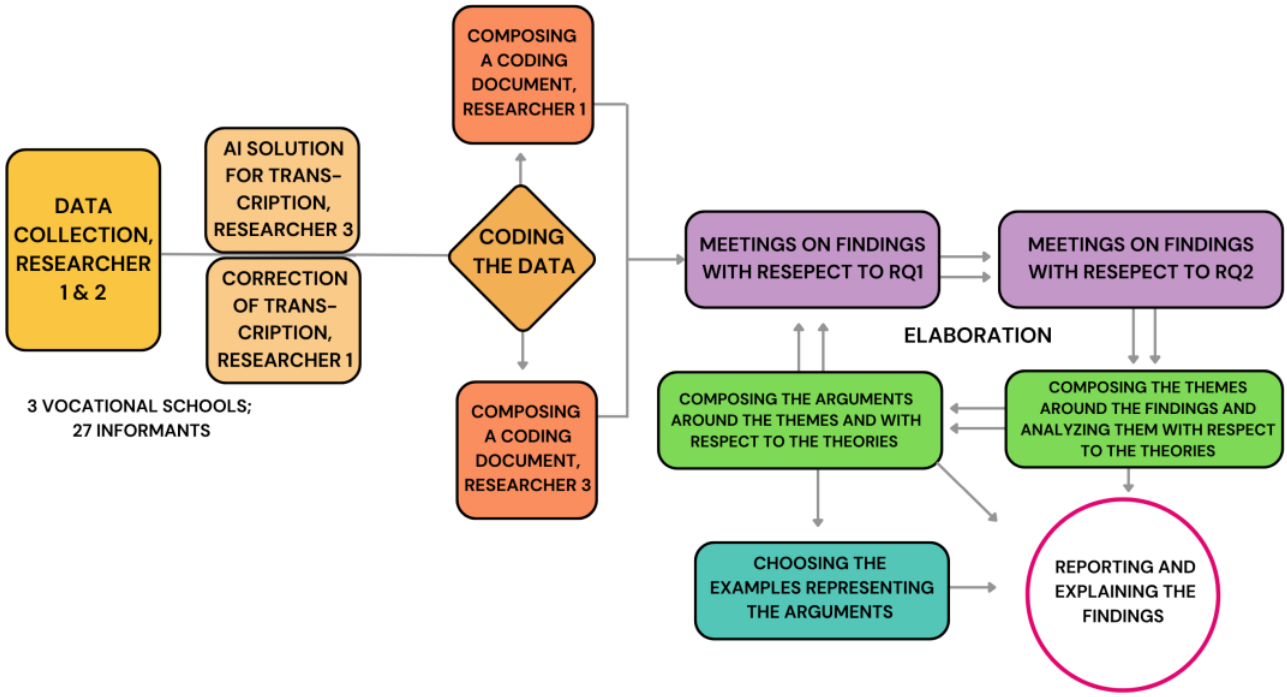
All interviews were conducted in Finnish with one or two researchers present. The data was anonymised at transcription stage. Technical auditing and IT infrastructure mapping are beyond the study's scope, so the data is based solely on staff accounts. Many informants had clearly prepared by reviewing their organisations' guidelines. The interviews were fully transcribed using Whisper's largest multilingual model (Radford *et al.*, 2023) and subsequently checked and edited by one of the authors. Regarding the data anonymisation, speech patterns were generalised to prevent identification of individuals or their institutions.

Analysis of the Data

The data was analysed thematically using an inductive approach (Braun and Clarke, 2006). The process began by systematically applying the research questions to the data and coding it comprehensively. Two researchers (one who took part in conducting the interviews and another who did not participate in them) independently extracted samples of different patterns into separate analysis documents. Thematic codes were developed iteratively. Coding was conducted with one research question at a time, with researchers meeting after each phase to discuss their findings. These discussions also explored the findings in relation to Ahmad *et al.*'s (2021) and Endsley's (1995) three states of knowledge in situation awareness as well as Vygotsky's (1978) ZPD. The phases of data collection and analysis are depicted in Figure 1.

During our analysis meetings, we assessed how the theoretical frameworks supported data interpretation. Vygotsky's (1978) ZPD emerged as essential for explaining observed practices. While we drew on Ahmad et al.'s (2021) and Endsley's (1995) three-level model of situation awareness, the distinction between perception and comprehension proved too subtle to apply consistently. Projection, however, was easier to recognise, typically emerging at IT and management levels where future-oriented decision-making was possible. Therefore, we used the model conceptually but did not classify findings strictly by its levels.

Figure 1. Phases of data collection and analysis in the study.



In line with qualitative research conventions, our analysis does not systematically report fractions or percentages. Unlike quantitative studies that rely on statistical power calculations, qualitative work emphasises depth of understanding, thematic patterns, context, and richness over numerical prevalence (Busetto *et al.*, 2020). Because the interviewees represented different roles within their institutions (teachers, administrative staff, IT personnel, and management), their perspectives reflect different points along the incident response process, including the various stages of escalation. For this reason, presenting percentages or fractions for each theme would not provide a meaningful picture and might even give a misleading impression of prevalence. Instead, the aim of the analysis is to generate a rich description of the incident response process as a whole and to show how it appears from the viewpoints of different actors across escalation levels.

Results

The informants (N = 27) provided valuable insights into how cybersecurity incidents are reported and managed within their organisations, particularly who they turn to for support when incidents are suspected. These points of contact were grouped into four thematic levels, forming an escalation path for incident response (RQ1). The first two result subsections examine this path: the first focuses on the school operations level and related IT support, while the second addresses digital management and escalation to external actors. These levels were derived from both informants' reports and IT staff descriptions of appropriate reporting channels. The third subsection explores the communication methods used for reporting incidents. The fourth applies Vygotsky's (1978) concept of ZPD to interpret how VET staff build situational awareness with or without peer support. This subsection also integrates Endsley's (1995) framework and Ahmad *et al.*'s (2021) model, linking the identified reporting levels, the development of situational awareness, and the role of collaborative learning in cybersecurity incident response.

Enhancing situation awareness and incident response through on-site support and customer interface of IT support and management

The teachers, study administrators, and student welfare representatives mostly identified the helpdesk or their own supervisor as the first point of contact. The digital management representatives also mentioned the helpdesk as the first contact point for all study-related staff. Therefore, the efficiency of the incident response process heavily depends on how well the helpdesk can receive and process information from the teachers, study administrators, and student welfare representatives. Information security officers were mentioned as contact points in five cases, and three teachers and one study administrator mentioned that they would contact a specific knowledgeable person or a member of the digital support team. One teacher mentioned contacting the service provider directly, although they later recognised that this might have been the wrong choice. One study administrator was unsure of who to contact, so they would walk to the staff room or generally contact someone from the safety organisation.

For some interviewees, it was very clear who they should inform, but for others, the processes were much more unclear, as the contexts and situations vary, as the following interview with a student affairs secretary illustrates:

> **R:** If something like an information or cybersecurity incident happened in your organisation or you would suspect something like that, what would you do? How would you handle it? What would happen?

I: I guess the first thing I'd do is call the help desk. Call them, or ... well usually call, especially if it's something urgent. It's quicker than email. Or maybe contact my immediate supervisor . . .

R: Okay, so if you noticed an information or cybersecurity issue, who all would you inform about it?

I: Probably everyone. Like, "Don't touch it, don't do anything—it's bad!" I don't know. At least the people nearby, for sure.

R: Well, let's go over a scenario. Say you notice a student's transcript of records has something completely wrong listed on it—like an approval, but it's not your signature or your co-worker's. What would you do?

I: We'd definitely contact the teacher and ask, "Why did you do this?" We'd fix it, for sure. I guess we're kind of sticklers like that. But sometimes you just have to; you can't, for example, evaluate things based on that. So yeah, we'd give guidance and instructions to make sure it's done properly in the future.

It was also noticeable that some processes were not considered concerning, even though they could technically be seen as phishing attempts. For example, when a student turns 18, they are officially responsible for themselves, and parents can no longer access their information or receive updates without the student's permission. However, some parents still try to obtain information about their child, for instance, by calling the student services office or asking teachers, even when the student has not approved information-sharing in the system. Despite this, we observed that such enquiries are usually not reported or even documented for monitoring purposes in the institutions. The informants did not consider these incidents to be serious because the motive behind the request is usually good in most cases. However, we consider this to be phishing, as it is an attempt to make an employee of the organisation disclose sensitive information about an adult to an entity that no longer has the right to access the information.

We also noticed that suspected incidents occurring outside office hours or outside IT support's operating hours tend to cause more challenges for the staff, as shown by an interview with a teacher:

R: Right, so if you noticed something suspicious in one of your systems, who would you contact or what would you do in that situation?

I: Well, I'd rely on the local IT-support guy.

R: What if it happened, say, last Thursday evening, just before the holidays? What would you do then?

I: Well, it kind of depends on what it was, but I guess I'd try to do something.

R: Let me give you a specific example. Let's say you noticed that your Excel file had somehow been emailed to the wrong address, outside the company. That would mean sensitive customer information had been leaked. What would you do in that case, on Thursday evening right before holidays?

I: Yeah, well, we do have the support portal on the intranet, but would it be fast enough (pauses to think)?

R: Let's assume, it wouldn't be fast enough.

I: Hmm (hesitates and then says uncertainly), I suppose I'd turn to my supervisor for support.

The support for creating situation awareness about potential incidents outside office hours was clearly weaker than during office hours or, more specifically, outside IT support operating hours. For example, IT support might only be available from 9 am to 3 pm, which does not even cover the institution's regular office hours. Overall, the data shows that while some processes are in place, they rely heavily on individual judgement, contextual interpretation, and the support available at the time.

Enhancing situation awareness in digital management and escalation to external entities

In VET institutions, managing cybersecurity incidents often involves engaging external entities to ensure effective responses. Staff members, including rectors, vice-rectors, and information security officers, highlighted several key escalation pathways. These include contacting a digital services manager, a data protection officer, or specialised external partners, such as the National Cyber Security Centre, cybersecurity companies, and insurance providers. Also, some respondents noted the importance of insurance-based services that enable rapid containment actions in collaboration with expert advisors during incidents.

Seeking external expertise also extends to collaborating with software service providers, educational networks of VET organisations, and professional working groups. For example, digital educators and IT specialists emphasised the value of accessing real-time updates and guidance from professional networks. Personal contacts and pre-prepared checklists were also mentioned as practical tools for navigating escalation processes. Many of these different measures were mentioned during the interviews, as shown by the following comments of an IT security specialist:

> We work with several IT service providers. For example, we purchase cybersecurity expert services from companies, using these as external resources to help secure our systems. Additionally, we have various insurance arrangements for these situations, ensuring that if an incident occurs, we can quickly initiate containment measures in collaboration with expert partners through our insurance providers. These are among the most significant supports from an operational perspective. Moreover, our IT specialists closely monitor updates and reports from cybersecurity centres and other sources. They have various channels that provide a steady flow of information about current developments in the cybersecurity landscape. Overall, I would say we have a strong network in place.

A noteworthy aspect of the data is that one organisation's head of cybersecurity highlighted the complex network of service provider agreements, where cybersecurity issues are either not clearly defined or missing altogether. Educational organisations currently have no centralised model, as contracts had been made over the years without a structured approach. However, he mentioned that they planned to review all agreements in the future. This finding was uncovered so late in our interviews that we did not have the opportunity to systematically ask the officials of other organisations about it. However,

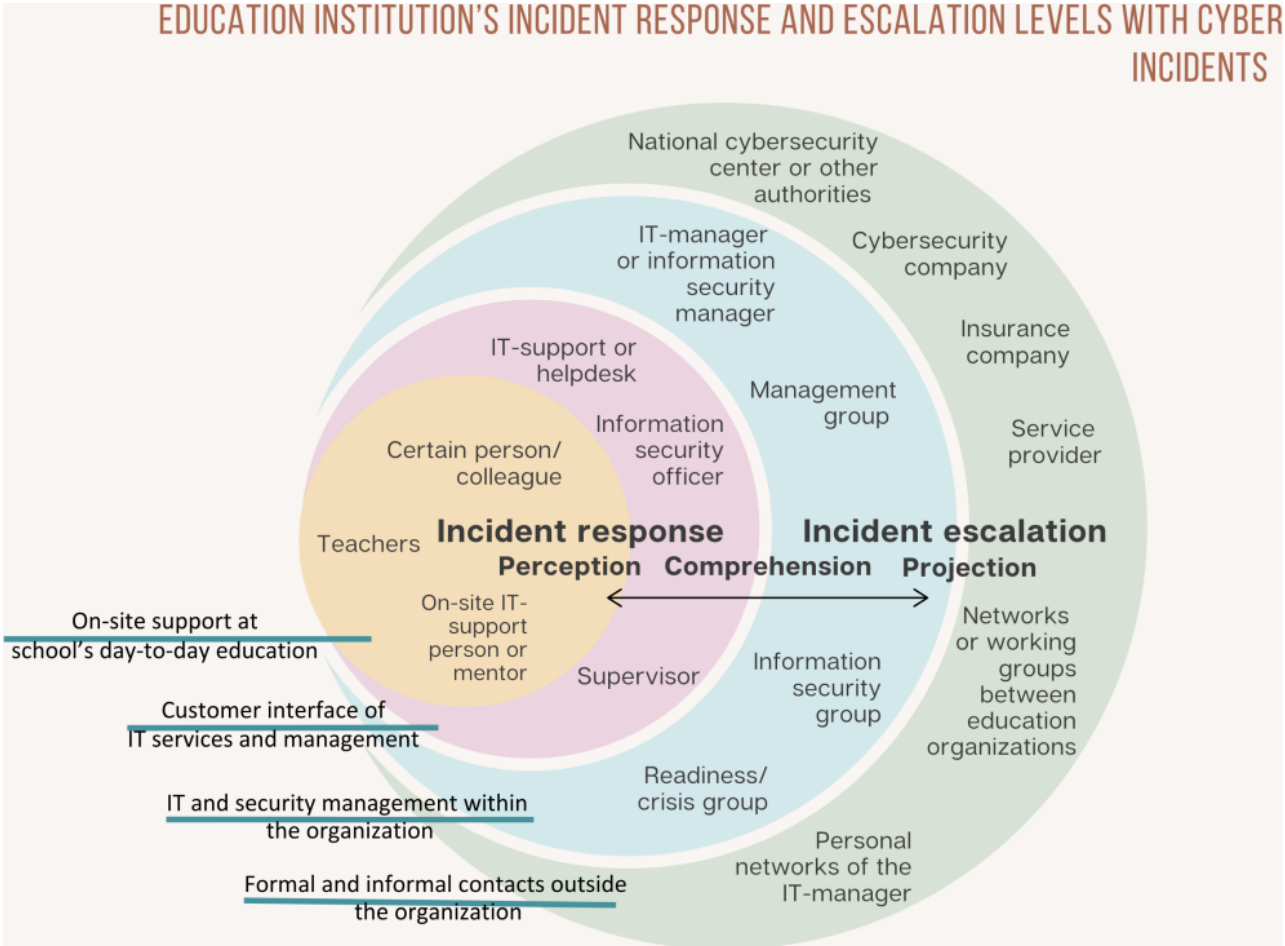
this finding suggests that similar shortcomings in contracts may be common in educational institutions.

Interpretation of incident response dynamics

The above findings relate to our first research question, which inquired about who the staff would consult when they suspect a cybersecurity incident and how these reporting practices unfold. The data indicates that real-world cybersecurity situations are rarely clear-cut. Instead, they often require situational analysis to determine whether an incident calls for action and who should be contacted in different cases. A reported event may turn out to be a one-off mistake, a misunderstanding of procedures, or something genuinely suspicious that requires escalation. For this reason, incident response cannot be reduced to a simple, linear process. It depends on reflection, interpretation, discussion, and the interplay between individual judgement and collaborative action. This reliance on judgement explains why staff sometimes turn to officially designated IT support, but at other times, they prefer to contact colleagues that are perceived as knowledgeable but whose roles do not formally include cybersecurity responsibilities. Although some procedures exist, they often depend heavily on individual interpretation and the support available at the moment.

The data further suggests that robust external networks and clearly defined escalation procedures are essential for effective incident response in VET institutions. Such networks

Figure 2. VET institution's incident response and escalation levels regarding cyber incidents.



support operational resilience by enabling timely intervention and access to specialised expertise when complex or high-risk incidents arise. Building projection capabilities through conversations with both internal and external experts allowed digital management to anticipate escalation outcomes. Examples of communication with experts include the use of insurance-based rapid response services and advice from national cybersecurity centres, both of which can help contain incidents and support effective recovery.

These dynamics are illustrated in Figure 2, which shows the layers or entities within VET organisations that provide and receive support at various levels of incident response and escalation.

In the central circle of the diagram, we illustrate the on-site support available for study-related working roles, which we consider as part of the school operations level. These include certain more experienced colleagues or teachers as well as on-site IT support staff available in various departments in some schools. The next circle represents the customer interface of IT services and management. This includes IT support or helpdesk services, the information security officer, and supervisors. The third level consists of IT and security management within the organisation, including various information and security management groups as well as the organisation's overall management groups. At the fourth level are external service providers for affected organisations or supervising and supporting organisations that handle incident or crisis management. This level also includes national authorities, law enforcement agencies, and insurance companies.

Ways of communication

Related to our second research question, the data showcased that vocational institute staff seemed to rely on both traditional and modern communication methods during cyber incidents. Phone call was one of the most commonly mentioned channels for reporting suspected cybersecurity incidents, appearing in thirteen cases. During one of the interviews, we asked a social work teacher to consider three possible ways to report a potential data or cybersecurity incident. The response is as follows: "Well, I'd call the IT support or send them a message, or, um, I can't think of a third option today, but maybe I'd then inform my supervisor that I've noticed something like this."

It is interesting that despite the rise of digital communication tools, staff seem to value phone calls for delivering urgent messages and enabling direct interaction during critical situations.

Email was another key communication tool, mentioned in nine cases. Real-time messaging tools, such as Teams and WhatsApp, were mentioned in eight cases. Service management systems, like IT support ticketing platforms, were also mentioned in nine cases. These systems allowed incidents to be logged, tracked, and resolved in a structured way while keeping a record of all actions for a later review. In addition, the institutes used specific emergency communication services and alarm systems for situations requiring rapid escalation or broad notifications. Alarm systems, in particular, provided automated alerts when immediate action was needed.

According to the data, there was considerable variation in the level of awareness of the informants regarding the VET institution's operational and communication practices. For some informants, it was clear that making a phone call or submitting a ticket would be the primary course of action. For others, such as the study secretary, whose comments are given below, the preferred communication channels were less clear:

> I can't really say, you know, we do have this institutional email. I can't say whether I'd have the authority to send something to everyone, at least not at the whole institutional level. Like, if it's something like, you know, don't open the program because it might leak all your information, personal data, well, maybe I could send it to the teachers in our field. And I could run to the teachers' staff lounge in our department, since they're the experts on this kind of thing. I mean, I know where their staff room is, so I'd probably just run there too.

In response to our second research question, we compiled Table 1 listing the various methods of reporting a suspected cyber incident mentioned in the data.

Table 1. Communication methods when reporting suspected cybersecurity incidents.

Communication method	Rationale for the method
Phone calls	For urgent messages and direct interaction during critical situations.
Email	Widely used for reporting and managing cybersecurity incidents.
Real-time messaging tools	Platforms like Teams and WhatsApp used for fast and informal communication.
Service management systems	Used for logging, tracking, and resolving incidents with structured workflows.
Emergency communication and alarm systems	For rapid escalation, broad notifications, and automated alerts to prompt immediate action.
Personal and direct face-to-face interaction with more capable colleague	Ensures clarity and immediate feedback.

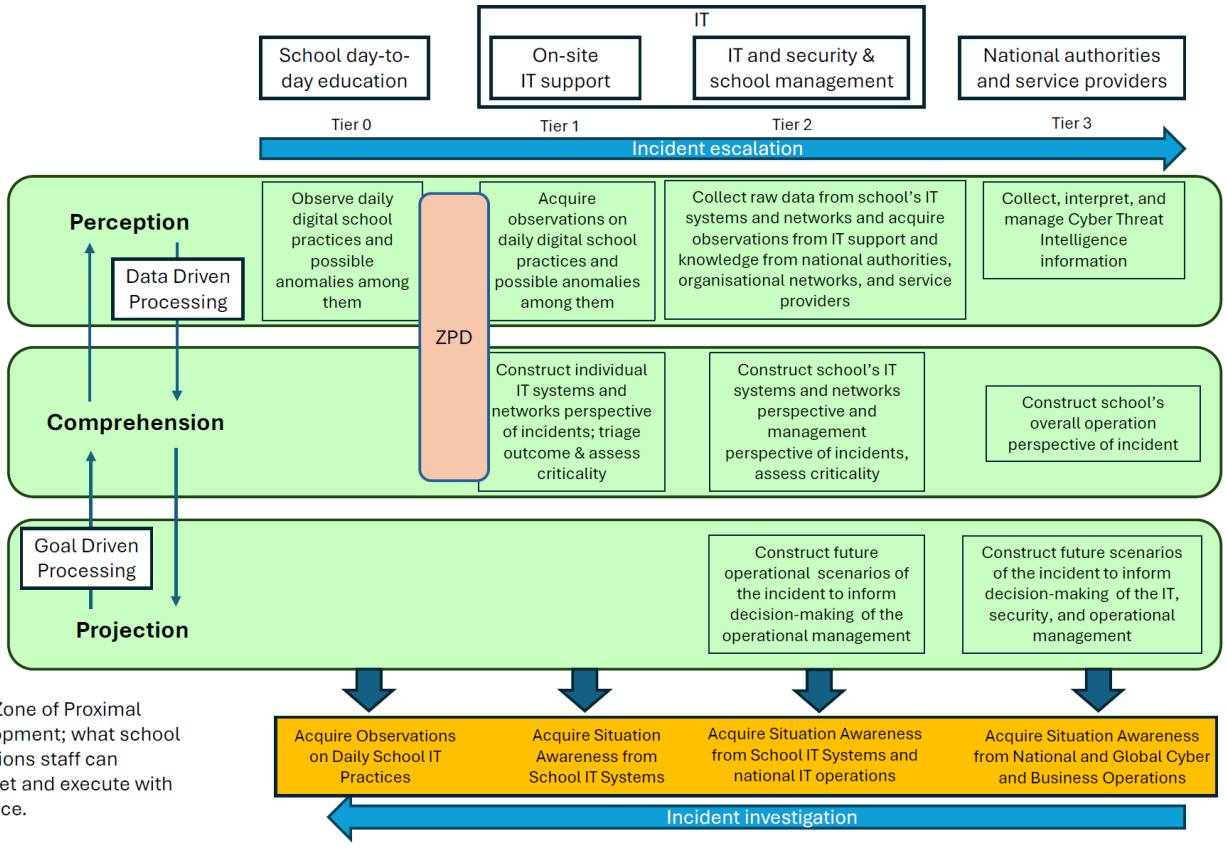
Zone of Proximal Development in incident response and situation awareness

According to our findings, Vygotsky's (1978) concept of ZPD offers a useful perspective for understanding how staff in VET institutions approach incident response and create situational awareness. The ZPD concept highlights the gap between what individuals can manage on their own and what they can achieve with guidance. This framework is particularly helpful in explaining how less confident or experienced staff handle cybersecurity incidents.

Some staff members confidently managed incidents and knew reporting protocols, while others hesitated and sought help from colleagues, supervisors, or IT support. This reliance shows how informal collaboration supports situational awareness, especially when procedures are unclear. Staff members unfamiliar with threats, like phishing, often gained knowledge and confidence through peer discussions, as experience and social learning filled gaps in formal preparedness. These interactions align with Vygotsky's view of learning as a social process. Within their ZPD, staff internalise new knowledge and skills by observing, imitating, and collaborating with more experienced peers. For example, a teacher who initially relies on IT support may, over time, develop a clearer understanding of appropriate steps. Through repeated experience and reflection, they gradually build confidence and independence in managing incidents.

Vygotsky's (1962, 1987) concept of tools and cultural artefacts is relevant to our findings, as IT systems and communication channels shape how staff respond to cybersecurity

Figure 3. Situation awareness in cybersecurity incident response in vocational education institutions (Adapted from Ahmad *et al.*, 2021).



ZPD= Zone of Proximal Development; what school operations staff can interpret and execute with guidance.

incidents. Many still prefer phone calls and messaging tools, such as Teams, as these provide immediate feedback and opportunities to confirm observations with more experienced colleagues. This interaction supports learning within the ZPD. In contrast, IT ticketing systems, while efficient for tracking and resolving issues, lack interpersonal engagement and do not foster the collaborative reflection that helps less experienced staff build situational awareness and confidence.

Figure 3 integrates Endsley's (1995) framework and Ahmad *et al.*'s (2021) model to provide a comprehensive view of incident response in VET institutions. It illustrates how the levels of incident response and the emergence of situational awareness are interconnected, framed within Vygotsky's ZPD to highlight the role of support in building institutional and individual capacity.

The figure adapts Ahmad *et al.*'s (2021) model, originally developed for finance, to VET institutions by integrating Endsley's (1995) perception–comprehension–projection framework. Vygotsky's ZPD is present in the communication between school operations and IT support, highlighting the role of guided learning. The model also incorporates tier 1–3 classification common in cybersecurity (cf. Husák and Čermák, 2022), with IT support handling basic tasks (tier 1), IT management conducting deeper analysis (tier 2), and external experts managing advanced cases (tier 3).

To address our second research question and the reviewer's suggestion, we mapped our findings against the phases of SA-CIR model (Ahmad *et al.*, 2021) and interpreted them through Vygotsky's (1978) ZPD. Table 2 summarises how observed practices align with both frameworks.

Table 2. Findings mapped to SA-CIR and ZPD.

Research findings	Element of SA-CIR	Perspective of ZPD
Non-technical staff are sometimes uncertain about what counts as an incident.	Perception: There is a challenge in recognising signals vs. noise.	Less experienced staff need support from colleagues to learn what qualifies as reportable.
Staff often use personal contacts before formal channels.	Perception or early comprehension: seeking sense-making input.	Peer guidance helps staff to develop awareness and interpret ambiguous situations.
Non-technical staff prefer phone calls to ticketing systems.	Late perception or comprehension: There is a need for immediate interaction to build shared understanding.	Phone conversations provide scaffolding: More knowledgeable colleagues guide decision-making.
There is uncertainty in incident handling outside office hours.	Gap in comprehension: There are gaps in procedures and escalation clarity	Lack of access to "more knowledgeable others" at certain times leaves staff without scaffolding.
There is notable reliance on external service providers, insurers, and Cybersecurity incident response teams.	Projection: Anticipation of outcomes, the involvement of specialised expertise, and the planning required for containment and recovery.	External actors function as "more knowledgeable others" for the technical staff which extend institutional capability.

The table shows that perception challenges in everyday incidents often triggered ZPD-style scaffolding from peers, while comprehension and projection phases were supported by formal IT staff and external experts. This mapping illustrates how SA-CIR processes are enacted in practice and how staff learning is embedded within them. Importantly, institutional learning occurs when staff observe and participate in structured escalation, turning individual experiences into shared organisational capability.

Conclusion and recommendations

This study examined incident response practices in VET institutions, focusing on who staff report to if they suspect a cybersecurity incident and the method used for reporting. Our findings show that while formal procedures exist, many staff members rely on informal networks, supervisors, and IT support to make sense of events and decide whether reporting is necessary. These personal contacts are especially important for building situational awareness at the perception level, in line with Endsley's (1995) model, and they help less experienced staff learn through collaboration, reflecting Vygotsky's (1978) concept of ZPD. However, the level of awareness for procedures varies, and outside-of-fice-hours incident handling often remains unclear. Similar concerns about the absence of clear frameworks or institution-wide practices have been noted in previous educational research (Sonhera *et al.*, 2021; Villegas-Ch *et al.*, 2021).

From an operational perspective, incident response in VET institutions should not be seen as an individual or purely technical activity but as a distributed capability involving staff, IT support, management, and external partners. This aligns with Ahmad *et al.*'s (2021) SA-CIR model, which emphasises the interplay between perception, comprehension, and projection in organisational incident-handling. Mixed reporting practices, such as combining helpdesk tickets with direct phone calls, not only reflect this interplay but they also reveal the tension between the human need for immediacy and the organisational need for systematic intelligence (cf. Schlette *et al.*, 2021).

Informal contacts and phone calls play an important role in everyday incident response, as they enable staff to seek guidance, reflect together, and gradually learn to judge whether a situation requires formal reporting. In this sense, such exchanges support the kind of collaborative learning and situational awareness-building described by Vygotsky's (1978) ZPD. At the same time, relying solely on these practices creates risks. Personal conversations do not necessarily leave incidents undocumented, but they can do so if there are no parallel processes ensuring that the information is captured. This may lead to incomplete records, uneven escalation, or missed opportunities to strengthen organisational learning. Current standards, such as ISO/IEC 27035-1:2023, NIST SP 800-61 Rev. 3, and the NIS2 directive, highlight the need for systematic documentation, consistent escalation, and traceable reporting. Therefore, while VET institutions should continue to support informal peer-to-peer exchanges as a way of developing staff competence, these must be integrated into formal reporting practices to ensure both resilience and compliance.

In light of these findings, we propose three priorities for practice. First, role-based instructions are essential: staff members without technical responsibilities, such as teachers and study secretaries, should not be expected to understand higher-tier escalation procedures but should have clear, simple guidance on who to contact, what to report, and when to escalate. This corresponds to defining responsibilities along escalation tiers without overburdening non-specialists (cf. Cichonski *et al.,* 2012; ISO/IEC 27035-1:2023). Second, institutions should connect informal support with formal systems. Phone calls and peer discussions are vital for learning within the ZPD, but these interactions need parallel mechanisms, such as logging a ticket afterwards, so that the obtained information contributes to organisational maturity, rather than remaining localised (Raković *et al.,* 2020; Schlette *et al.,* 2021). Third, preparedness must extend beyond office hours. Simple fallback procedures, including designated on-call contacts and service provider hotlines, are needed to ensure that incidents reported outside IT support's operating times do not vanish from the organisational radar (cf. Cichonski *et al.,* 2012). Scenario-based training, tailored to different roles, can further support staff in identifying their boundaries of responsibility and recognising when escalation is necessary.

In sum, strengthening incident response in VET institutions requires clear, role-based instructions, systematic documentation, and room for collaborative learning. When these elements are combined, everyday practices can be connected with the structured processes emphasised in current standards (ISO/IEC, 27035-1:2023; Nelson *et al.,* 2025) and with the principles outlined in the SA-CIR model (Ahmad *et al.,* 2021). In this way, institutions can bring together the human side of learning and the organisational need for consistency, moving towards a more resilient and reliable incident response.

Funding

The research was fully supported by the Finnish Work Environment Fund, under grant No. 230316.

Author Contributions

Conceptualization: A.O., T.S., and K.S.; methodology: A.O., T.S., and K.S.; validation: A.O.; formal analysis: A.O., T.S., and K.S.; investigation: A.O. and K.S.; writing—original draft preparation: A.O., T.S., and K.S.; visualization: A.O. and T.S.; and project administration: A.O. All authors read and agreed to the published version of the manuscript.

Data Availability Statement

The data is not publicly available due to confidentiality agreements with the participating educational institutions, which consented to take part in the study on the condition that the data would not be shared with third parties.

Disclosure Statement

No potential conflict of interest was reported by the authors.

References

Abrahams, T.O., Ewuga, S.K., Dawodu, S.O., Adegbite, A.O. and Hassan, A.O. (2024) 'A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection', *Computer Science & IT Research Journal*, 5(1), pp. 1–25. doi: 10.51594/csitrj.v5i1.699.

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T. and Baskerville, R.L. (2021) 'How can organizations develop situation awareness for incident response: A case study of management practice', *Computers & Security*, 101, pp. 102–122. doi: 10.1016/j.cose.2020.102122.

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A. and Janicke, H.A. (2020) 'A Holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom', *Applied Sciences*, 10(10), p. 3660. doi: 10.3390/app10103660.

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: Berg, pp. 104 –138.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology*, 3(2), pp. 77–101.

Busetto, L., Wick, W. and Gumbinger, C. (2020) 'How to use and assess qualitative research methods', *Neurological Research and Practice*, 2(14). doi: 10.1186/s42466-020-00059-z.

Cedefop (2025) *What is new in IVET? Key pointers from statistics.* European Centre for the Development of Vocational Training. Available at: https://www.cedefop.europa.eu/files/whatsnewinivet_2025.pdf (Accessed: 20 October 2025).

Celeny, D., Maréchal, L., Rousselot, E., Mermoud, A. and Humbert, M. (2024) *Prioritizing investments in cybersecurity: Empirical evidence from an event study on the determinants of cyberattack costs*. arXiv preprint. Available at: https://arxiv.org/abs/2402.04773 (Accessed: 10 April 2025).

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012) *Computer security incident handling guide (NIST special publication No. 800-61)*. Gaithersburg, MD: National Institute of Standards and Technology.

Clapper, T.C. (2015) 'Cooperative-based learning and the zone of proximal development', *Simulation & Gaming*, 46(2), pp. 148–158. doi: 10.1177/1046878115569044.

Endsley, M.R. (1995) 'Toward a theory of situation awareness in dynamic systems', *Human Factors*, 37(1), pp. 32–64. doi: 10.1518/001872095779049543.

European Union (EU) (2023) *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union* (NIS2 Directive). Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (Accessed: 20 December 2025).

Husák, M. and Čermák, M. (2022) 'SoK: Applications and challenges of using recommender systems in cybersecurity incident handling and response', in *Proceedings of the 17th international conference on availability, reliability and security (ARES'22)*. Association for Computing Machinery, New York NY, pp. 1–10. doi: 10.1145/3538969.3538981.

ISO/IEC 27035-1:2023, Information technology — Information security incident management — Part 1: Principles and process. International Organisation for Standardisation & International Electrotechnical Commission. Available at: https://www.iso.org/obp/ui/en/#iso:std:78973:en (Accessed: 20 December 2025).

Nelson, A., Rekhi, S., Souppaya, M. and Scarfone, K. (2025) *Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile* (NIST SP 800-61 Rev. 3). Gaithersburg, MD: National Institute of Standards and Technology, US Department of Commerce. doi: 10.6028/NIST.SP.800-61r3.

Ofte, H.J. and Katsikas, S. (2023) 'Understanding situation awareness in SOCs, a systematic literature review', *Computers & Security*, 126, p. 103069. doi: 10.1016/j.cose.2022.103069.

Organization for Economic Cooperation and Development (OECD) (2023) *Building future-ready vocational education and training systems*. OECD Reviews of Vocational Education and Training. Paris: OECD Publishing. doi: 10.1787/28551a79-en.

Radford, A., Kim, J. W., Xu, T., Brockman, G., McLeavey, C. and Sutskever, I. (2023) 'Robust speech recognition via large-scale weak supervision', in Krause, A., Brunskill, E., Cho, K., Engelhardt, B., Sabato, S. and Scarlett, J. (Eds.), *Proceedings of the 40th International Conference on Machine Learning*, Cambridge MA: JMLR, pp. 28492–28518.

Raković, L., Sakal, M., Matković, P. and Marić, M. (2020) 'Shadow IT – Systematic literature review', *Information Technology and Control*, 49(1), pp. 144–160. doi: 10.5755/j01.itc.49.1.23801.

Schlette, D., Caselli, M. and Pernul, G. (2021) 'A comparative study on cyber threat intelligence: The security incident response perspective', *IEEE Communications Surveys & Tutorials*, 23(4), pp. 2525–2556. doi: 10.1109/COMST.2021.3117338.

Sonhera, N. (2022) 'Cyber Incident Handling Framework for Schools in South Africa: Views of Experts', *Journal of Higher Education Theory & Practice*, 22(17), pp. 28–48. doi: 10.33423/jhetp.v22i17.5663.

Sonhera, N., Kritzinger, E. and Loock, M. (2021) 'Roles and responsibilities for school role players in addressing cyber incidents in South Africa', *Eurasian Journal of Social Sciences*, 9(3), pp. 123–137.

Viano, A. (2024) *Cyberattacks on higher ed rose dramatically last year, report shows*, *EdTech*, 12 June. Available at: https://edtechmagazine.com/higher/article/2024/03/cyberattacks-higher-ed-rose-dramatically-last-year-report-shows (Accessed: 10 April 2025).

Villegas-Ch, W., Ortiz-Garcés, I. and Sánchez-Viteri, S. (2021) 'Proposal for an implementation guide for a computer security incident response team on a university campus', *Computers*, 10(8), p. 102. doi: 10.3390/computers10080102.

Vygotsky, L.S. (1962) *Thought and language*. Cambridge, MA: MIT Press.

Vygotsky, L.S. (1978) *Mind in society: The development of higher psychological processes*. Cambridge, MA: Harvard University Press.

Vygotsky, L.S. (1987) 'Thinking and speech', in Rieber, R.W. and Carton, A.S. (Eds.) *The collected works of L.S. Vygotsky: Problems of general psychology*, vol. 1. New York, NY: Plenum, pp. 39–285.