Cybersecurity Practices, Challenges and Posture in Small and Medium Enterprises: A Survey-Study in Sweden

Anton Lindkvist, Eira Höglund and Fatiha Djebbar
Department of Engineering Science, University West, Trollhättan, Sweden

fatiha.djebbar@hv.se
anton.lindkvist@student.hv.se
eira.hoglund@hv.se

Abstract: The ongoing digitization has increased businesses' dependence on IT systems, thereby increasing their susceptibility to cyberattacks. This problem is particularly significant for Small and Medium Enterprises (SMEs) due to their limited resources and expertise in cybersecurity. Considering their essential role in the economy, protecting SMEs from cyber threats is vital for economic stability and growth. This study presents a survey analysis involving tech-oriented SMEs in Sweden to comprehensively assess their cybersecurity posture. The survey included 369 Swedish SMEs across various regions of Sweden. The quantitative and qualitative analyses indicated a lack of cybersecurity knowledge, challenges in developing secure products, and inadequate compliance with cyber-standards due to constraints related to lack of guidance, budget, time and staff shortage.

Keywords: SMEs, Cybersecurity posture, Cyber Threats, Cybersecurity awareness, Standard and compliance

1. Introduction

Recent technological advancements have revolutionized society, enabling extensive online interactions and increasing businesses' reliance on IT infrastructure, thus heightening their exposure to cybersecurity threats (Kappe et al., 2023). In Sweden, small enterprises (1-10 employees) constitute 97% of registered companies, with SMEs making up 99.9% of the business sector, playing a vital role in economic stability (SAERG, 2020). However, SMEs face significant vulnerabilities due to limited resources and minimal cybersecurity expertise (Basheer Ullahi et al., 2022; Djebbar and Nordström, 2023). Protecting SMEs from cyberattacks is crucial, yet 60% lack recovery capacity within six months, leading to severe financial impacts (SAERG, 2021; IVA, 2022; Cartwright and Edunc, 2023). Nordic leaders like Denmark and Finland also struggle with cybersecurity standards expertise. This study evaluates cybersecurity readiness in Swedish tech-focused SMEs (under 250 employees, revenue below 50 million euros) using 369 survey responses (300 from 2,400 calls, 69 from forms), analyzing security practices and adherence to standards (European Commission, 2003). It identifies challenges, investment drivers, and policy compliance, offering recommendations to enhance cybersecurity against threats like ransomware (ISACA, 2021). As a pioneering study in Sweden, it builds on Nordic research to safeguard SMEs (Fleron et al., 2020).

2. Related Work

This chapter presents the theoretical background for the study, outlining key concepts essential for understanding the research. Each section focuses on a specific aspect that contributes to the overall context and foundation of the work.

2.1 Background

This section focuses on the importance of cybersecurity for SMEs in Sweden, as they rely more on digital technologies for their operations and growth.

2.1.1 SMEs and their significance in the economy

SMEs are vital to economic health, driving entrepreneurship, innovation, and integration into supply chains (Cartwright et al., 2023). They form the largest business sector, typically 95% of firms, supporting jobs, growth, and innovation, and per the World Trade Organization, over 90% of businesses, 60–70% of employment, and 55% of GDP in developed economies, plus 20% of biotech patents in Europe (Bayraktar, 2019). Nationally, SMEs boost growth, tax revenue, and jobs, aiding local businesses and enabling international engagements that benefit economies (Varga, 2021).

2.1.2 Cybersecurity in SMEs

Despite their economic importance, SMEs often fall behind in cybersecurity, leaving them vulnerable to attacks that can severely affect their operations. Unlike larger companies, SMEs typically do not prioritize cybersecurity to the same extent, and several factors contribute to this disparity (Chidukwani et al., 2022):

- Lack of internal expertise: SMEs frequently lack dedicated resources and expertise in cybersecurity, hindering their ability to implement and maintain necessary security measures (Ponemon Institute, 2018).
- Financial constraints: Limited financial resources make it difficult for SMEs to invest adequately in cybersecurity (Ponemon Institute, 2018).
- Lack of knowledge on effective application of cybersecurity: Many SMEs do not understand how to effectively implement and manage cybersecurity measures, including best practices and threat management (Ponemon Institute, 2018).

2.1.3 Importance of compliance for SMEs

Retaining returning customers is vital for SME growth and stability due to their size and limited resources. Creating a sense of security and confidence in the company is essential. Data breaches threaten customer information and the company's reputation. Investing in cybersecurity and adhering to standards and laws is crucial to protect customer data (Lloyd, 2020). Larger companies often depend on SME networks for products and services. Therefore, compliance with cybersecurity standards and regulations such as the NIST framework, ISO 27001:2022 (ISO/IEC, 2022), ETSI (Djebbar and Nordström, 2023), and GDPR (Freitas, 2018) is essential for SMEs in Europe, including third-party processor compliance (Lloyd, 2020). The NIST Cybersecurity Framework, developed by the National Institute of Standards and Technology, aims to help organizations identify, manage, and mitigate cybersecurity risks. The framework consists of five core functions: Identify, Protect, Detect, Respond, and Recover, which together provide a model for a systematic and resilient cybersecurity effort (NIST, 2024). Keeping up with evolving regulations can be challenging for SMEs, and staying informed offers advantages. Proactive SMEs should also conduct a risk analysis study to adapt to changes and enhance customer trust through strong data security practices (Lloyd, 2020; Djebbar et al., 2023).

2.2 Related Work

SMEs are essential to the global economy, significantly contributing to employment and generating over half of the world's GDP (Bayraktar, 2019). Their influence extends into financial realms, making them crucial in cybersecurity discussions. The European Digital SME Alliance states that 60% of SMEs cannot recover from a cyberattack within six months (SAERG, 2021). SMEs make up 95% of businesses in most countries (European Commission, 2003). Despite their prevalence, they often lack strong cybersecurity measures (Kappe et al., 2023). Disruptions in IT infrastructure pose a serious threat to their viability, especially as they focus on digitization over IT security. While some use basic security measures like backups and firewalls, overall awareness is low, leading to a fragmented security approach and a lack of proactive strategies (Kappe et al., 2023). Micro and small businesses are particularly vulnerable due to limited resources and expertise, making them more susceptible to cyberattacks (Cartwright and Edunc, 2023). The evolving technological landscape poses challenges for SMEs in staying updated, so enhancing cybersecurity awareness is a fundamental step. Various training programs exist, though they can be overwhelming (Ponsard and Bal, 2019). Authors (Järvinen and Shojaifar, 2020) offer a framework for improving cybersecurity across different SME profiles, identifying five types: cybersecurity abandoned, unskilled, expert-connected, capable, and cybersecurity provider SMEs. A study from Ahlborg University (Falch et al., 2023) suggests that SMEs can protect themselves by understanding the importance of cybersecurity investments based on the NIST framework. The study emphasizes the need for comprehensive protection strategies. Denmark, a highly digitized nation, still sees many SMEs lacking adequate security measures due to insufficient expertise and the complexity of multiple standards (Fleron et al., 2020). Adhering to standards and regulations is crucial for gaining customer trust and avoiding fines, but SMEs often lack the resources to comply effectively (Freitas, 2018; Pedroso et al., 2021). Authors in (Fernandez de Arroyabe et al., 2023) examine SME resilience in managing, adapting to, and recovering from cyber incidents, highlighting machine learning's role in identifying security relationships. Similarly, (Carías et al., 2020) provides a framework for simplifying cyber resilience practices. European countries show varying digitization levels, affecting their cybersecurity experiences. A 2022 EU report (European Union, 2022) compares cybersecurity awareness across 27 countries. In Sweden, 17% of managers are very well informed about cyber risks, with 28% conducting training in the past year. In Finland, 13% of managers are very well informed, with 22% having conducted

training. In Denmark, 28% of managers are very well informed, with 18% having conducted training. The work in (Armenia et al., 2021) recommends the SME Cyber Risk Assessment (SMECRA) for dynamic risk assessment. Although the NIST Cybersecurity Framework (CSF) is widely used, many studies lack practical guidance for SMEs (Chidukwani et al., 2022). The European Union Agency for Cybersecurity (ENISA, 2021) identifies common challenges, including low awareness and inadequate protection, leading to vulnerabilities like weak passwords and unlocked devices. SMEs often view cybersecurity as an additional cost rather than an investment and implementing standards like ISO 27001 is difficult due to limited expertise. Only 12 Swedish SMEs are fully compliant with ISO 27001 (Certifiering.nu, 2024). The BYOD trend, accelerated by COVID-19, presents additional security challenges for SMEs, which often lack the budget for secure devices. Low management support further exacerbates these issues (ENISA, 2021). Clear guidance for implementing cybersecurity standards is needed, as highlighted by StandICT.eu and SMESEC (StandICT, n.d.; SMESEC, n.d.). ENISA's report (ENISA, 2016) categorizes obstacles to standard adoption, emphasizing the need for increased knowledge, better capabilities, and cooperation. Nordic countries like Finland and Denmark generally perform well in cybersecurity compared to other European nations (European Union, 2022). However, there is a lack of comprehensive studies on Swedish SMEs' cybersecurity posture. This work aims to analyze their security weaknesses to prioritize cybersecurity and improve protection as digitization increases. With better knowledge and awareness, Swedish SMEs can safeguard their operations more effectively.

3. Research Methodology

The main phases of this study are outlined in Fig. 2. During the data-gathering phase, information was collected through a survey targeting approximately 2,400 SMEs in Sweden. The survey was aligned with the NIST framework to assess compliance with its core functions. It was administered both via phone interviews and email, with the majority of responses approximately 300 obtained through phone interviews after 2,400 calls. An additional 69 responses were gathered through email

distribution. The survey was anonymous and designed to evaluate several factors primarily related to cybersecurity preparedness (see Fig. 1). These factors correspond to the five core functions defined in the NIST framework (NIST, 2024): Identify, Protect, Detect, Respond, and Recover. Given the particular emphasis on the Identify and Protect functions in most cybersecurity efforts, a greater number of factors were included in these categories to reflect their critical role.

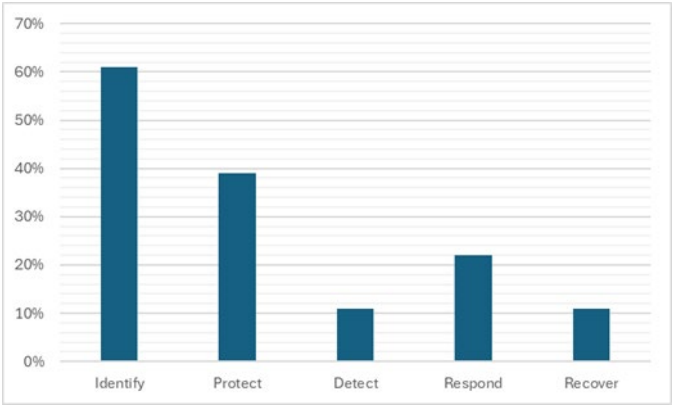


Figure 1: Categorization of the evaluated factors in the survey based on the NIST framework (NIST, 2024)

In total, 369 companies responded to the survey. In parallel, a literature review was conducted to examine existing research on SME cybersecurity. This review used targeted keywords such as cybersecurity, compliance, economy, SMEs, survey, and Sweden to identify relevant studies. The findings were synthesized to highlight common themes and discrepancies, allowing for comparative analysis with the survey results. The data analysis phase employed both qualitative and quantitative methodologies to examine security measures within SMEs. Qualitative analysis focused on evaluating the effectiveness of preventive security actions, preparedness for incidents, and response strategies. Quantitative analysis involved statistical evaluation of survey responses to assess the overall security posture of SMEs. This mixed-method approach enabled a comprehensive analysis and comparison, directly supporting the study's stated objectives.

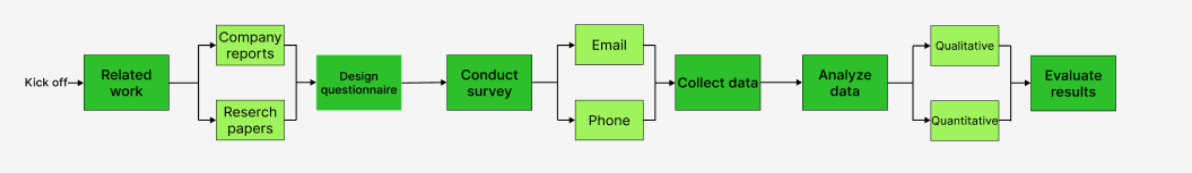


Figure 2: Flow diagram of the research methodology

4. Survey Study

This section describes the tasks carried out, encompassing the data collection process from the survey-study and subsequent data analysis.

4.1 Data Collection

This section outlines the tasks performed, including the data collection process for the survey study and the subsequent data analysis. Data collection relied on two primary sources. First, a literature review was conducted by searching scholarly databases (IEEE, Google scholar, Scopus) and company reports using specific keywords. The search scope was expanded after the initial results to gather additional relevant data. The reviewed literature was summarized and compared both with one another and with the survey results. Despite challenges in identifying high-quality literature, most sources reached similar conclusion. The second source involved a survey study targeting Swedish tech companies. A comprehensive questionnaire was initially administered through phone interviews with 2,400 SMEs. A total of 300 companies responded across six Swedish regions: Blekinge, Norrbotten, Östergötland, Skåne, Stockholm, Västra Götaland. Additionally, the survey was distributed via email to tech SMEs, yielding responses from 69 additional companies. In total, 369 SMEs participated in the survey, representing a significant sample size that adds robustness and credibility to the study. Survey responses were provided by either the CEO or the IT security officer. The 369 tech companies represent various sectors, including:

- Manufacture of electronic devices
- Manufacture of machines and other means of transport
- Manufacture of motor vehicles, vehicle parts, and accessories
- Manufacture of medical and dental instruments and accessories
- Telecommunications and computer programming and data processing companies.

4.2 Data Analysis Methods

To analyze the collected data, both qualitative and quantitative methodologies were employed. The questionnaire included open-ended written sections and multiple-choice questions. For qualitative data, thematic analysis was applied to identify recurring themes within the responses, categorizing them to provide an overarching understanding of the results. This approach ensured clear and well-supported insights from the textual responses.

Quantitative analysis focused on examining numerical data from the survey. Pivot tables were utilized for data cleaning and frequency analyses, enabling clear visualization of respondent's answers and facilitating comparisons with previous studies. Chi-square tests were conducted to validate the findings, identifying significant differences within the results. Additionally, we performed descriptive analysis on data from prior literature and surveys to identify prevalent trends among Swedish SMEs. These trends were then compared and evaluated against the data obtained in the current survey. This study is based on the participant population outlined in Table 1, which details the number of organizations categorized by employee count and region (headquarters).

Table 1: Shows the participant population through the number of organizations per number of employees per region (headquarters)

Number of employees	Blekinge	Norrbotten	Östergötland	Skåne	Stockholm	Västra Götaland	Other	Don't want to answer	Sweden
1-4	32	33	40	38	33	31	2	0	209
5-9	8	8	8	6	5	5	0	1	41
10-19	10	5	4	7	4	3	1	0	34
20-49	5	2	4	12	12	12	0	0	47
50-99	3	1	0	1	4	4	0	0	13
100-199	0	1	3	1	0	2	0	0	7
200	1	0	5	2	5	4	1	0	18
Total number of organizations	59	50	64	67	63	61	4	1	369

5. Result

This chapter presents the results of the study, highlighting the key findings derived from the data analysis. Each section addresses a specific outcome, offering insights that respond to the research questions and support the overall conclusions of the work.

5.1 Performance Analysis

The survey results are based on responses from 369 participants; however, not all participants provided answers to every factor evaluated. Table 2 presents the frequency of responses for each factor. Variations in the number of responses stem from certain assessed factors that raised privacy concerns or required follow-up questions based on participants' initial answers. For assessments offering "yes/no/don't know" options, only responses marked as "yes" or "no" are included, as the "don't know" option is considered too ambiguous for meaningful interpretation.

Table 2: Number of SMEs responding to each evaluated factor

Question in Appendix 1	Number of participants
1	369
2	369
3	369
4	353
5	200
6	208
7	210
8	193
9	181
10	340
11	359
12	360
13	174
14	246
15	369

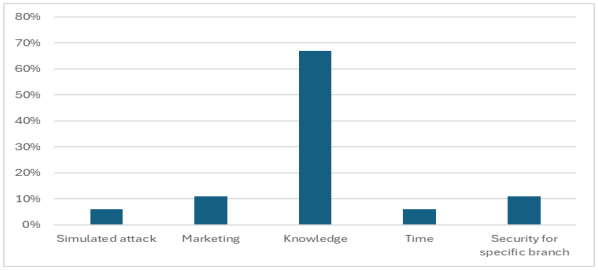
Some of the assessed factors have follow-up with textual responses. The number of participants who responded to these follow-ups is displayed in Table 3.

Table 3: Number of responses for the follow-up questions

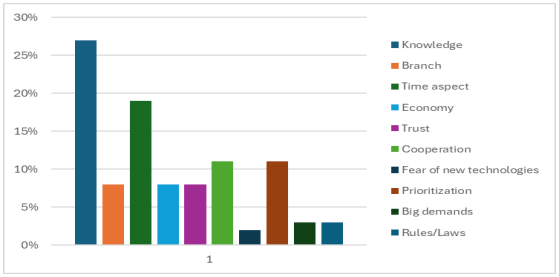
Follow-up questions in Appendix 2	Number of participants
1	37
2	18
3	59

5.2 Cybersecurity Challenges

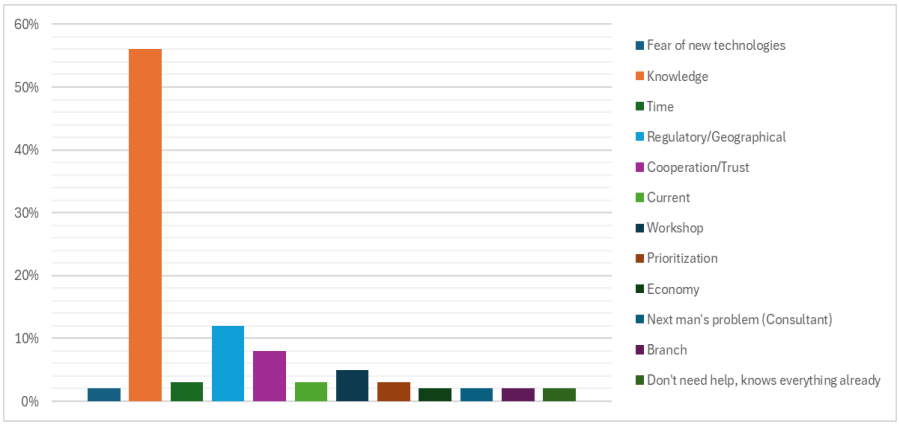
Data collected from both phone interviews and the online survey indicate that 27% of respondents (Fig. 3b) attribute their challenges in developing secure digital products and services to a lack of cybersecurity knowledge. Additionally, 19% of respondents cite time management as a contributing factor to these difficulties. Other factors mentioned include financial constraints, prioritization issues, collaboration challenges, compliance with laws and regulations, and trust-related concerns. Notably, 67% of respondents emphasized that addressing knowledge deficiencies is crucial for obtaining the necessary support to implement robust security measures, as illustrated in Fig. 3a. In response to inquiries about safe digitization, 56% of textual responses highlighted a widespread lack of societal knowledge about cybersecurity (Fig. 3c). Several respondents expressed a strong interest in expanding their understanding, acknowledging personal knowledge gaps, while others pointed out similar deficiencies among colleagues in their workplaces. Notably, one comment emphasized the importance of integrating education on digital safety and cybersecurity during early schooling stages.



(*a*)



(*b*)



(*c*)

Figure 3: Cybersecurity issues and needs in SMEs: (a) forms of assistance required in cybersecurity. (b) the challenges faced by participants in creating secure digital products and services, and in (c) the issues participants reported concerning digitization and cybersecurity

5.3 Techniques and Technologies Demand

The quantitative findings indicate that the most utilized techniques and technologies among organizations include cloud solutions, web and mobile applications, embedded systems, and hardware, as shown in Fig. 4 According to the results exhibited in Fig. 5, 16% of participants reported perceiving greater demands for digital security from private customers, 39% noted higher demands from public organizations, and 45% observed no

distinction between sectors. Additionally, 40% of participants expressed a need for financial assistance to support the implementation of cybersecurity measures, while 61% indicated a desire for training in cybersecurity. Only 7% of respondents stated that they did not require any support (see Table 4).

Cybersecurity preparedness: The frequency analysis presented in Fig. 6 reveals that 59% of tech SMEs employ a systematic approach to monitor their digital security. Among these organizations, 87.5% have conducted a risk analysis of their digital information, evaluating potential consequences in scenarios involving loss, theft, or unavailability. Furthermore, 91% of this subset have designated an individual responsible for overseeing the digital security of their products, solutions, and services, including the tools used in their development. Additionally, 89% have appointed IT security personnel tasked with managing internal processes such as communication, authentication, storage, encryption, GDPR compliance, and procedural protocols.

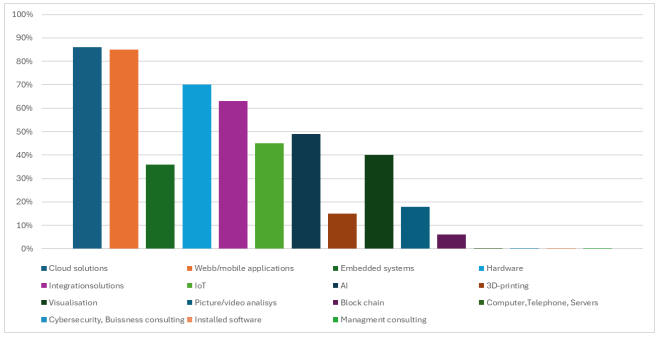


Figure 4: Techniques and technologies used by the organizations

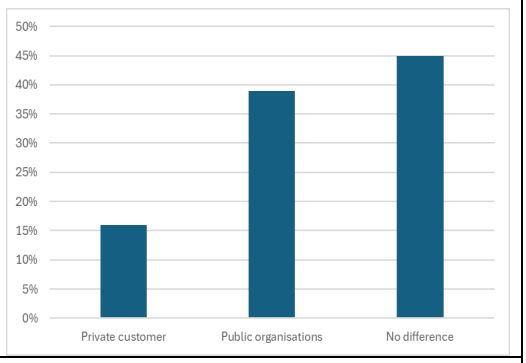


Figure 5: Sectors with the highest demand for digital security

Table 4: Organizations desired areas for support.

Suggestion	Yes	No
Inspiration and information through e.g. webinars	50%	50%
Network meetings & exchange of experiences	53%	47%
Training in security	61%	39%
Individual advice	41%	59%
Support in innovation, product or service development with specialist expertise	35%	65%
Financial support	40%	60%
Participate in joint development projects	43%	57%
Help with finding and attracting staff/skills	31%	69%
Help find the right suppliers who can help us move forward	30%	70%
No support needed	7%	93%

Among the organizations employing a systematic process, 59% actively adhere to it. Of these, 40% are officially certified according to ISO 27001:2022 or compliant with its regulations without formal certification, while 8% are in the process of obtaining certification. However, only 43% of these organizations have prepared to ensure compliance with current and upcoming legislation and regulations, including NIS 2 and CRA. Notably, 70% of all surveyed organizations reported encountering no obstacles in developing secure digital products or services.

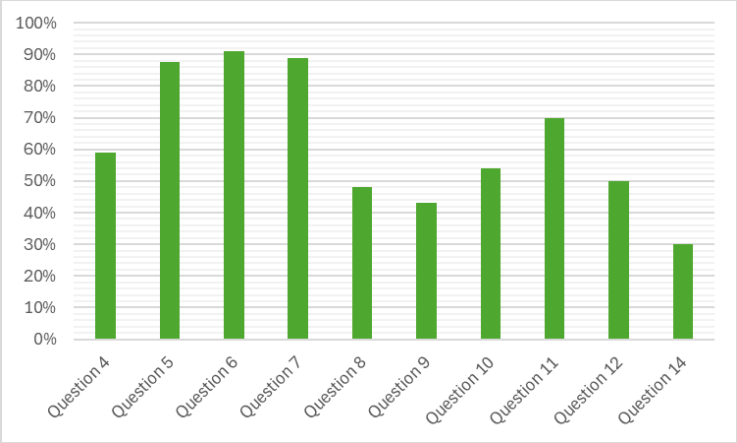


Figure 6: Frequency analysis for assessed binary factors

Approximately 54% of organizations impose digital security requirements on their subcontractors and partners, while 70% face market or client demands regarding the digital security standards of their products, solutions, and services. Additionally, about half of the organizations serve both private clients and public institutions. Multivariate analysis: Chi-square tests were performed for each assessed factor to quantify disparities between observed and expected values. While some differences were apparent without statistical testing, these tests provided additional support to the analysis.

Table 5: Chi-square test showing responses discrepancies regarding the assessed security factors

Question in Appendix 1	Category	Observed	Expected	$(O-E)^2/E$	Chi X^2-value	P-value	Critical value	Total sum
4	Yes	207	176.5	5.270538244	10.54107649	0.001167504	3.841	353
	No	146	176.5	5.270538244				
5	Yes	175	100	56.25	112.5	2.77665E-26	3.841	200
	No	25	100	56.25				
6	Yes	189	104	69.47115385	138.9423077	4.53433E-32	3.841	208
	No	19	104	69.47115385				
7	Yes	187	105	64.03809524	128.0761905	1.08016E-29	3.841	210
	No	23	105	64.03809524				
8	Yes	92	96.5	0,20984456	0,419689119	0,517092209	3,841	193
	No	101	96.5	0,20984456				
9	Yes	77	90.5	2.013812155	4.027624309	0.04476093	3.841	181
	No	104	90.5	2.013812155				
10	Yes	184	170	1.152941176	2.305882353	0.128885073	3.841	340
	No	156	170	1.152941176				
11	Yes	252	179.5	29.28272981	58.56545961	1.96638E-14	3.841	359
	No	107	179.5	29.28272981				
12	Yes	179	180	0.005555556	0.011111111	0.916051072	3.841	360
	No	181	180	0.005555556				
13	Private customer	27	58	16.56896552	168.8753388	2.13396E-37	5.991	174
	Public organisations	68	58	1.724137931				
	No difference	79	58	7.603448276				
14	Yes	0	123	123	246	1.93421E-55	3.841	246
	No	246	123	123				

The critical value varied based on the degrees of freedom (DF) associated with each factor. Notably, 72% of the tests conducted yielded a chi-square value exceeding the critical threshold, as shown in Table 5. When the chi-square value surpasses the critical value, the null hypothesis is rejected, indicating a significant difference between observed and expected values. This result signifies a departure from the expected distribution, demonstrating statistically significant discrepancies between groups. However, in 27% of the tests, the observed chi-square value was below the critical value (Table 5), meaning the differences between observed and expected values were not statistically significant. In these cases, the null hypothesis could not be rejected, indicating insufficient evidence to support a significant difference between the groups.

6. Conclusion and Future Work

This study surveyed Swedish tech SMEs to assess their cybersecurity readiness, focusing on security practices, challenges, investment factors, and compliance with standards, revealing that prioritization of technologies like

cloud solutions, web applications, and embedded systems often overshadows cybersecurity, introducing challenges such as limited knowledge, financial constraints, and ambiguity in standards implementation, with knowledge gaps being the most critical. Many SMEs perceive cybersecurity as a cost, with 55% noting stricter public sector demands, 40% complying with ISO 27001, and 21% preparing for NIS2 and CRA, yet most lack internal policies due to insufficient expertise and investment, highlighting the need for support like enhanced training, financial resources, and expertise to strengthen frameworks and reduce vulnerabilities. Growing demand for baseline cybersecurity measures from subcontractors reflects rising awareness, though the survey's 15.4% response rate was limited by privacy concerns, varying respondent knowledge, and industry differences, emphasizing clearer survey design. Future research should expand to diverse regions and industries in Sweden, address "don't know" responses, and incorporate cybersecurity knowledge and investment insights for a comprehensive analysis of SME practices.

Acknowledgement

We would like thank Ola Stensby at Lindholmen Science Park for providing us with the opportunity to conduct this study and guiding us along the way.

References

Armenia, S., Angelini, M., Nonino, F., Palombi, G. and Schlitzer, M.F., 2021. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems, 147, p.113580.

Basheer Ullahi, S.I.N., 2022. Developing cyber security strategies for business organization to prevent data breaches. KASBIT Business Journal, 15(4), pp.71–88.

Bayraktar, M.A., 2019. The importance of SMEs on world economies.

Cartwright, E.C. and Edunc, E.S., 2023. Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. Computers & Security, 131.

Carías, J.F., Borges, M.R.S., Labaka, L., Arrizabalaga, S. and Hernantes, J., 2020. Systematic approach to cyber resilience operationalization in SMEs. IEEE Access.

Certifiering.nu, 2024. Ackumulerat antal utfärdade certifieringar. [online] Certifiering.nu.[Accessed 1 July 2024].

Chidukwani, A., Zander, S. and Koutsakis, P., 2022. A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access, 10, pp.85701–85719.

Djebbar, F. and Nordström, K., 2023. A comparative analysis of industrial cybersecurity standards. IEEE Access, 11, pp.85315–85332.

ENISA, 2016. Information security and privacy standards for SMEs. [online].[Accessed 1 July 2024].

ENISA, 2021. Cybersecurity for SMEs - challenges and recommendations. [online] ENISA. [Accessed 1 July 2024].

European Commission, 2003. SME definition. [online] European Commission. [Accessed 23 June 2024].

European Union, 2022. SMEs and cybercrime.

Falch, M., Olesen, H., Skouby, K., Tadayoni, R. and Williams, I., 2023. Cybersecurity strategies for SMEs in the Nordic Baltic region. Journal of Cyber Security and Mobility.

Fernandez de Arroyabe, J.C., Arroyabe, M.F. and Bal, S., 2023. Cybersecurity resilience in SMEs: A machine learning approach. Journal of Computer Information Systems.

Freitas, M.d.C., 2018. GDPR compliance in SMEs: There is much to be done. Journal of Information Systems Engineering & Management, 3(4), p.30.

ISACA, 2021. Surge in ransomware and 10 biggest attacks in 2021. [online] ISACA. [Accessed 1 July 2024].

ISO/IEC, 2022. Information security management systems. [online]. [Accessed 1 July 2024].

Järvinen, H. and Shojaifar, A., 2020. Classifying SMEs for approaching cybersecurity competence and awareness.

Kappe, M., Härting, R.-C., Karg, C. and Deffner, D., 2023. Cybersecurity in SMEs – drivers of cybercrime, insufficient equipment and prevention. Procedia Computer Science, 225, pp.3631–3640.

Lloyd, G., 2020. The business benefits of cyber security for SMEs. Elsevier. [online].[Accessed 10 June 2024].

NIST, 2024. The CSF 1.1 five functions. [online] Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [Accessed 23 January 2025].

Park, L.S., n.d. Lindholmen Science Park. [online] Available at: https://www.lindholmen.se/sv [Accessed 23 December 2024].

Pedroso, L.M., Araújo, V.M., Cota, M.P. and Magalhães, J.P., 2021. How can GDPR fines help SMEs ensure the privacy and protection of processed personal data. [online], pp.1–6.

Ponemon Institute, 2018. State of cybersecurity in small and medium size businesses.

Ponsard, J.G. and Bal, S., 2019. Survey and lessons learned on raising SME awareness about cybersecurity.

StandICT, n.d. Building the expert network to reinforce Europe's role in global standards-setting. [online] Available at: https://standict.eu/ [Accessed 23 January 2025].

SMESEC, n.d. A lightweight cybersecurity framework for thorough protection. [online] Available at: https://www.smesec.eu/ [Accessed 10 December 2024].

Sweden ICT, n.d. Sweden Secure Tech Hub. [online] Available at: https://www.swedenict.se/sweden_secure_tech_hub/ [Accessed 23 December 2024].

The Swedish Agency for Economic and Regional Growth, 2020. Information Security Report 0339: The Ability of Small and Medium-Sized Enterprises to Digitalize and Grow in a World Where Information and Cybersecurity Are Becoming Increasingly Important. [online] SAERG. [Accessed 1 December 2024].

The Swedish Agency for Economic and Regional Growth, 2021. Number of companies in different industries, 2006–2021. [online] SAERG. [Accessed 1 December 2024].