Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P5291-cd

Building cyber resilience in SMBs - lessons from the project Cyber Innovation Network

Levente Nyusti

Security & Risk, Institute for Energy Technology (IFE), Norway. E-mail: levente.nyusti@ife.no

Stine Aurora Mikkelsplass

Security & Risk, Institute for Energy Technology (IFE), Norway. E-mail: stine.mikkelsplass@ife.no

Aleksander Lygren Toppe

Security & Risk, Institute for Energy Technology (IFE), Norway. E-mail: aleksander.lygren.toppe@ife.no

Per-Arne Jørgensen

Security & Risk, Institute for Energy Technology (IFE), Norway. E-mail: per.arne.jorgensen@ife.no

Small to medium-sized businesses (SMBs) form the backbone of Norway's economy. SMBs are defined as businesses or enterprises with fewer than 100 employees and constitute over 99 percent of Norway's active businesses. Consequently, SMBs frequently hold key positions within our society in sectors such as healthcare, telecommunications, and energy, as well as serving as suppliers for critical infrastructure. However, SMBs often don't have the resources to employ dedicated security staff or to outsource their cybersecurity needs. The project Cyber Innovation Network (CIN) aims to build cybersecurity competence in SMBs by creating a collaboration between industry, academia and research institutions. Our project shows that while these SMBs lack the know-how to protect against cyber threats, this type of collaboration can provide effective countermeasures in the ever-evolving threat landscape. The CIN project has received much positive feedback. This paper details our approach for teaching fundamental cybersecurity principles for SMBs. Furthermore, this paper also presents our approach, experiences, feedback received and lessons learned in building cybersecurity competence in SMBs.

Keywords: Cybersecurity, Small to medium-sized businesses, Security awareness, Resiliency, Employee training.

1. Introduction

In Norway, Small to Medium-sized Businesses (SMBs) are defined as businesses or enterprises with fewer than 100 employees (Nærings- og fiskeridepartmentet 2019). In 2024, The Confederation of Norwegian Enterprise released a report about SMBs, stating that in 2022, 99% of enterprises in Norway were SMBs (The Confederation of Norwegian Enterprise 2024). As reported in The Norwegian National Security Authority's (NSM's) report for 2024, SMBs deliver vital services or products for both private citizens and industries, integral for modern society, and potentially serve as suppliers for Critical Infrastructure (CI) (NSM 2024b), such as healthcare and societal services, as well as electricity, gas and water supply for a well functional society. In an evolving digital threat landscape SMBs face challenges with the tools and competence necessary to defend themselves against digital threats and cyberattacks. However, due to the relatively small workforce and limited revenue of these businesses, hiring a full-time cybersecurity specialist or fully outsourcing cybersecurity management is often not financially feasible. As a consequence, the SMBs are often the most vulnerable and least capable to withstand and recover from cyberattacks (NSM 2024b). As also reported in (NSM 2024b), cybercriminals exploit SMBs' limited resources and cybersecurity knowledge to their advantage, making them easy targets. Furthermore, it is also a general understanding that the police will most often not have the resources to follow up cases where such cyberattacks are reported (SMBNorge 2024).

Through the project Cyber Innovation Network (CIN), we aimed to build competence and upskill the SMB workforce in topics related

to cybersecurity though a collaboration between research, academia and industry. Topics includes subjects within general security measures, the evolving threat landscape, risk management and developing contingency plans. This was done hosting a two-day introductory "crash course" in cybersecurity, where we provided easy-to-understand overviews specifically tailored for SMBs. This course was held twice, and the SMBs were invited to join free of charge. This paper details our approach for teaching fundamental cybersecurity principles for SMBs. Furthermore, this paper also presents our approach, experiences, feedback received, and lessons learned in building cybersecurity competence in SMBs.

Section 2 discusses the background for this work, including some of the challenges SMBs face. In Section 3, the cybersecurity challenges related to SMBs are described, and how these can be addressed. Section 4 shows the structure of the cybersecurity course we developed and how these courses were held. In Section 5, we present the results achieved, in form of interest for these courses and feedback received from the participants. In Section 6 we discuss the challenges of creating such a course and lessons learned. Finally, Section 7 concludes this paper.

2. Background

In 2023, a Norwegian IT company was compromised, and as a result of that, customers of the IT company lost access to their systems completely, and it took approximately seven months before these systems were recovered (Norheim 2023). In the article, it is explicitly mentioned that three SMBs lost access to their systems for a longer period, resulting in loss of up to 4.5 million Norwegian krone. The cyber-insurance only covered three months of service charge, which was according to the service level agreement, leading to significant monetary losses for the customers.

Use of assistive tools that utilize Artificial Intelligence (AI), like ChatGPT (OpenAI 2022), allows users to work more effectively and be more productive. Unfortunately, cybercriminals benefit from this technology the same way, which also presents a challenge for SMBs. While the full potential of AI is still under research, cybercriminals have already successfully used this technology to launch more deceptive attacks easier. AI has been utilized for cyberattacks giving instruction to the cybercriminal, craft better phishing emails and create deepfakes (Alawida et al. 2024), (Mirsky and Lee 2021). While legitimate tools like ChatGPT have guardrails in place to make it more diffcult to use it maliciously, there are also AI models that are purpose-built for cybercriminals, e.g. WormGPT (Lakshmanan 2023) and FraudGPT (Falade 2023).

SMBs face several challenges, like limited resources and time to follow-up suppliers; limited or no capability to handle incidents or implement technical security measures like endpoint-protection or configuring a firewall to protect the network. These, and other security measures seen as necessary in order to protect SMBs are listed in (NSM 2024a). While at least some of these challenges could be addressed by e.g. consultancy agencies, the cost of such services is often beyond what these companies have budget for. However, competence in managing supplier relations and requirement specification is lacking, and the SMBs are less trained and prepared in what to do when a cyber-attack strikes. While it is a challenge for SMBs to allocate the resources necessary, research and academia is often highly updated in the field of cybersecurity, and might be able to solve some of the cybersecurity needs SMBs have. This includes the challenge of learning how to stay ahead of the cybercriminals and how to apply some cybersecurity best practices, to build cybersecurity resilience in an ever-evolving threat landscape. According to (Næringslivets Sikkerhetsråd 2022), 28% of the reported security incidents are related to the lack of employees security awareness.

As SMBs lack the resources to handle cybersecurity appropriately, one solution often utilized is to hire an Information and Communication Technology (ICT) professional, who would also be responsible for cybersecurity. However, as cybersecurity is recognized to be a comprehensive field, it is challenging for one person to set up, operate and maintain the ICT systems, stay updated in both fields, and follow cybersecurity and internal controls best practices, which state that one should use separation of duties (Hu, Kuhn, and Yaga 2017).

3. Identifying and addressing SMB cybersecurity challenges

The goal of this project was to utilise the competence and skill already present in higher

education and academia to improve the security and resilience of SMBs in terms of cybersecurity and preparedness to handle an incident. We aimed to examine *how to effectively build competence and upskill the SMB workforce in cybersecurity challenges.* Specifically, we wanted to focus on "quick and easy" security measures that would not require any prerequisite knowledge about cybersecurity, only the most basic IT skills. An additional goal of the project was to create a network for local SMBs, a forum for knowledge sharing and collaboration regarding cybersecurity challenges. To achieve this goal, we followed several steps: 1) Identify SMB need and challenges through survey design and objective, sample selection, and data collection and analysis. 2) Design cybersecurity seminar, including development of course content, creating a training format, and participant engagement with knowledge sharing and group work. Lastly, 3) evaluation of program with feedback collection and limitations.

3.1. *Identifying SMB needs and challenges*

Developing a course based on the needs require input from the SMBs themselves. We started the information gathering process by looking into their needs and current challenges using the business associations network and meetings. We held two meetings in neighbouring counties, where the business associations invited their members for an informal information gathering regarding SMB cybersecurity challenges. The meetings started with an introduction to the CIN project, including partners and overall objectives. Following this, participants were split into groups of 2-4 persons to discuss current cybersecurity challenges. Lastly, we summarised all the feedback collectively. From the two information meetings, there were over 50 participants in total. Feedback we gathered included insufficient cybersecurity competency, financial cost of cybersecurity personnel, shared responsibility with vendors and suppliers, reliance on vendors and suppliers, challenges upskilling current workforce in cybersecurity.

3.2. *Designing and developing an engaging cybersecurity course*

To enhance learning, the presenters created a fictitious small startup business use-case, called EventTicket. During the course, the participants were assigned to different groups and were tasked to solve group activities that had EventTicket as the subject. In the tasks where it was required that the participant has more extensive knowledge about the enterprise, it was encouraged that the participants use their own enterprise as the subject.

4. Course structure

The course was built up by four sessions each day. Between each session, we had a short break of 15 minutes. The structure of the seminar was organised for two days. The first day focused on introduction, terminology and the concepts followed by a risk assessment workshop and security measures. The second day sessions focused on the Threat Landscape and Demonstration of Cybersecurity Tools; Contingency Plan; Event Handling and Recovery; Requisition Requirements for Suppliers & Employee-training

Introduction & Terminology and Concepts

This was an introductory session, where the participants got to know the CIN network, program, partners, the fictive scenario introduced, and common terminology and concepts used in cybersecurity. In addition to setting the goal and expectations for the outcome of this course, this session ensured that the participants had the necessary vocabulary to follow the rest of the course. Asset, vulnerability, safety, security, and risk are some of the definitions explained in this session.

Risk assessment

In this session, the participants were introduced to the basic methods and principals of risk assessment and current regulations and standards for cybersecurity relevant for SMBs. The method used as guideline were based on the ISO 27005 risk assessment process. Here, the participants got a basic understanding of risk assessment, risk management, how to comply with current regulations and a step-by-step guide for risk assessment and building a risk matrix. Finally, the participants were shown how to create a basic risk mitigation table supported by a risk tool developed and adapted by the CIN network.

Security Measures

We addressed how to mitigate risks using ransomware attack as a scenario for the session, where we systematically convey how to prevent, contain and recover from such an attack. The session was primarily technically focused, but we also addressed the importance of implementing the security measures as a part of a larger planned process. This is important as to not overload the organization and to build better understanding for the policies chosen. We referred to Norway's national ICT resources where applicable during this session, such as the Norwegian National Security Authority, specifically the NSM's ICT Security Principles (NSM 2024a). Further, the Data Protection Authority's guidance and templates on GDPR and Internal Control were also presented. General resources such as Nettvett (Nettvett 2024), NorSIS (NorSIS 2024) were also used, particularly as a more personal guidance for individuals, not only in a business context. Examples of some categories where security measures were addressed include Internet Exposed Resources, Identities and Accounts, Phishing, Social Engineering, Third Party systems and Vendors, Data Loss and Recovery. Focus was on the most critical measures, such as Multi-Factor Authentication (MFA), software updates, and establishing a sustainable ICT security culture. Finally, the participants performed a group activity where they could reflect on security measures that are currently in-place at their enterprise, and what security measures are missing, which ended in a plenum discussion.

Threat Landscape

The participants were presented an up-to-date digital threat landscape based on openly available intelligence reports from public and private sectors. During the lecture, the participants were presented information about whom to alert in case of a breach, depending on which sector is the most relevant for the SMB. NSM have announced that there should be low threshold for SMBs to report incidents to the national cybersecurity centre (NCSC) regardless of severity and consequences. The information used building up this lecture session included the NSM's yearly national security report Risk (NSM 2024b), ENISA's foresight (enisa 2024) and Telenor's digital security report (Telenor 2024). The NCSC has a national pulse indicator for cyber threats (nsm.no/pulse) and an alert page from NCSC for security vulnerabilities and recommendation actions to follow (NCSC 2025). Some of the new threats mentioned by ENISA involves compromised value chains, disinformation campaigns and more IoT devices online on unsecured networks. Knowing the threats and methods is essential for building good security measures around the values for an SMB by protecting their most valuable assets.

One of the best sources to learn and get insights is from those who have experienced cyber-attacks, as they can inform how they handled the incident and recovered from the situation. However, sharing information after incidents about lesson learned requires following a certain protocol. For this we mentioned that there exists the Traffic Light Protocol (TLP) (CISA 2022) for classification of incidents and how to share relevant information about a security incident to the security communities and authorities.

Participants were encouraged to share own cybersecurity experiences and challenges among each other in order to build trust. They were also encouraged to subscribe to both national and different community driven security news channels. This to help with notifications of new vulnerabilities and potential threats when building resilient SMBs. The risk assessment process presented in the first session was utilized to identify potential threats. At the end of this session, the participants were given a group assignment to identify possible threats that would be relevant for EventTicket use-case, and also what type of threats are relevant for their own enterprise.

Demonstration of Cybersecurity tools

Demonstration of cybersecurity tools was more of a practical session, where the participants were presented a few cybersecurity tools that are openly available from vendors like Hak5. In addition to seeing these tools and realising how trivial it is to purchase and use these, the participants also got demonstrated a few attack scenarios and what threat actors can achieve using these tools. In this session, the participants were also introduced to the concept Open-Source INTelligence (OSINT), physical cybersecurity tools, such as the Hak5 Pineapple (Hak5 2024) and software tools such as Shodan (Shodan 2024). Once the participants realised the threat these

tools present, we also presented what makes these attacks possible, and what security measures can mitigate these threats. The group activity for this session was to use OSINT techniques presented to gather as much information as possible about an enterprise or a person (with consent) in the group.

Contingency Plan, Event Handling and Recovery

In this session, the participants were introduced to the idea that cybersecurity incidents are going to occur, the only question is when (Paulsen and Toth 2016). For this reason, especially for SMBs, exhaustive planning is utterly important, as it can be the difference between bankruptcy and successful recovery. To appropriately convey this, the participants were presented with what contingency plan, event handling and recovery are, what differentiates these, why these are important and how to prepare to handle a cyber incident. For this session, we used resources like The Norwegian Business and Industry Security Council's (NSR's) emergency poster (NSR 2022), NSM ICT Security Principles (NSM 2024a) and The National Institute of Standards and Technology's (NIST's) Small Business Information Security (Paulsen and Toth 2016).

Requisition Requirements for Suppliers

In this session we presented the importance of setting requisition requirements in a greater detail and why risk assessment is important to better quality and value for the SMBs when performing requisition. Furthermore, we also presented how to follow-up the suppliers in a shared responsibility model in practice. The group activity encouraged the participants to identify the cyber assets in their own company and identify appropriate requirements for their own business insurance. In such a way, the participants could identify what digital assets were critical for their operation, and how long they could stay in business (availability), should something happen to the service supplier. The main message during this session was to pinpoint that the SMBs are always responsible for IT operations. This includes all information and data used and stored in the suppliers services. The same applies for devices and computers, and all the accounts and identities used by the business.

Agreements based on "good weather conditions" when cyber-attacks strike, are not much worth for an SMB. A good agreement requires that both parties understand their responsibilities and duties when operationalising the conditions. Especially, when third-party subcontractors are involved in delivering the services for the SMB to understand potential supply chain risks.

During the presentation, we also introduced product security as a topic, and especially the risk introduced by placing unsecured IoT devices into the existing infrastructure without necessary hardening. A good practice to reduce the attack surface is to place IoT devices on a dedicated network segment. We presented the guidelines from NSM on supplier requirements (NSM 2020) as a guideline to address and comply with in order to reduce some of the uncertainties in a shared-responsibility-model agreement in practice.

Employee Training

The focus of this session was how to empower employees to contribute to the overall security of the business. Focusing on employee engagement, the session outlined various ways management can build a secure workforce. Figure 1 illustrates one such way, where top management is responsible for setting cybersecurity on the agenda and keeping up the engagement. We highlighted the importance of building competence, which in turn empowers and motivate employees to contribute to securing the business. Participants were presented with various scenarios highlighting cybersecurity awareness among employees. As part of the cybersecurity training, employees should be taught how to protect themselves and their families from their own digital environment. When employees understand that the same security practices used at work can protect their personal and private data, cybersecurity habits become ingrained in their daily lives. Other topics for this session were how often employee training should occur, how management can encourage it and bring more attention to cybersecurity. Examples include online courses, posters, gamification techniques and newsletters. The group activity for this session was to create an annual wheel for cybersecurity topics in EventTicket AS and discuss how the use of this wheel should be implemented. Figure 1 shows a

workflow for how to ensure employee engagement.

Fig. 1 How to create employee engagement

5. Results

In total, two courses were held at the Østfold University College in Fredrikstad. These courses were announced using social media sites like LinkedIn, creating a post on the municipality's website and sending marketing emails to those that were in contact with the project members regarding this course. All these included information about the course like how many sessions there would be, title for these sessions and a short description about what to expect. The first course was held in January 2024, the second in September 2024.

Mentimeter (Mentimeter 2024), an interactive online survey platform, was used to collect feedback from the participants. In order to receive feedback on different aspects of the course, the survey was divided into three sections. First, the participants were asked to give feedback on the subjects presented during the course using a ranking scale. The second section asked participants to type in what they found most useful during the course. The answers were given in an open-ended text box, i.e., they were not restricted by pre-defined alternatives. While the participants answered, Mentimeter dynamically formed a word cloud of their responses. Lastly, we asked participants for recommendations on areas for improvement and topics to be covered in greater detail. Responses were collected through an open-ended text box and visualized as a word cloud.

Fig. 2. shows the feedback received regarding the subjects included in the course. To measure this, the participants were asked to vote how much they agree with the following four statements, starting at the top: (1) "The subjects were easy to understand", (2) "The subjects were conveyed in a manner that was easy to understand", (3) "The subjects were difficult" and (4) "The subjects were relevant for me". The scale went from 1 to 5, where 1 represent "Strongly disagree" and 5 represent "Strongly agree". The number on each scale shows the average for the given question. The distribution visualization shows how the responses vary for each question.

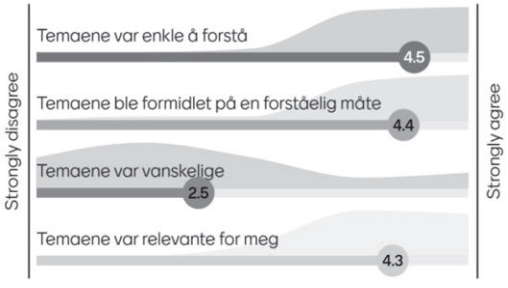

Fig. 2. Feedback received after the first session

By their nature, word clouds create new objects for the same word if the word was misspelt or written in another language. For this reason, instead of including a figure of the word cloud, we summed up the same values (misspelt and foreign language) and only include the top 5 here. The top 5 from the word cloud "what was the most useful about this course" are the following: Risk management; preparedness; practical session; vulnerabilities; get to know each other. The top five phrases from the word cloud on "recommendations on what could have been done better, and what subjects we should have included more" were as follows: AI; nothing; templates; setup; and ISO27000.

One of our key goals was to also establish a cybersecurity network for SMBs, enabling them to share insights and experiences to make their businesses more secure. Insights from the project also highlighted the need for a dedicated forum where SMBs can learn about cybersecurity, with topics specifically relevant to them. To address this, we decided to create a board comprising one

representative from each partner organisation—IFE, Østfold university college, and the business associations. The board will organise one to two cybersecurity courses per year for SMBs.

6. Discussion

Day 1 and day 2 of the course was structured differently, both in terms of content and working groups. The first day we focus primarily on risk management, while day 2 was structured as sessions with diverse topics such as threat landscape, contingency plan, event handling and recovery. Both days, the participants were engaged, actively asking questions and working together during group activities. This indicates that the participants were actively listening and found the subjects interesting and useful. As Fig. 2. shows, the course got positive feedback, where the responses indicated that the subjects were understandable, conveyed in an easy-to-understand manner, not too difficult, and relevant for the participants. In total, 26 participants filled out the survey.

As mentioned earlier, one of the main challenges remain to the SMBs host and maintain an up-to-date ICT infrastructure due to core business focus and less ICT resources. SMBs are often dependent on suppliers and outsource IT services for management and operation. It is crucial that SMBs have the capabilities to learn and translate the functional and technical requirements and communicate these during requisition to a supplier.

One challenge for this project was to decide on topics to fit the competence levels of the participants. To support the varied competence level for security measures, we had some specialised material to be used as aid in discussions if needed, such as secure coding practises, network topologies, and vulnerability scanning. The first time this course was held, there was a wide range of cybersecurity expertise and knowledge levels by the participants. Although this was expected, communicating cybersecurity to such a diverse group of participants was challenging.

Another challenge was presented by how we, the cybersecurity experts, communicate with each other compared to those with less cybersecurity experience. To communicate efficiently with each other, we often rely on the use of complex terminology and acronyms. While this makes communication between cybersecurity experts efficient, it introduces another layer of confusion for those with less experience in this domain. Acknowledging this, our presentations were prepared to include as few of these terminologies and acronyms as possible. However, while presenting the course, we often either presented subjects as well-known facts or introduced terminologies and acronyms. This was especially a challenge when attempting to answer a question from the audience. While we were transparent about this challenge to the audience, and asked them to stop us and let us know if we use an expression or term they were not familiar with, they were often hesitant to do so. It was however highly beneficial that we were not the only presenter in the room, as our colleagues often recognized when this happened, and could either supplement the presenter or let the presenter know about this.

7. Conclusion

This paper presented our methodology to create a course in which we educate SMB employees on the complex topic that is cybersecurity. Once the necessary subjects were identified, we created a two-day cybersecurity course, where we gave a presentation about these subjects, concluding the presentation with a group activity. In this paper, we included the course structure, a quick overview of the content and the feedback received.

Based on our experience, and the feedback received, creating such courses and performing them is highly relevant and educational for the participants. The feedback shows that: 1) The subjects were easy to understand, 2) The subjects were presented in a manner that is easy to understand, 3) The subjects were not difficult, 4) the subjects chosen were highly relevant for the participants. Our finding is that the structure of this course worked well, and the group activities were a crucial part that helped participants engage with, and learn, the material. This underscores the importance of in-person engagement in cybersecurity education, especially for people with no previous experience in the topic.

Acknowledgement

We would like to thank Østfold Fylkeskommune for funding the CIN project. Furthermore, we would like to acknowledge our partners from Østfold University

College; Ketil Stølen for the work he put into developing the course itself, the material, and presenting the lectures, and Vikash Katta and André Hauge for the initiative putting this on the agenda and the efforts put into the development of these courses. Lastly, we would like to thank our partners from Sarpsborg- and Fredrikstad Næringsforening for a successful collaboration.

References

Alawida, Moatsum, Bayan Abu Shawar, Oludare Isaac Abiodun, Abid Mehmood, Abiodun Esther Omolara, and Ahmad K. Al Hwaitat. 2024. "Unveiling the Dark Side of ChatGPT: Exploring Cyberattacks and Enhancing User Awareness." *Information* 15 (1): 27. https://doi.org/10.3390/info15010027.

CISA. 2022. "Traffic Light Protocol (TLP) Definitions and Usage | CISA." August 16, 2022. https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage.

enisa. 2024. "Foresight Cybersecurity Threats For 2030 - Update 2024: Extended Report." Report/Study. ENISA. 2024. https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-extended-report.

Falade, Polra Victor. 2023. "Decoding the Threat Landscape : ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, October, 185–98. https://doi.org/10.32628/CSEIT2390533.

Hak5. 2024. "WiFi Pineapple." Hak5. 2024. https://shop.hak5.org/products/wifi-pineapple.

Hu, Vincent, Richard Kuhn, and Dylan Yaga. 2017. "Verification and Test Methods for Access Control Policies/Models." NIST Special Publication (SP) 800-192. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-192.

Lakshmanan, Ravie. 2023. "WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks." The Hacker News. July 15, 2023. https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html.

Mentimeter. 2024. "Interactive Presentation Software." 2024. https://www.mentimeter.com/.

Mirsky, Yisroel, and Wenke Lee. 2021. "The Creation and Detection of Deepfakes: A Survey." *ACM Comput. Surv.* 54 (1): 7:1-7:41. https://doi.org/10.1145/3425780.

Nærings- og fiskeridepartmentet. 2019. "Småbedriftslivet - Strategi for små- og mellomstore bedrifter." https://www.regjeringen.no/globalassets/departementene/nfd/dokumenter/vedlegg/smabedriftslivet-uu.pdf.

Næringslivets Sikkerhetsråd. 2022. "Mørketallsundersøkelsen 2022 er nå tilgjengelig." 2022. https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2022-er-na-tilgjengelig.

NCSC. 2025. "Varsler fra NCSC - Nasjonal sikkerhetsmyndighet." January 2025. https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/.

Norheim, Håkon Jonassen. 2023. "Saksøkte eget IT-selskap etter hackerangrep." NRK. October 11, 2023. https://www.nrk.no/rogaland/saksokte-eget-it-selskap-etter-hackerangrep-1.16576138.

NSM. 2020. "Riktige og gode krav til IKT-tjenesten og til leverandør - Nasjonal sikkerhetsmyndighet." July 1, 2020. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/riktige-og-gode-krav-til-ikt-tjenesten-og-til-leverandor/.

———. 2024a. "NSM ICT Security Principles - Nasjonal Sikkerhetsmyndighet." June 18, 2024. https://nsm.no/advice-and-guidance/publications/nsm-ict-security-principles.

———. 2024b. "Risiko 2024 - Nasjonal sikkerhetsmyndighet." February 12, 2024. https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2024.

NSR. 2022. "Nødplakat for digitale angrep." 2022. https://www.nsr-org.no/aktuelt/nodplakat.

OpenAI. 2022. "ChatGPT." 2022. https://chatgpt.com.

Paulsen, Celia, and Patricia Toth. 2016. "Small Business Information Security: The Fundamentals." NIST IR 7621r1. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7621r1.

Shodan. 2024. "Shodan." Shodan. 2024. https://www.shodan.io.

SMBNorge. 2024. "Kriminalitet Mot Næringslivet Må Tas På Større Alvor! | SMB Norge." June 11, 2024. https://smbnorge.no/kriminalitet-mot-naeringslivet-ma-tas-pa-storre-alvor/.

Telenor. 2024. "Digital Sikkerhet 2024." Digital Sikkerhet 2024 - Har vi Tid Til å Vente? 2024. https://www.telenor.no/om/digital-sikkerhet/2024/.

The Confederation of Norwegian Enterprise. 2024. "Tall og fakta om SMB." February 6, 2024. https://www.nho.no/tema/sma-og-mellomstore-bedrifter/tall-og-fakta-om-smb/.