Are We Ready for the Next Attack? Empirical Findings on Cybersecurity Awareness and Training

Sonja Spitzer
IFES Institutit für Empirische Sozialforschung*
sonja.spitzer@ifes.at

Stefan Schauer
Center for Digital Safety & Security
AIT Austrian Institute of Technology †
stefan.schauer@ait.ac.at

Stefan Rass
LIT Secure and Correct Systems Lab
Johannes Kepler University Linz ‡
stefan.rass@jku.at

Christine Schuster-Himmel
IFES Institutit für Empirische Sozialforschung*
christine.schuster-himmel@ifes.at

ABSTRACT

This paper examines how cybersecurity training and awareness building contribute to organizational preparedness against cyberattacks, particularly in organizations where cyber-physical and supply-chain interdependencies amplify cascading impacts. Building on the evolving threat landscape reported by ENISA and CrowdStrike and policy drivers such as the EU NIS2 Directive, we report findings from a representative empirical study of $n = 1014$ employees in Austrian companies. The results show that basic technical safeguards (e.g., antivirus, firewalls, access control) are widely implemented, while organizational preparedness remains uneven as emergency plans and clear incident procedures are often missing or unknown to staff. Cyber threat knowledge is largely limited to common terms (e.g., phishing), and awareness of supply-chain cybersecurity is particularly underdeveloped. Training is not systematic, since only about half participated in trainings over the last 12 months, and content retention declines sharply if it has been over one year since the training took place. We discuss implications for preparedness and recommend recurring, practical training cycles, including tabletop and simulation-based exercises that make incident response and supply-chain dependencies actionable for employees.

Keywords

cybersecurity, awareness, security training, preparedness, supply chain, employee security perception

INTRODUCTION

Across Europe and beyond, recent security studies and risk reports consistently point to an increased frequency and sophistication of cyberattacks, including advanced persistent threats (APTs) and hybrid threats. Critical infrastructures, especially in the energy sector, transport, healthcare, and public services, remain high-value targets (BBC News 2021; Bing and Kelly 2021), while supply-chain incidents have demonstrated how compromised or faulty update mechanisms can trigger cascading operational disruption and significant economic impact (Zetter 2020; Mugu et al. 2024; Amorim et al. 2025). These developments underline that cybersecurity is not a matter of purely technical protection and defense measures but cybersecurity awareness and the human factor plays a major role in making infrastructures more resilient against cyberattacks. Moreover, cybersecurity risk is no longer confined to isolated IT systems but emerges from tightly coupled cyber-physical and organizational interdependencies.

*www.ifes.at
†www.ait.ac.at
‡www.jku.at/lit-secure-and-correct-systems-lab/

As a consequence, recent initiatives, directives and laws in the EU but also in the USA and Asia address these issues. The NIS2 Directive (European Comission 2022) (which extends the former NIS directive (European Comission 2016)) puts a strong emphasis on achieving a high common level of cybersecurity across the European Union by increasing the protection of "essential entities" and "important entities" (as critical infrastructures are referenced therein, in general). In the NIS2 Directive, a core focus is put on an organization's supply network, i.e., its dependencies on suppliers and customers based on technical and organizational relations. Besides going into detail on the technical measures for protecting critical systems, the Directive emphasizes a process-oriented view together with the importance of awareness building and trainings for the employees. Similar directives and laws such as the American Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (CISA 2022), the Singaporean Cybersecurity Act (Singapore Statutes Online 2018), or the Security of Critical Infrastructure (SOCI) Act and the Critical Infrastructure Risk Management Program (CIRMP) (Department of Home Affairs 2023) in Australia explicitly reference recurring trainings and exercises as the main measure of building awareness among critical infrastructure employees.

Against this background, we initiated the project SOPHIE in 2022, funded by the Austrian Research Funding Agency (FFG) as part of the security research program KIRAS (Austrian Institute of Technology (AIT) 2023). Its main objective is to enhance the resilience of supply chains against cyber attacks with a strong focus on tailored training measures and simulation exercises to increase risk awareness and improve cybersecurity. Therefore, the project builds on business process and cascading effects analysis and develops models for simulating cyber incidents with the aim to integrate them into advanced training programs and table-top exercises for cybersecurity awareness. A core part of the project is a broad empirical study conducted among 1014 employees of companies across various infrastructure sectors in Austria. Therein, we asked about the importance of cybersecurity in their respective organizations and how cybersecurity processes are integrated into the overall business processes. This creates the backbone for the training and awareness building activities.

In this paper, we present the main results of this study and discuss the employees' general knowledge about cyberattacks and incidents as well as their impacts on the respective organizations in the past. Additionally, we put a strong focus on the frequency and contents of cybersecurity trainings as well as their influence on cyber awareness. In this context, we highlight the importance of constant and recurring training activities, emphasizing the strong connections between cybersecurity trainings, the improvement of awareness and the preparedness of organizations against cyberattacks. Building on the learning and implications of our study, we present impacts on preparedness and discuss several security measures and activities.

CYBERSECURITY INCIDENTS AND AWARENESS

Cyber Threat Landscape

Looking at recent studies and analyses towards the cybersecurity threat landscape in Europe but also globally, ENISA (ENISA 2025), CrowdStrike (Crowdstrike 2025), Fortinet (FortiGuard labs 2025) and Allianz (Allianz 2025) provided in-depth reports on recent incidents and the top threats. Over all four reports, social engineering and identity compromise take the top position, including phishing attacks, credential theft, stealing of information. ENISA reports that phishing is the dominant intrusion vector (60%) (ENISA 2025). Looking at the Fortinet report, it underlines this claim by characterizing an "industrialized" credential supply chain with over 100 billion records shared on underground forums in 2024 (+42% YoY) (FortiGuard labs 2025). Additinally, Fortinet further highlights a substantial increase in credential availability to data theft activity, observing a 500% increase in compromised logs and 1.7 billion stolen credential records shared (FortiGuard labs 2025). Taken together, these results indicate that identity compromise is sustained not only by phishing at scale but also by persistent credential recirculation in underground markets, increasing the likelihood that single-account compromise escalates into enterprise-wide intrusion.

The second top category is vulnerability exploitation, characterized by high volume and accelerating weaponization. ENISA identifies vulnerability exploitation as a cornerstone of initial access (21.3%) and emphasizes that campaigns may weaponize vulnerabilities within days of disclosure (ENISA 2025). Fortinet's telemetry reports 97+ billion exploitation attempts detected in 2024 (FortiGuard labs 2025). The combined evidence suggests that exposure management and patching are no longer best framed as periodic hygiene activities; rather, they must be treated as continuous, risk-based processes aligned with adversary automation and compressed exploitation timelines.

Ransomware and extortion remain core drivers of high-severity incidents and economic loss. CrowdStrike reports that Europe-based victims constitute 22% of entities named on extortion or leak sites, placing Europe as the second most targeted region after North America (Crowdstrike 2025). It further documents that 92% of Europe-based victims were named on ransomware-associated leak sites (Crowdstrike 2025). From an impact standpoint, Allianz

provides evidence for that based on their claims, which attributes 60% of the value of large cyber claims (>€1m) in first half of 2025 to ransomware (Allianz 2025). Allianz also highlights a growing coupling of extortion with exfiltration, reporting that 40% of the value of these claims included data theft, a significant increase from 25% in 2024 (Allianz 2025). This is a strong indication that modern ransomware needs to be understood as a combination of service disruption, data breach and coercion problem rather than an type of incidents solely affecting availability.

The reports also converge on cloud and IoT exposure as structural amplifiers of the core threat categories above. Fortinet reports several operational indicators, e.g., 70% of cases involved new logins from unexpected geographies, and 20% showed new API activity for existing users (FortiGuard labs 2025). With regards to edge and IoT technology, Fortinet reports > 20% of exploitation attempts targeted at IoT devices, suggesting that routers, cameras, and perimeter devices remain high-value targets for automated scanning and botnet activity (FortiGuard labs 2025). ENISA's EU sector distribution highlights that public administration (38.2%) and other essential sectors are prominent targets, since these sectors frequently operate complex hybrid infrastructures and provide high-visibility services that are attractive for disruption and extortion and have a high exposure for cloud and edge technologies.

Top Security Measures

Taking these four reports on the cyber threat landscape into account yields five prominent security measures that repeatedly emerge as high-leverage controls from all of those reports. These recommendations strongly align with the reports' dominant threat categories described in the previous section, i.e., intrusion attacks based on phishing or credential theft, rapid exploitation of vulnerabilities, ransomware and extortion often coupled with data theft, disruptive campaigns aiming at organizations' availability, and cloud exposure.

Considering identity compromise as a primary entry point, strong authentication and privilege governance becomes a foundational aspect to improve organizations' cyber security. ENISA reports phishing as the dominant intrusion vector (60%) (ENISA 2025) and lists identity management including the implementation of multi-factor authentication (MFA) as a critical mitigation strategy towards ransomware attacks (ENISA 2025). The CrowdStrike report similarly emphasizes securing the entire identity ecosystem and recommends phishing-resistant MFA, e.g., by using hardware keys, as a central control (Crowdstrike 2025). Also the Allianz report reinforces identity-centric hygiene by highlighting MFA as a basic preventive measure (Allianz 2025). Operationally, this measure implies the implementation of phishing-resistant MFA for privileged and remote access as well as Privileged Access Management including least privilege, separate admin accounts or just-in-time elevation as well as continuous monitoring for anomalous authentication and privilege escalation.

Given compressed time-to-exploit and pervasive scanning, the reports support shifting from periodic patch cycles to continuous exposure management. For example, ENISA notes vulnerability exploitation as a cornerstone of initial access (21.3%) and highlights that vulnerabilities may be weaponized within days of disclosure (ENISA 2025). As a mitigation strategy, Continuous Threat Exposure Management (CTEM) can support operators to counter such attacker asymmetry (FortiGuard labs 2025) and operationalizes this via a "CISO playbook" including adversary emulation and risk-driven remediation (FortiGuard labs 2025). In practice, this measure builds upon complete asset discovery including services open to the Internet, risk-based prioritization based on exposed systems, exploitability, and business criticality, together with validation through continuous security testing.

To contain intrusions before they become entrance for ransomware or extortion events, segmentation and hardening recur as essential controls. For example, network segmentation is a critical mitigation strategy when it comes to ransomware attacks and frames baseline cyber hygiene as including network and endpoint controls (ENISA 2025). Fortinet's report underscores the scale and breadth of exploitation pressure with 97+ billion exploitation attempts being recorded in 2025 (FortiGuard labs 2025), and further notes that > 20% of exploitation attempts targeted IoT devices (FortiGuard labs 2025), indicating the importance of IoT inventory together with patching and firmware management, and isolation. This measure therefore includes the segmentation of critical systems and identity infrastructure, the hardening of configurations, especially for perimeter and remote access, and the explicit governance for IoT assets, combining inventory, isolation, credential hygiene, and update discipline.

In addition, the reports consistently imply that detection speed and response maturity substantially reduce impact, especially for extortion-driven incidents. Here, baseline cyber hygiene explicitly includes endpoint behavior monitoring, auditing, and related controls (ENISA 2025) whereas other strategies include scaling security operations through agentic AI and integrated detection and response capabilities (Crowdstrike 2025). Accordingly, effective cyber hygiene, early detection, and incident response capabilities can be seen as key levers for reducing losses from cyberattacks (Allianz 2025). Implementations typically include Endpoint Detection Response (EDR) and Extended Detection Response (XDR) coverage, centralized log management across identity, endpoint, network and cloud control planes as well as open-source intelligence (OSINT) investigation workflows.

Finally, resilience planning is treated as core aspect, overall, since modern attacks routinely aim for operational disruption. Accordingly, resilience and business continuity management processes, more specifically backup, remote storage, data loss prevention, and network segmentation, are critical mitigation strategies (ENISA 2025). As ransomware is a major contributor to the value of large claims (Allianz 2025), this strengthens the case for robust recovery capability. Preparedness is repeatedly linked to exercising, with routine tabletop exercises and red/blue teaming being highly recommended (Crowdstrike 2025). Particularly when it comes to readiness against DDoS attacks, which are considered to be the most prevalent threat across sectors in the EU (ENISA 2025), it is important to include runbooks, upstream mitigation and communication as core aspects within continuity planning. More precisely, this measure requires immutable offline backups with proven restore capabilities, Data loss prevention (DLP) and encryption mechanisms to reduce exfiltration leverage together with Incident Response (IR) and Business Continuity Management (BCM) processes covering ransomware, leak-site extortion and service disruption.

Cybersecurity Awareness

The general aspect of cybersecurity awareness has been investigated in different studies and under various aspects in the past. With regards to small and medium enterprises (SMEs), which are also a core focus of the study we present here, the work of (Fertig and Schütz 2020) provides a systematic and in-depth review on how information security awareness (ISA) is measured in the literature. Therein, the authors highlight that questionnaire-based methods and transparent review practices (e.g., expert recruitment, search documentation) are the main choice of evaluating ISA; however, they argue for a more behavioral-based testing, which the design of our study accounts for as we aim for a participatory education for security (more details given in the next section). In a similar way, Ponsard et al. discuss practical instruments for cybersecurity awareness, e.g., quizzes covering attitudes, behavior or knowledge, self-assessment questionnaires, etc., to engage time-constrained stakeholders (Ponsard et al. 2019). Additionally, (Bada and Nurse 2019) proposes a core program for cybersecurity awareness that builds trust through in-person engagement, maintains lists of third-party providers that undergo credibility checks, and emphasizes a sustained communication strategy. The authors also report that concepts like marketplaces where solutions can be discussed and exchanged are not utilized as much as they could be. The setup of our study is very much aligned with both works, as we are aiming for a employee-centric design and focus on accessible materials, clear positioning, and actionable advice for non-specialists (more details given in the next section). A more recent study (Tetteh 2024) is also closely related, as it identifies issues and challenges of SMEs in cybersecurity posture and identifies technical as well as organizationsl measures, which very much relates to our study described here with the exception that we also have a distinct focus on supply chain security.

Another systematic review on cybersecurity awareness in SMEs (Junior et al. 2025) highlights the limited progress in cybersecurity studies for SME as well as major gaps between current standards and their practical implementation in SMEs. Further, it underlines the importance of the human factor as a common threat vector. Complementing this, (Erdogan et al. 2023) describes a survey-based analysis underscoring SMEs' difficulties in sustaining balanced cybersecurity practices and the need to strengthen awareness. These are concerns that the employee-centric orientation of our study also underlines and reinforces our focus on clearer methods and reproducibility. Likewise, (Benjamin et al. 2024) provides a curated overview of recent SME cybersecurity frameworks and assessment approaches, offering contextual grounding for situating our study within the broader solution landscape, including artificial intelligence. The work of (Kereopa-Yorke 2023) complements this by discussing AI/LLM-enabled support for SMEs and proposes a tailored, implementation-oriented LLM approach, aligning with our emphasis on practical, employee-facing guidance and evaluative rigor.

METHODOLOGY AND SURVEY SETUP

The data reported in this paper are based on the quantitative survey carried out as part of the SOPHIE project. The main objective of the survey was to gain insight into the security culture and awareness practiced in companies through the statements of employees. For this reason, it is noted at the outset that this perspective cannot be interpreted as representing the company's viewpoint. Including the employee perspective is important because the human factor is central, particularly in the field of cybersecurity, and research into lived security culture should logically begin with the employees themselves. In this way, it is possible to examine which strategies, measures, and guidelines actually resonate with employees.

Data Collection and Sampling

Data collection was conducted via an online panel. The individuals contacted received an online link to the survey, which they could complete themselves. Sampling was quota-controlled to ensure a representative sample of the

GENDER	%
Men	53
Women	47

AGE OF EMPLOYEE	%
up to 29 years old	21
30–39 years old	24
40–49 years old	23
50 years old or older	32

EDUCATION	%
without a high school diploma	55
with a high school diploma	45

FUNCTION	%
Division/Department Heads, Executive Management	13
Other Senior Staff	14
Employees in IT, Operations, Data Protection, Supply Chain	14
Other Employees	59

LENGTH OF EMPLOYMENT	%
up to 2 years	17
2 to 5 years	21
5 to 10 years	22
10 to 20 years	20
more than 20 years	19

COMPANY SIZE	%
10 to 19 employees	13
20 to 49 employees	15
50 to 249 employees	23
250 or more employees	48

INDUSTRY	%
Energy, Water Supply, Waste Management, Transportation, Communications Technology, Financial Services	33
Manufacturing and Production	21
Construction	8
Retail	13
Food Service, Arts, and Culture	5
Education and Teaching	8
Other	11

LOCATION STRUCTURE	%
one	26
additional locations within Austria	56
additional locations in other EU countries	32
additional locations in non-EU countries	19

Figure 1. Overview on the sample composition for the survey

target group. Quota characteristics included federal state, age × gender and company size. The population or target group is defined as employees in companies with more than 10 employees in Austria. Additionally, the collected data was weighted by company size, federal state of employment, age × gender and industry. These quotas and weightings are based on official employment data in Austria; to provide a relation: overall, there are 4,483,009 people in employment, of whom 3,941,170 are employees and of whom 3,244,707 employees in companies with more than 10 employees (Statistik Austria 2024). More details on the sample composition are given in Figure 1.

The survey took place from late April to early June 2025. The median response duration was 14 minutes; responses lasting less than 4 minutes, as well as cases with other anomalies, particularly those with high rates of non-response or straightlining (selecting the same answer option for multiple survey-items), were excluded from the analysis. A screenout or automatic termination of the survey occurred for individuals who did not belong to the target group. Excluded were freelancers, self-employed individuals, those in marginal employment, homemakers, retirees, schoolchildren or students, apprentices, individuals on parental leave, and the unemployed. The sample was designed to include only individuals who are in an employment relationship and work in companies with 10 or more employees in Austria.

A total of 1039 responses for the survey were fully completed, of which 74 were excluded due to quality issues. In some cases, these quality issues were flagged during the data collection phase, allowing additional responses to be conducted during the fieldwork period. Ultimately, 1014 responses were included in the analysis. As a thank you for their time, respondents were credited with €1.50 for completing the survey. Due to the control quotas used in the survey and the subsequent weighting of the data, the sample can be considered representative of employees in companies with more than 10 employees in Austria. Survey results from samples are always subject to random variation. The range (maximum margin of error) for 1000 responses is 3.1 percent. The results should therefore be interpreted as plus or minus 3.1 percent.

Questionnaire

The questionnaire consisted of 67 questions. It covered three main areas: first, demographic questions about the respondents; second, demographic questions about the employer or the company where the respondent works; and third, content-related questions tailored to the KIRAS project. About one-third of the questionnaire consisted of questions on sociodemographic and company-specific statistics. The content-related questions were almost all closed, mostly Likert scales, but also included single-choice and multiple-choice questions. Ten hybrid (half-open) and two open questions were also included. The survey was estimated to take 20–25 minutes in advance, this was communicated to the respondents on the introductory screen. In addition, the questionnaire included attitude measures from a Security Awareness Index, which were adapted from the work of Zerr (Zerr 2007) and Zerr and Benner (Zerr and Benner 2017). These item batteries were included in our survey because they address topics such as employee personal responsibility, corporate philosophy, management attention, and influence on task completion, which, according to their study, are essential characteristics for measuring awareness among employees.

Analysis Methodology and Interpretation of Data

The data were analyzed exclusively using descriptive methods. The results include individual statements from the employees' perspective; that is, statements made by respondents about their own companies. As explained earlier, the individual perspective is highly relevant in the field of cybersecurity because the human factor and individual experiences are of central importance, particularly when examining the security culture in practice.

SURVEY RESULTS

IT Security within Companies

As first indication from the results of our survey, we saw that technical security measures are well established in most companies. Roughly eight out of ten employees reports that their organization use antivirus software (81%), access control restrictions (80%) and firewalls (80%). Approximately three quarters indicate that password management policies (77%) and backup strategies (75%) are set up and documented in these organizations. About two thirds of the respondents (64%) report that they have implemented data encryption. Other technical measures like network monitoring (52%), two-factor authentication (54%), and penetration testing (22%) are mentioned less frequently, with more than one quarter of respondents unable to provide any information on these topics.

In contrast, the implementation of organizational measures and formal regulations is less advanced in the organizations covered in the survey. Only 42% of the respondents report that their organizations have an emergency plan covering the case of a cyberattack. Overall, 57% of the respondents confirm that there are security guidelines for IT systems in their respective organizations, while 17% say that there are none and 25% are unable to provide any information. Although two thirds of respondents report adhering to security policies (68%), only one third are aware of a defined procedure for dealing cyber incidents (34%), while more than half (52%) have never heard of such procedures. Furthermore, while a large majority (83%) report an open culture regarding IT-related problems in their organizations, only slightly more than half (56%) know whom to contact in the event of a security incident.

Knowledge of Cyber Threats

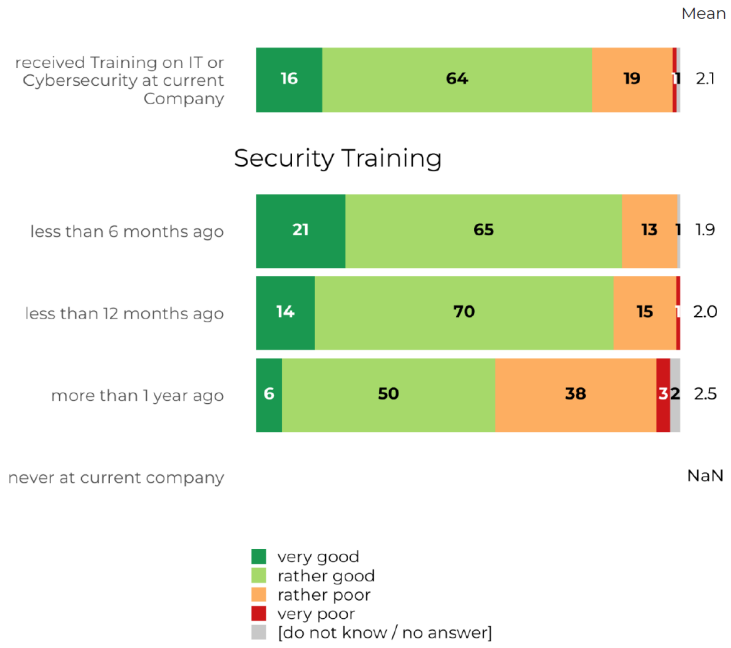
When it comes to the overall threat landscape, knowledge of specific types of cyberattacks is rather high-level among the participants of our survey and corresponds to the content covered in training courses already completed. In particular, 68% of the respondents are familiar with phishing and know the general principles behind that attack strategy and 64% know about malware being sent as email attachments. However, the knowledge about other attack vectors is considerably lower, i.e., for ransomware (29%), social engineering (22%), DDoS attacks (22%), man-in-the-middle attacks (15%), or zero-day attacks (13%).

With regards to real attacks, respondents generally consider the risk of a cyberattack on their own company in the next 12 months to be low. In detail, the average response is 4.4 on an 11-point scale (ranging from 0 = very low to 10 = very high), which is below the midpoint on the scale (5). However, the perceived probability of an attack increases with the size of the company and the number of national and even more with international locations. The average score for perceived probability of an attack is 3.4 among employees at companies with 10–19 employees, 3.7 among employees at companies with 20–49 employees, 4.3 among employees at companies with 50–249 employees, and 4.9 among employees at companies with more than 250 employees. The same applies to the number of locations. The average score is 3.7 for employees at a single location, 4.5 for employees at additional locations within the country, 5.0 for employees at companies with multiple locations within the EU, and 5.5 for employees at companies with multiple locations outside the EU.

For comparison, a quarter of respondents (27%) reported that their company had been affected by a cyber incident in the past year, including 4 percent that indicate "negative consequences" such as data loss, business interruption, or damage to reputation. However, almost half of the employees participating in the survey were unable to provide more detailed information.

Awareness and Security Training

The survey clearly shows that cybersecurity awareness and training measures are established and implemented in many of the companies covered. Overall, only 47% of respondents participated in IT or cybersecurity trainings within the past twelve months, while 31% report never having received training in their current organization; another 9% are unable to provide any information on this (see Figure 3). For those who have participated in trainings, the content predominantly focuses on classical IT security topics such as data protection (90%), password management (83%) and malware (83%). Current attack scenarios such as social engineering (46%), ransomware (43%), and supply chain attacks (35%) are addressed less frequently.



Question 39: How well do you remember the content of your last training or awareness-raising session?
Basis: Received training on IT or cybersecurity at your current company [n=608]

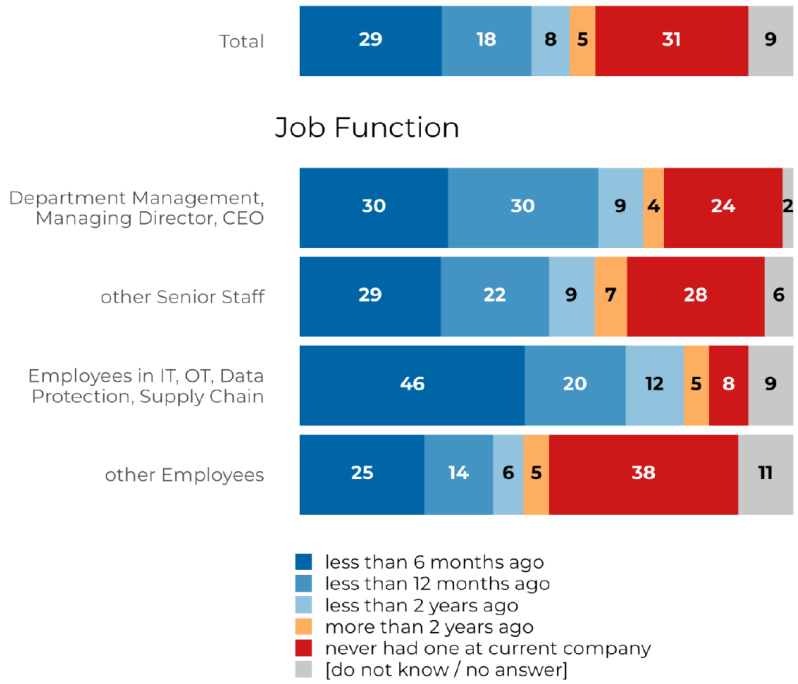
Figure 2. Overview on how well respondents remember the content of their last training session (based on 608 people that have participated in trainings in the past 12 months).

Besides the existence of trainings and awareness measures, the survey indicates that their regularity and repetition are also a crucial factors. Only a minority of employees report that there are quarterly or semi-annual classroom trainings (16%), online trainings (25%), awareness campaigns (29%), simulated attacks (20%), or information on current threats (33%) happening in their respective organizations. As shown in Figure 2, if the frequency of trainings is low and the last training took place more than a year ago, it has a significant impact on the people's ability to remember the contents. If the respondents had security training in the last year, the vast majority (84%) can remember the content well (according to their individual perception); if the training happened more than a year ago, only a slightly more than half of the participants (56%) can remember the content well. Additionally, the survey also indicates that many companies are lacking mandatory training cycles or continuous measures. If respondents have not yet participated in any training, it is due to the availability of such opportunities: almost three-quarters (73%) of those who have never received training at their current company also report that this is simply because no such programs were offered.

Furthermore, the survey also indicates that employees who do not hold primary security, IT, OT, or management roles (i.e., the role is "general" or "other") are a decisive factor in the context of cybersecurity. A closer look at the data (see Figure 3) reveals that more than one-third (38%) of these "other" employees have never received training or awareness-raising measures at their current company. A similar percentage (39%) of "other" employees received such training or measures at least once in the last year. Although they are not directly involved in security-related activities or processes, these individuals still make security-related decisions in their day-to-day work; without having some general security knowledge or awareness of security threats, they can become a major attack vector for the organization.

Cybersecurity Perception

Understanding employees' perception of cybersecurity is crucial because their attitude and viewpoint significantly influence how security guidelines are understood, accepted, and actually implemented in everyday work. As already mentioned in Section "*Methodology and Survey Setup*" above, the studies by (Zerr 2007; Zerr and Benner 2017) show that these factors also shape how risks are perceived, responsibilities are assigned, as well as actions and priorities are set in everyday work. When comparing the security and risk perceptions of the respondents in our study, clear differences emerge, pointing to discrepancies: on the one hand, the answers regarding security and risk perception can vary for one individual respondent, and on the other hand, the answers can vary between the individual and organizational perspectives.



Question 35: When did your last IT- or Cybersecurity training or awareness-raising measure take place at your current company? Basis: Total [n=1.014]

Figure 3. Overview on the timing of the last training activity in the respective organization. Besides the total number, also the numbers per staff category are listed.

Organizational Framework for IT and Cybersecurity Aspects

While 62% of the respondents agree that IT security problems are taken very seriously within their respective company, but only just under half of them (47%) perceive that their direct supervisor places strong emphasis on information and data security. At the same time, the data on restrictions and usability indicates that almost a quarter (23%) of the respondents perceive security measures as restrictive, burdensome or difficult to implement, saying that rigid IT security policies make their own work more difficult.

Implementation of IT and Cybersecurity Aspects by Employees

With regards to the implementation of cybersecurity measures, our survey draws a rather ambivalent picture, in which cybersecurity is widely recognized as important and compliance with regulations is highly valued by employees, whereas actual responsibility is delegated to IT and one's own contribution is perceived as limited. In detail, roughly two-thirds of respondents (68%) consider cybersecurity measures to be important for the future of the company, and just as many say they comply with all guidelines themselves. At the same time, there is a clear discrepancy between the attribution of responsibility and perceived personal effectiveness, i.e., almost half of the respondents (46%) understand the responsibility for cybersecurity topics primarily within the IT department, and just under a third (30%) consider themselves to be able to contribute only little to the security of the company. This points to a gap between formal agreement, compliance and a subjectively anchored assumption of responsibility and underlines that this difference between formal compliance and an employee's own sense of responsibility should be specifically addressed in training courses.

Security and Stability along the Supply Chain

The outcomes of our survey further indicate that cybersecurity along the supply chain is not yet a priority for many employees, and that the associated requirements are only beginning to be incorporated into everyday work. Although 60% of respondents say that cyberattacks threaten the stability of supply chains and are therefore seen as a significant risk (see Figure 4), only 18% report that their company has already addressed cybersecurity along the supply chain. On the contrary, 41% are unable to answer this question, which indicates a limited transparency or a lack of visibility regarding relevant activities. In addition, 20% of respondents say that there is a lack of awareness of the risks posed by cyberattacks within the supply chain in their own company. This picture is in line with the fact

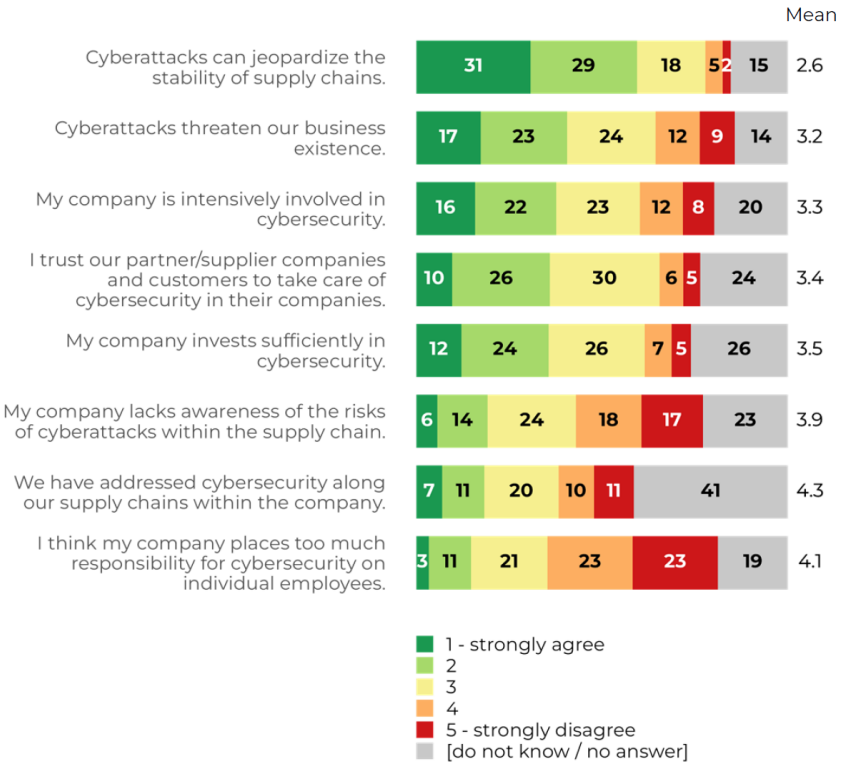


Figure 4. Overview on the respondents' perception on security and stability in the supply chain of their respective organizations.

that a little over one-third (36%) trust that partner or supplier companies and customers take care of cybersecurity in their own companies.

Besides the awareness of existing cybersecurity measures, we also focused on current regulation related to supply chains, in particular, the NIS2 Directive, which has a strong focus on improving cybersecurity along the supply chain (European Comission 2022). In this context. three-quarters of respondents (75%) are unable to answer the question of whether their own company will be affected by the NIS2 Directive in the future, with 10% answering "yes", and 15% answering "no". Broken down by job function, the results highlight that "other" employees have the highest percentage of being unable to answer (82%), which could be explained by the NIS2 Directive being a rather new regulation that is not very knowledgeable by employees not related to IT topics. However, even at management level, there is a lack of knowledge about the NIS2 with two-thirds (66%) of (deputy) department heads or executives and almost three-quarters (73%) of other senior employees cannot answer this question. Additionally, among employees working in IT, OT, data protection, and supply chain context, more than half of the respondents (54%) also were unable to answer this question, indicating that they are not aware of the NIS2 Directive.

In summary, our survey indicates a clear discrepancy between the majority recognizing the risk of cyberattacks to the supply chain and the rather small perception of a need for internal measures. From the participants' answers, there is little evidence of systematic engagement with the general topic of cybersecurity in the supply chain. The comparatively high level of trust in external partners also indicates a potential shift of responsibility to external parties.

INTERPRETATIONS AND RECOMMENDATIONS

Technical and Organizational Aspects

A first major finding from our survey is that many companies have established basic technical safeguards such as antivirus software or firewalls, with an additional focus on strengthening identity management (e.g., using multi-factor authentication) or network monitoring. In that way, they are following the major recommendations from ENISA (ENISA 2025), CrowdStrike (Crowdstrike 2025) or FortiNet (FortiGuard labs 2025) as described in the first section. However, the survey indicates that clear responsibilities, continuous monitoring, and strategic

IT security frameworks are often lacking, particularly in small and medium-sized enterprises. In this way, our results are aligned with the outcomes presented in (Erdogan et al. 2023) and (Junior et al. 2025). Larger and more internationally operating companies are more likely to have formalized processes, clearly defined procedures and designated responsibilities.

For example, only 34% of the employees reported that there are guidelines in their respective organizations on how to respond or act in case of a cyber incident; 45% of respondents reported that they are unaware that such a guideline exists and 14% are convinced that such guidelines do not exist in their organizations. For small enterprises (10-19 employees), these numbers drop to 11% (guidelines exists), 29% (guidelines do not exist) and 58% (not aware of guidelines), respectively. For large enterprises (above 250 employees), 42% of respondents indicated that such guidelines are implemented and only 8% say that it does not exists (with 42% not being aware of any guideline).

A reason for that could be the lack of resources - particularly budget - for cybersecurity activities within small enterprises. This is based on an interesting result from the survey which states that small enterprises (10 to 19 employees) often lack the funding to dedicate extra budget to cybersecurity, as, for example, already indicated in (Tetteh 2024)). In this context, 5% of respondents stated that they have a dedicated budget for cybersecurity, 59% stated that they have no financial resources for it, and 36% were unable to answer this question. Here, it is important to note that many of the employees surveyed likely do not have sufficient knowledge about the existing cybersecurity budget in their company (see Section "*Limitations and Open Points*"). This is particularly noticeable in the high number of "don't know/no answer" responses. Nevertheless, it appears that as company size increases, so does concrete knowledge of such a budget. For example, 12% of respondents working in companies with 20 to 49 employees state that they have a budget; among respondents in companies with 50–249 employees, the figure is 20%; and in large companies with 250 or more employees, 31% are aware of a budget for cybersecurity.

Cybersecurity Awareness and Perception

With regards to the employees' knowledge on cyber threats, the results from our survey strongly indicate that only a few basic terms and concepts (i.e., phishing, malware/ransomware, etc.) are known to the general workforce in the organizations covered in our survey and that more specific forms of attacks are largely unknown. Additionally, the respondents showed a rather low estimation of the risk of a cyber attack on their respective organization. The participants were asked to provide an estimation about the risk that their company might become target of a cyber-incident, using a scale from 0 (very unlikely) to 10 (very likely). The average assessment was 4.4, which is slightly less than half of the scale, indicating that the risk appears under-rated compared to real-life events. Moreover, there is indication for a correlation with the size of the company (bigger companies are rated with higher risks of a cyber-attack) and the time since the last security training (the longer ago, the lower is the risk rating, with least ratings is a cyber-incident has never been experienced). Bringing these results into relation, there could be a connection indicating that a limited knowledge on cyber threats results in a reduced risk awareness. We have not yet further explored on this in the present WiP paper, but we plan to perform further statistical analyses on this matter.

Besides this knowledge on cyber threats, one major aspect in our survey was the employees' awareness about cybersecurity in general, and security trainings in detail. This includes information about cybersecurity measures and trainings as well as the repetition of these trainings within the respective organizations. As described in the previous section, only 27% of respondents were informed about cyber incidents in the first place, which would be an indication that the communication of cyber attacks and their consequences to the all employees is rather low in these organizations. This can be underlined with other results from our survey, as about 50% the respondents felt not too well informed about IT or cybersecurity measures and guidelines (giving an average of ≈ 2.5 on a 1..5 Likert scale ranging from "very well informed" to "not informed"; excluding "no answer" in this average). Consistently with this, costly security actions like penetration tests have been reported as regular practice by only 22% of participants, while 18% indicated that no such tests were done and about 61% do not know if any penetration test has happened (this could be explained as such tests are usually not made public). Analogous answers were provided for the existence of emergency plans, which 42% of participants reported to exist, whereas 16% of respondents told to have no such plans at hand (the remainder of respondents indicated that they were unaware of any such plans). When it comes to supply chains, our survey shows that cybersecurity aspects are under-represented in employees' awareness or in the company's security policy design: among 1014 participants answering on a scale from 1 ("no supply chain risk awareness/management") up to 5 ("well developed awareness/risk management of supply chain incidents"), an average response of ≤ 3.3 points out that some awareness about supply chain risks exists, but it has room for improvement.

Overall, this emphasizes the limited availability of organizational measures as stated in the previous subsection and in the literature (Erdogan et al. 2023; Junior et al. 2025; Tetteh 2024). Our survey indicates a decent need for information campaigns to raise employees' awareness about guidelines and emergency plans including the actions

that are required to be taken in cases of a cyber incident. This also includes the planning of trainings and hands-on exercises, making sure that employees not only hear about what in theory needs to be done but are also able to practice security measures under realistic conditions.

Cybersecurity Trainings

Training activities have been a core aspect of our survey and the results clearly indicate that cybersecurity trainings represent an important tool to prepare employees for incidents and, at the same time, increase their awareness for cybersecurity threats. A first view on the results provides the impression that there is a correlation between an employee's risk perspective (as covered in the previous paragraph) and the time since the last training: the estimation for a cyber incident happening at the respective company is more critical if an employee recently attended a training or an awareness-raising measure. Although we have not done the statistical analysis, yet, for this WiP paper, this would better reflect the real-life occurrence of cyber threats within organizations.

Further, the results from our survey provide an indication that cybersecurity trainings are mainly focused on employees working in the IT and OT context (66% said that they received a training in the past 12 months) although it would be favorable to train all employees on these topics. In particular, the percentage of employees on management level (i.e., 24%) and senior level (i.e., 28%), that have not received a training in their current organizations is worrying (see also Figure 3. The highest ratio is within the group of "other employees" where 38% said that they never received a training. It can be argued that the "other employees" might not be too much involved in the IT processes of an organization; however, we want to stress that phishing and ransomware attacks are particularly targeted at (and most effective in) this group of employees, as they often represent the initial vector of compromise in such an attack. Out of the respondents, who have never received training at their current company (i.e., $n = 313$), 73% reported that there simply was no security training offered that they could have taken, while 12% did not take it because it was not mandatory, and another 8% out of lack of interest. This could also be linked to the fact that budgets for cybersecurity measures are low and, therefore, training capacities might be limited and not offered to all employees (if they are offered at all).

Related to the specific content, participants who received IT or cybersecurity training at current company (i.e., $n = 608$), reported that they underwent trainings that covered aspects of data protection, the correct behavior in a case of an IT incident, but also matters of correct password management and other (standard) security precautions. However, only 43% of those 608 respondents also were trained on ransomware scenarios, and only 35% reported that they heard about supply chain attacks.

Moreover, the more time passed since the last training also influences how well the employees remember the contents of that training. In detail, 86% of the trained employees remember the contents "very good" or "good", if the training took place just six months ago; this holds true for 84% if it took place less than 12 months ago. For periods of more than 12 months, only 56% remember the contents "very well" or "well". Accordingly, this implies that shorter training cycles (at least every 12 months) will improve the effectiveness of the training and thus also the preparedness of the employees for cyber incidents.

Additionally, 39% of all respondents reported to never have taken part in a training involving a simulated attack scenario at their current company, with at least 23% telling to never have been informed about contemporary threats, having been in online trainings (26%) or awareness campaigns. This strongly points to the need for more hands-on training activities, such as simulation or scenario-based tabletop exercises, particularly when it comes to cybersecurity within supply chains, with an emphasis to understand dependencies of the enterprise to external actors and forces.

Recommendations

Based on our findings and implications described in the previous sections, we would recommend the implementation of specific cybersecurity awareness trainings on top of already existing programs.

1. **Technical measures** according to the state-of-the-art. This is already very well covered in current reports and guidelines issued by ENISA, CrowdStrike or other studies like (Erdogan et al. 2023; Junior et al. 2025) (as mentioned in Section "*Top Security Measures*") and also well-implemented in organizations according to the responses in our survey. A major aspect is to keep hardware and software up to date and patch known vulnerabilities (which will also be a major requirement in the EU's Cyber Resilience Act).

2. **Information campaigns** on existing IT Security Policies and emergency plans in an organization for all employees. Although people working in an IT- or OT-related context are already well-informed about these

regulations (as our survey shows), we see it as important that the information reaches a wide audience within an organization, since emergency plans, in particular, become more effective the more people know about them.

3. **General awareness campaigns** about the cyber threat landscape, attacker strategies and security measures. Similarly to the information campaigns, making a large part of the employees aware of how cyber attacks (e.g., phishing, ransomware, etc.) work will improve their attention and preparation for real incidents. This can be done using webinars, video tutorials or "simulated" phishing attacks initiated by the organization itself.

4. **Table-top exercises** as a combination of training and awareness building to let people "experience" a cyber-incident, challenging them to take actions according to emergency plans, and to actively seek contact to responsible persons and cyber experts (if these roles are explicitly defined, and known). These exercises can be done "offline" as pen-and-paper version or "online" using a closed virtual environment, i.e. a Cyber Range, where people can test their skills hands-on.

5. **Simulation exercises** to understand potential impacts of cyber incidents on business processes, particularly along the supply chain. This can also be understood as a combination of training and awareness measures, as people are motivated to look beyond the boundaries of their daily business processes. By exploring the dependencies on external resources and events hands-on in a specific scenario, they expand their own cybersecurity perception and improve their preparation for complex effects and less likely scenarios.

LIMITATIONS AND OPEN POINTS

Although we have reached a rather high sample of 1014 participants in our survey, who are employed by different companies from different sectors (see Section "*Methodology and Survey Setup*" above), we want to stress again that the findings and implications of the survey need to be understood in this context. For example, we are unable to provide information on how many different companies the respondents work for, due to the survey design and to protection of the respondents' anonymity.

Additionally, the validity of the results applies to employees in companies with 10 or more employees in Austria and is therefore limited in some aspects. First, statements about companies are based on personal assessments and should therefore be understood as subjective perceptions; such assessments may differ from the actual organizational realities. Second, it is not always certain that respondents can validly assess certain organizational characteristics, such as questions regarding budgets or specific structural conditions within the company. Third, socially desirable response behavior, limited validity of individual assessments, and subjective perceptual biases must be considered as general limitations of the data collection.

Furthermore, various forms of potential sampling bias must be considered. In terms of selection bias, the sample consists exclusively of individuals who are part of an online survey pool and who generally agree to participate in surveys. An attempt was made to reduce potential non-response bias by keeping the survey open for an extended period. Coverage bias cannot be ruled out, as participation required sufficient language proficiency in German. Additionally, self-selection bias is possible, as an incentive was offered upon completion of the online survey to increase willingness to participate.

Finally, we want to highlight that the implications and improvements drawn in the previous section are based on a descriptive analysis of the survey results. As we are presenting our work in progress, we are in the process of producing more significant analyses, including statistical inference and hypothesis testing, to gather more grounded implications from the data.

CONCLUSION AND VISION

The scientific literature and technical reporting from various industrial actors substantiates the situational demand for increased security preparation of employees, going beyond pure reliance on technical security measures. Although such measures have been widely implemented and deployed, humans remain the weakest – and often the "less informed" – element of the security chain. Our survey indicated that limited resources (time and budget) and a lack of structure in security awareness and training activities could be a reason for that. Further, a long turnaround time for trainings (above 1 year) decreases their effectiveness as participants hardly remember the contents. Regarding training setups, our survey shows that table-top exercises and simulated attack scenarios are underrepresented, whereas they could provide more active involvement and hands-on experience for the employees. Hence, we conclude from our survey results that recurrent communication and information campaigns will improve employees' awareness of cybersecurity threats and measures. Combined with hands-on trainings, employees will be better prepared for cyber attacks and, as a further consequence, the organizations' resilience will be improved.

Accordingly, we will further investigate on the relations between information campaigns and cybersecurity awareness and how tailored training activities like hands-on security assignments and threat scenario simulations can support improving cybersecurity awareness and the overall organizational resilience. For the future, we envision more strategic activities and processes for improving cybersecurity awareness to be integrated in organizations of all size. This could be realized in an interplay of classical learning sessions, e.g., in workshops, discussion groups or (online) training courses, and interactive, simulated hands-on training scenarios. These awareness building activities could be supported by artificial intelligence, e.g., to create realistic storylines adaptable to beginners and experts, as well as immersive technologies such as virtual or augmented reality. This will make the trainees' experience in those scenarios more realistic, giving them the opportunity to encounter threats and attacks as well as to implement measures in a practical, real-life setup.

ACKNOWLEDGEMENT

This work was supported by the research project SOPHIE (Project-Nr. FO999905291), which is funded by the Austrian Federal Ministry of Finance (BMF) as part of the Austrian National Security Research Program KIRAS.

REFERENCES

Allianz (2025). *Cyber security resilience 2025 – Claims and risk management trends*. Tech. rep. Munich, Germany: Allianz Commercial.

Amorim, V., Fernandes, A., and Filipe, V. (Jan. 2025). "Analyzing the Impact of the CrowdStrike Tech Outage on Airport Operations and Future Resilience Strategies". In: *Procedia Computer Science*. CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 256, pp. 633–640.

Austrian Institute of Technology (AIT) (Nov. 2023). *SOPHIE - Resilienz von Supply Chains gegenüber Kaskadeneffekten aus dem digitalen Raum*.

Bada, M. and Nurse, J. R. C. (July 2019). "Developing cybersecurity education and awareness programmes for Small and medium-sized enterprises (SMEs)". In: *Information & Computer Security* 27.3, pp. 393–410.

BBC News (May 2021). "Cyber attack 'most significant on Irish state'". In: *BBC News*.

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., and Adeusi, K. B. (May 2024). "Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies". In: *Global Journal of Engineering and Technology Advances* 19.2, pp. 134–153.

Bing, C. and Kelly, S. (2021). *Cyber attack shuts down U.S. fuel pipeline*.

CISA (2022). *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*. Tech. rep. Washington, DC, USA.

Crowdstrike (2025). *2025 Global Threat Report*. Tech. rep. Austin, Texas, USA, p. 53.

Department of Home Affairs (2023). "Security of Critical Infrastructure (Critical infrastructure risk management program) Rules". In: *Federal Register of Legislation*, LIN 23/006.

ENISA (Nov. 2025). *ENISA Threat Landscape 2025*. ENISA Reports.

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., and Pickering, J. (2023). "Cybersecurity Awareness and Capacities of SMEs:" in: *Proceedings of the 9th International Conference on Information Systems Security and Privacy*. Lisbon, Portugal: SCITEPRESS - Science and Technology Publications, pp. 296–304.

European Comission (2016). "NIS Directive (2016/1148)". In: *Official Journal of the European Union*, pp. L 194/1.

European Comission (2022). "NIS 2 Directive (2022/2555)". In: *Official Journal of the European Union* L 333/80.

Fertig, T. and Schütz, A. E. (2020). "About the Measuring of Information Security Awareness: A Systematic Literature Review". In: *Hawaii International Conference on System Sciences*.

FortiGuard labs (2025). *2025 Fortinet Global Threat Landscape Report*. Tech. rep. FortiGuard Labs.

Junior, C. R., Becker, I., and Johnson, S. (Nov. 2025). "Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity". In: *arXiv:2309.17186 [cs]*.

Kereopa-Yorke, B. (June 2023). "Building Resilient SMEs: Harnessing Large Language Models for Cyber Security in Australia". In: *arXiv:2306.02612 [cs]*.

Mugu, S. R., Zhang, B., Kolla, H., Balaji, S. R. A., and Ranganathan, P. (Oct. 2024). "Lessons from the CrowdStrike Incident: Assessing Endpoint Security Vulnerabilities and Implications". In: *2024 Cyber Awareness and Research Symposium (CARS)*, pp. 1–10.

Ponsard, C., Grandclaudon, J., and Bal, S. (2019). "Survey and Lessons Learned on Raising SME Awareness about Cybersecurity:" in: *Proceedings of the 5th International Conference on Information Systems Security and Privacy*. Prague, Czech Republic: SCITEPRESS - Science and Technology Publications, pp. 558–563.

Singapore Statutes Online (2018). *Cybersecurity Act 2018*. Tech. rep. Singapore.

Statistik Austria (2024). *Arbeitsmarktstatistiken 2023 Ergebnisse der Mikrozensus-Arbeitskräfteerhebung und der Offene-Stellen-Erhebung*. Tech. rep. Statistik Austria.

Tetteh, A. K. (2024). "Cybersecurity Needs for SMEs". In: *Issues In Information Systems*.

Zerr, K. (2007). "Security-Awareness-Monitoring". In: *DuD Datenschutz und Datensicherheit* 31.7, pp. 519–523.

Zerr, K. and Benner, A. (Feb. 2017). "Kennzahlen eines mitarbeiterorientierten Sicherheitsmanagements". In: *Datenschutz und Datensicherheit - DuD* 41.2, pp. 80–87.

Zetter, K. (2020). "SolarWinds Hack Infected Critical Infrastructure, Including Power Industry". In: *The Intercept*.