Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27861-cd

Human-Centered Cybersecurity Training for SMEs: Results from developing and testing a tailored training approach.

Stine Aurora Mikkelsplass

Risk and Security Department, Institute for Energy Technology, Norway. E-mail: stine.aurora.mikkelsplass@ife.no

Espen Nystad

Human and Organizational Factor Department, Institute for Energy Technology, Norway. E-mail: espen.nystad@ife.no

Per-Arne Jørgensen

Digital Sovereignty Department, Institute for Energy Technology, Norway. E-mail: per.arne.jorgensen@ife.no

Small and medium-sized enterprises (SMEs) face increasing exposure to cyber threats yet often lack the resources and expertise needed to implement robust security measures. This paper presents findings from a project addressing this challenge by developing and evaluating a tailored approach to cybersecurity training for SMEs. The project, led by IFE in collaboration with an SME industry partner, aimed to strengthen the SMEs' digital resilience through targeted and practical training. Building on previous research on SME cybersecurity, this work adopts a human-centered approach integrating psychological principles, human factors, and technical expertise. A comprehensive needs analysis was conducted to identify organizational vulnerabilities and competency gaps. Based on these insights, a modular training program was designed, emphasizing risk awareness, threat landscapes, and incident preparedness. Interactive methods, including group exercises and facilitated discussions, were used to increase engagement and learning outcomes. The training was piloted within the partner SME, followed by a structured evaluation assessing relevance, usability, and behavioral impact. Findings indicate that targeted training supports employees' understanding of cybersecurity risks and response strategies. However, sustainable behavioral change requires continuous reinforcement and strong leadership commitment. To support scalability, the project produced a step-by-step guide enabling SMEs to develop customized training programs aligned with their operational context. This work demonstrates that innovative, human-centered approaches to cybersecurity education can effectively enhance SMEs to digital resilience. By providing a practical, adaptable training framework, this study offers a concrete pathway for SMEs to strengthen their cybersecurity capabilities.

Keywords: awareness, SME, cybersecurity, training, human-centered, resilience, competence building

1. Introduction

Emerging digital threats, combined with a long history of cyber-attacks against small and medium enterprises (SMEs) (Unger, 2021) demonstrate that SMEs may be particularly vulnerable to such threats. Limited resources, constrained expertise, and a lack of access to relevant cybersecurity tools make SMEs an easy target (Junior et al., 2025). Therefore, such businesses, need a clear understanding of their information assets, dependencies and potential threats (NSM, 2024a). To address this challenge, employees can serve as an effective line of defense against cyber-attacks by participating in training and following established security routines. However, this requires that the company's cybersecurity policy is known and understood by employees, that the training methods and content are adapted to the target group, and that security measures are perceived as appropriate (Karlsson et al., 2017). The most effective way to ensure these conditions is to involve employees in designing and implementing security measures (Hedström et al., 2011). E-learning courses are a time-efficient and widely used approach to employee training, but organizations often struggle to ensure that employees complete such courses consistently over time (Haney et al., 2022).

This paper presents results from a Norwegian Research Council-funded project conducted in 2025 aimed at strengthening cybersecurity competence in SME organizations. The study addresses the following research questions; RQ1: How can a general cybersecurity course be tailored to the needs of a specific SME, with attention to people, organization, and technological conditions? RQ2: How can engagement with SME stakeholders support the development of cybersecurity training that improves employee awareness and resilience?

The paper is structured into the following chapters: it begins with the background and motivation for the project, moves on to discuss the applied methodology and results from an SME case study, then presents a discussion on implementing customized training, and concludes with final remarks.

2. Background and related work

2.1 *Relevant cybersecurity standards and principles for SME*

Though there are several cybersecurity standards and best-practice principles available for SMEs, it can be challenging to grasp and align comprehensive standards such as the ISO 27001/27002 and NIST Cyber Security Framework for an SME with limited resources. In Norway, the National Security Authority (NSM) has developed basic information, communication and technology (ICT) principles as guidelines for SMEs, offering simplified security measures and controls derived from a harmonized version of the ISO 27002. The NSM ICT security principles are adopted to the Norwegian SME context, and addresses 21 security principles and 118 security measures across the following categories: (1) “Identify and map” to establish understanding of the organization and services, (2) “Protect and maintain” to maintain and withstand a secure state over time, (3) “Detect” to identify known threats and vulnerabilities, and the last principal (4) “Respond and recover” to prepare, handle and recover from an incident. However, following even a minimum of these principles can be overwhelming for smaller SMEs, as they require some basic knowledge within IT, risk assessment and vulnerability management. To enable more SMEs to take advantage of these principles, further simplification is needed. In our project, we suggest identifying a minimum subset of these security controls to be pragmatically prioritized together with the SME. Combined with a mapping of staff's cyber maturity, this comprises the basis for developing learning goals for a customized course with an approach that may be replicated by other SMEs.

2.2. *Human-Centered Training and Competence Building*

To achieve effective outcomes when designing cybersecurity courses for SMEs, it can be useful to draw on principles from learning theory that improves motivation by focusing on the things that matter and are relevant in the learner's everyday work situation. One relevant principle is the use of collaborative learning, which have shown to bring improvements in involvement and motivation (Laal & Ghodsi, 2012). When learning occurs in groups rather than individually, an increased understanding can be produced by the sharing of different viewpoints and experiences. In the context of cybersecurity, discussions can also contribute to a shared understanding of policies and practices. Another principle is to anchor the learning in concrete examples from the participants' own work context. This helps connect new knowledge to already existing practices and understanding, and can improve transfer of training to the work setting (Kolb, 1984; Nafukho et al., 2017).

Nyusti and colleagues (2025) introduced a cybersecurity course tailored for a diverse group of SMEs, delivered through a two-day classroom-based format that combined foundational instruction with collaborative group activities. Course topics ranged from incident preparedness to employee engagement, approached from a cybersecurity perspective. Unlike the prior course, which targeted participants from various business sectors, the work presented in this article examined how these courses could be used in a tailored approach to cover a gap between recommendations from cybersecurity standards and the actual challenges faced by SMEs to reach compliance with the standards. We address how to perform practical steps to assess a company’s current situation in relation to staff maturity level, risks and threat landscape and how to use this as a basis for implementing cybersecurity

competence building and practices, and improve cybersecurity awareness in the company.

We explored how employees in small and medium-sized businesses can be involved in training and awareness-raising activities about relevant threats, vulnerabilities and security measures in a way that contributes to motivation, engagement and compliance.

The emphasis has been on developing a method that other businesses can easily replicate, enabling SMEs to strengthen their cybersecurity competence for the benefit of both their company and their employees. The method focuses on designing training based on the company's and employees' specific needs and assumptions, finding learning methods that make the staff engage with the material, implementing the course and evaluating course effectiveness. The project is based on the assumption that engaging training promotes greater understanding, motivation and appropriate security behavior.

The experiences from the project can serve as a guide for how SMEs can plan and carry out this type of training, either on their own or with support from external actors.

3. Approach and findings

This project employed a mixed-method, human-centered approach grounded in collaboration between researchers and the SME. The project drew on both qualitative and quantitative methods to build a comprehensive understanding of the SME's cybersecurity maturity. Qualitative approaches, such as interviews, workshops, site observations, and document analysis, allowed us to gain insight into daily work practices, perceived risks, and organizational routines. These insights were complemented by quantitative data from a cybersecurity maturity survey, enabling us to examine broader patterns across the workforce. The purpose with this combination of methods was to understand the SME's operational context, employee needs, and existing cybersecurity maturity level.

The following four stages were established for the comprehensive method: (1) identify needs for competence improvement, (2) development and customizing of the training materials and completion of courses, (3) evaluation of the courses, as well as (4) summary and guidance with handover for them to conduct further internal training by themselves.

3.1. Identifying and analyzing needs

*S*ite visits and workshops were conducted to better our understanding of the organizational structure, operational activities, core supporting systems of the SME and relevant information assets, risks and vulnerabilities. Additionally, we focused on identifying the cybersecurity maturity level of the SMEs employees. The steps of the needs analysis are described below.

3.1.1 *Familiarization with the SME*

Approach: An initial meeting was held with the company to get an introduction to the SME, as well as a tour of the facilities. Employees from the SME's administration and production groups were represented in the needs analysis. The initial meeting aimed to introduce the SME to the research group, clarify roles and expectations, gain an overall understanding of the company's daily operations, computer systems, data management infrastructure and their dependencies. The familiarization phase also included a review of company documentation, such as the official company presentation, which provided a more comprehensive overview of the organization's roles and functions.

Findings: The SME employs 16 staff members and operates within the waste-management sector, organized into production and administrative functions. The management group oversees the overall operations, while the operational team handles core processing waste management activities. ICT services are outsourced to an external IT provider, but due to the complexity and business-critical nature of the systems, the company retains an internal IT role. This in-house specialist manages daily IT operations and serves as the primary liaison with external providers.

The company interacts with its customers through a web portal used for communication and order placement, requiring high system availability. The company's IT environment can be characterized as hybrid, combining on-premises services, i.e. local file access with cloud-based Microsoft 365 services, including security functions managed by the IT provider. The external provider also hosts the Enterprise

Resource Planning (ERP) system and the customer portal.

Not all employees had previously undergone computer security courses or training under the auspices of the company, but tips and information about data security were distributed at irregular intervals by the IT manager. In addition, data security was addressed in the company's weekly internal meetings.

3.1.2. *Risk assessment*

Approach: A joint workshop was held with SME representatives to assess risks, identify key information assets , and evaluate relevant vulnerabilities and threats (Næringslivets sikkerhetsråd, 2024). The research group facilitated a risk assessment and covered topics focusing on the SMEs ICT systems. All information was documented in an excel sheet.

Findings: The risk assessment was further analyzed by the research group to identify additional dependencies, vulnerabilities, and threats. The findings from this risk assessment were then mapped to the security controls in NSM ICT Security Principles, a framework for ICT security published and maintained by the Norwegian National Security Authority (NSM, 2024b).

3.1.3 *Alignment with management*

Approach: Systematic learning and follow-ups require grounding based in management and leadership. Therefore, the results of the site visit and risk assessment were presented to the CEO to inform management of the project's findings and approach and include the CEO's perspective.

Findings: The alignment with management allowed the research group to gain the CEOs perspective on which challenges the SME faced, both in terms of protecting against cyber-attacks, but also in terms of digitalization and prospects for the company. This dialogue offered valuable input for understanding management's viewpoint and ensuring the project's direction reflects organizational priorities.

3.1.4 *Maturity assessment*

Approach: Tools to assess employee cybersecurity maturity or awareness do exist (e.g. (Parsons et al., 2014). However, because each SME may be different in what information systems they have, how they use those systems, and what specific vulnerabilities and risks are relevant to the company, it may be necessary to tailor the assessment to each company. We developed a maturity assessment for addressing the cybersecurity maturity of the SME employees, based on the knowledge acquired in previous steps. This assessment took the form of an anonymous survey consisting of 23 statements that the respondents were asked to indicate their agreement with, on a 7-point response scale. The survey addressed both non-technical and technical topics, and focused on the understanding of threats, data systems, and information assets, securing devices, cybersecurity awareness and attitudes, and the identification and handling of possible threats. The survey was distributed to all staff members.

Findings: 75% of the employees completed the survey. Some main findings were that the staff baseline of cybersecurity knowledge and understanding was relatively high, but there was a difference in maturity levels between the two groups of employees, and a high degree of variation in the responses to questions about security-related behavior and attitudes. This could indicate lack of clarity or understanding of company policies in some areas. There were also variations in attitudes towards the importance of employees for company cybersecurity. The mapping provided input to course development by pointing to the knowledge level of employee groups, variations in behavior and attitudes, and the extent to which internet was used or required for work tasks.

3.2. *Course Development and Implementation*

The course material created in this project served as a prototype to evaluate our method. The developed course was partially based on previous work done with SMEs (Nyusti, Mikkelsplass, Lygren Toppe, et al., 2025) as notes in Section 2.2. This basis was further developed using input from workshops, assessments of business risks and critical systems, identified threats and vulnerabilities, conversations with senior management, and findings from the maturity survey. Based on this input, a course with the following four core topics was developed:

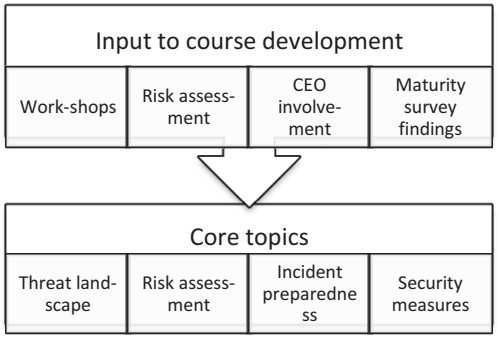

Figure 1 Core topics

Threat landscape: The survey indicated a gap in staff awareness regarding the current digital threat environment, including rapid technological change, evolving geopolitical conditions, the complexity of interconnected systems, and the risks posed by social engineering.

Risk assessment: the needs identification indicated a gap in foundational knowledge of risk assessment in relation to cyber security and core company operations. The maturity assessment found that staff had no clear agreement on the company's information assets.

Incident preparedness: the needs identification indicated a lack of knowledge and preparation on how to prepare for, and handle, incidents affecting ICT or operational systems. Risk assessment identified the need for an incident preparedness plan that could be supported by a table-top exercise. For instance, this exercise helped inform which vendors, customers and third-party suppliers would be crucial to contact if an incident occurred.

Security measures: the survey indicated high degree of variation among employees regarding security-related behavior and use of security measures, for instance it was reported that some downloaded non-standard software to company computers or logged into personal accounts on the company PCs.

The pedagogical structure of the course was designed to ensure systematic learning and active engagement among participants. Every topic began with an overview of the key concepts, followed by an activity to engage participants. Activities varied between topics, but they all followed the same approach: individual – group – plenary (IGP). In practice, this means that the participants were first asked to consider a task or activity individually, then discuss their thoughts within a group. Lastly, we would have a plenary discussion sharing findings from all participants. The training was delivered in two half-day on-site sessions, with mixed groups from administration and production teams. The agenda was structured so that the first topic established a foundation, with each subsequent topic building on the previous one to enhance understanding. A dedicated tabletop cybersecurity incident exercise was incorporated to enable participants to simulate and respond to realistic cybersecurity scenarios.

All materials and activities were customized according to participants' roles and the identified baseline cybersecurity maturity for the SME staff. This tailoring ensured relevance to the SME context and addressed the specific needs of both administrative and production staff members.

3.3. *Evaluation*

Approach: After the course, the participants replied to a survey aimed at evaluating the content and execution of the course. The evaluation was based on a self-assessment of three of the four levels of evaluation described by (Kirkpatrick, 1996). The employees' own experience of the course (level 1) was assessed with statements about the relevance and difficulty level of the four course topics and to what extent participants felt that they benefited from each of the topics. For the learning approaches (PowerPoint presentation, group tasks, peer discussions and exercise) the participants evaluated memorability and engagement. Ratings for level 1 used a 5-point scale from very low to very high, except difficulty level, which was rated from *much too advanced* to *much too easy*. Improvement in knowledge, skills or attitudes (level 2) was assessed by asking whether the course had increased the employee's understanding of information assets, threats and vulnerabilities; improved ability to contribute to the company's cybersecurity and improved cybersecurity awareness. Expected changes in cybersecurity behavior as a result of course participation (level 3) was assessed by a single question. For levels 2 and 3 the participants rated agreement with the statements on a 7-point scale from *Strongly agree* to *Strongly disagree* (see Figure 3).

Findings: 80% of the participants responded to the evaluation survey.

Employee experience of the course (level 1): 80% of the respondents rated the course topics “preparedness", "security measures", and "threat landscape" as relevant for their work situation to a very large extent or to a large extent, while the corresponding number for the topic "risk assessment" was 63%. Group tasks and peer discussions were rated as the learning approaches most conducive to remembering the material, and group tasks, peer discussions and the exercise were seen as the most engaging approaches.

63% of participants strongly agreed or agreed that the course contributed to increased understanding of information assets, threats and vulnerabilities; improved their ability to contribute to cybersecurity and improved their understanding of why cybersecurity is important (level 2 in Figure 3).

Only 37% of respondents expected to make changes in their cybersecurity behavior (level 3 in Figure 3).

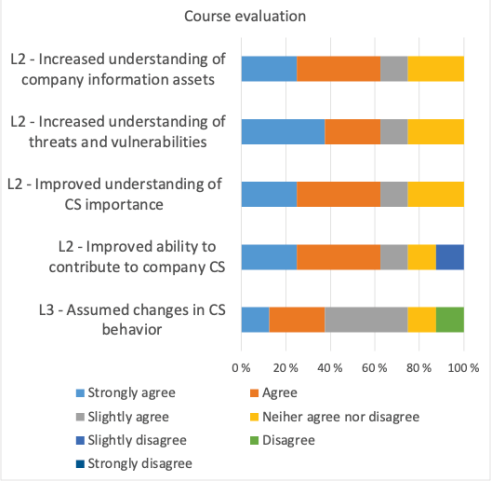

Figure 3, showing level 2 (L2) and 3 (L3) course evaluation (according to Kirkpatrick)

3.4 *Developing a Reusable Methodological Toolkit*

The project resulted in a reusable methodological toolkit for SMEs, consisting of a step-by-step guide and a web-based tool with templates and checklists to support practical implementation.

The step-by-step method developed in this project follows the sequence anchoring and planning, needs analysis, development, implementation, and evaluation. To support SMEs in applying the approach, we provide several practical resources and downloadable templates, including a risk- and value-assessment checklist, a maturity survey, and an evaluation form. To make our work available for other SMEs, the templates and guides developed in this project have been made available on IFE’s website https://cybersikkerhet.ife.no. The following recommendation requires a continuous improvement approach to provide new input for measuring and improving cybersecurity awareness.

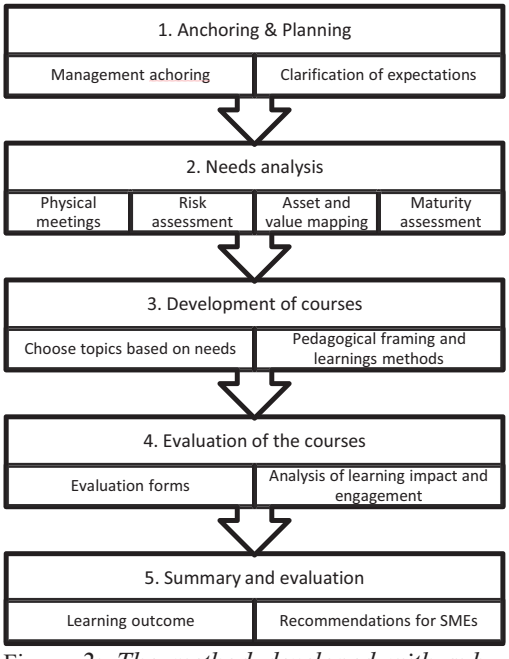

Figure *2: The method developed with sub-tasks*

4. Discussion

Addressing RQ1, the study demonstrates that tailoring a general cybersecurity course to the needs of a specific SME requires a systematic process that integrates organizational, technological, and human factors. The project employed a comprehensive needs analysis involving site visits, workshops, document reviews, and assessments of work practices, enabling the researchers to gain a detailed understanding of the SME’s structure, systems,

and risk exposure. By examining operational dependencies, ICT configurations, and security routines, the team ensured that the course content directly reflected the SME's actual technologies and vulnerabilities.

The participant feedback indicated that group activities and peer discussions were successful learning approaches, while observations made by the researchers indicated that company context contributed to perceived course relevance. Participant's own evaluation of improvements in knowledge, skills or attitudes and changes in behavior indicates that the participants take-away from the course was more in the form of increased understanding and changes in attitudes than impacts on behavior. This is in line with previous research on the effect of cybersecurity training (Prümmer et al., 2025). In our case this result could reflect the proportion of knowledge-related vs behavior-related topics in the course, and it corresponds to the result from the maturity assessment that staff already had a relatively good understanding of what behaviors were needed to secure SME information. This finding also shows that cybersecurity courses may need to better highlight the link between knowledge, attitudes and security practices, as well as a possible need for additional strategies to drive behavior change, such as support from management or suitable incentives.

The mid-course tabletop exercise allowed participants to explore business-continuity options during a simulated cyber incident and clarify roles and responsibilities. Employees shared insights into system dependencies, business processes, and supply-chain concerns, expressing strong trust in external IT providers for restoring operations. The exercise raised practical questions about what employees should do before, during, and after an incident and underscored the value of shared situational awareness.

Turning to RQ2, the findings highlight the importance of stakeholder engagement in developing effective cybersecurity training. Management involvement aligned the project with strategic priorities and strengthened its legitimacy, while employee workshops captured tacit knowledge and operational challenges that grounded the training in real practices. Collaborative learning through peer discussions, group tasks, and tabletop exercise, supported shared understanding and showed how employees' situational knowledge contributes to the discussions. Co-developed templates, checklists, and assessment tools further built internal capacity.

4.1. *Challenges and Limitations*

Implementing the course in a real SME setting highlighted several practical and organizational challenges. As noted in prior research (Karlsson et al., 2017), meaningful behavioral change in cybersecurity requires ongoing reinforcement, visible leadership support, and integration of new practices into existing policies and processes. The delivery format, two half-day, on-site sessions with mixed groups from administration and production, introduced operational constraints related to shift coverage, logistics, and participation tracking. Due to limited staffing redundancy, only a small number of production employees were available to attend, which reduced representation from key operational roles. As a single-SME pilot with a small participant group, the study is also limited by the absence of long-term follow-up to evaluate sustained impact.

Participation dynamics varied across the two course groups. The CEO joined the first group, which appeared to encourage stronger engagement, curiosity, and openness to discussion. In contrast, the second group showed slightly lower engagement. Since senior management is chiefly responsible for a company's security, having the CEO attend the course demonstrates to employees that cyber-security is taken seriously. This experience suggests that including managers or designated cybersecurity champions in each session may strengthen employee participation, reinforce shared responsibility for security practices, and help anchor learning in the company's operational reality. Group composition, prior involvement in the project, and participants' familiarity with the topics all appear to influence engagement levels and learning outcomes.

5. Conclusions and Future Work

Employees are the company's greatest resource, making it essential for the management teams to invest in skill development and increase cybersecurity awareness. One of the findings is that the training program should provide for

continuous evaluation and adaptation of the content, for example, by using questionnaires that measure the participants' experience, learning outcomes and changes in attitudes. In this way, an SME can ensure that the training remains relevant and meets the actual needs of the organization. Discussing and sharing security challenges with colleagues should not be underestimated, as they contribute to a common understanding of threats and guidelines for good practice to build a resilient culture within the company.

Effective cybersecurity training begins with management support, clear planning, and a thorough needs analysis of information assets and skills gaps. The resulting course is tailored to the company's context and employee maturity, using engaging, practical methods. Training must be ongoing to address evolving threats and business needs. Success requires embedding training in the organization, ensuring relevance for employees, and driving real change in practice.

Acknowledgement

This project was funded by the Norwegian Research Council for the program call NCC-NO: "Innovasjonsstøtte til morgendagens cybersikkerhet", project 357653. We also want to thank our close collaborating SME partner, and a special thanks to the great staff.

References

Haney, J., Jacobs, J., & Furman, S. (2022, November). *NIST Security Awareness Study*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=933391

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373–384. https://doi.org/10.1016/j.jsis.2011.06.001

Junior, C. R., Becker, I., & Johnson, S. (2025). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. *Journal of CyberSecurity*, 1–31. https://doi.org/10.48550/arXiv.2309.17186

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, *67*, 267–279. https://doi.org/10.1016/j.cose.2016.12.012

Kirkpatrick, D. (1996). Great Ideas Revisited: Revisiting Kirkpatrick's Four-Level Model. *Training & Development*, *50*, 54–57.

Kolb, D. (1984). Experiential Learning: Experience As The Source Of Learning And Development. In *Journal of Business Ethics* (Vol. 1). Prentice Hall.

Laal, M., & Ghodsi, S. (2012). Benefits of collaborative learning. *Procedia - Social and Behavioral Sciences 31 (2012) 486 – 490*. https://doi.org/10.1016/j.sbspro.2011.12.091

Næringslivets sikkerhetsråd. (2024). *Mørketallsundersøkelsen 2024*. https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2024

Nafukho, F., Alfred, M., Chakraborty, M., Johnson, M., & Cherrstrom, C. (2017). Predicting workplace transfer of learning: A study of adult learners enrolled in a continuing professional education training program. *European Journal of Training and Development*, *41*, 00–00. https://doi.org/10.1108/EJTD-10-2016-0079

NSM. (2024a). *Risiko 2024—Nasjonal sikkerhetsmyndighet*. Nasjonal sikkerhetsmyndighet. https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2024

NSM. (2024b, June 18). *NSM ICT Security Principles—Nasjonal sikkerhetsmyndighet*. https://nsm.no/advice-and-guidance/publications/nsm-ict-security-principles

Nyusti, L., Mikkelsplass, S. A., Lygren Toppe, A., & Jørgensen, P.-A. (2025). Building Cyber Resilience in SMBs—Lessons From the Project Cyber Innovation Network. *35th European Safety and Reliability Conference (ESREL 2025) and the 33rd Society for Risk Analysis Europe Conference (SRA-E 2025)*, 2908–2915. https://doi.org/10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P5291-cd

Nyusti, L., Mikkelsplass, S. A., Toppe, A., & Jørgensen, P.-A. (2025). *Building Cyber Resilience in SMBs—Lessons From the Project Cyber Innovation Network* (p. 2915). https://doi.org/10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P5291-cd

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on End-users: A Meta-analysis. *Computers & Security*, *150*, 104206. https://doi.org/10.1016/j.cose.2024.104206

Unger, A. (2021). *Susceptibility and Response of Small Business to Cyberattacks* [Master's thesis]. Utica College.