

Assessing Cybersecurity Readiness Among SME

Bjarne Lill¹^a, Clemens Sauerwein¹^b, Alexander Zeisler²^c, Carina Hochstrasser³^d
and Nico Mexis⁴^e

¹Department of Computer Science, University of Innsbruck, ICT Building, Technikerstraße 21a, Austria

²Salzburg University of Applied Sciences, Urstein Süd 1, 5412 Puch/Salzburg, Austria

³University of Applied Sciences Upper Austria, Campus Steyr, Logistikum

⁴Faculty of Computer Science and Mathematics, University of Passau, 94032 Passau, Germany

Keywords: Information Security, Cybersecurity, Small and Medium-Sized Enterprise, SME, Workshop.


Abstract: Information security is a critical issue for small and medium-sized enterprises (SMEs) around the world. These organisations face an increasing number of security incidents and the sophistication of attacks. In order to remain competitive and protect their and their customers' critical information, it is essential that SMEs can manage their cybersecurity risks appropriately. Accordingly, it is important that these SMEs can rely on tailored information security assessments and frameworks. However, there is a scarcity of knowledge regarding their specific needs and the practical implementation of cybersecurity within these organisations. To address this knowledge gap, an exploratory study was conducted on the SME cybersecurity situation, with a particular focus on the implementation level of cybersecurity controls within SMEs in Austria and Germany. We surveyed 30 SMEs regarding their cybersecurity implementation situation in 2023. Our findings show, among other things, a very heterogeneous picture regarding the implementation level of cybersecurity controls and outline areas for action.


1 INTRODUCTION


Information security is a much-discussed topic in today's world, where the number and sophistication of security incidents and breaches are constantly increasing (Markakis et al., 2019; World Economic Forum, 2024; European Union Agency for Cybersecurity, ENISA, 2023). Small and medium-sized enterprises in particular are vulnerable due to their often limited resources and knowledge in this area (Markakis et al., 2019; Pawar and Palivela, 2022). SMEs can suffer serious consequences, including complete bankruptcy, following a successful information security attack (National Institute of Standards and Technology, U.S. Department of Commerce, 2016; Rodríguez-Corzo et al., 2018a). Their vulnerability and often low level of information secu-


urity can make them a tempting target (Sukumar et al., 2023; Chidukwani et al., 2022; Pawar and Palivela, 2022). Coupled with their large number and importance to the global economy (SMEs account for around 90% of businesses worldwide (World Bank Group, nd)), information security in SMEs is an important issue. This is reflected in various regulatory directives to strengthen the information security of SMEs, such as the NIS2 Directive (European Commission, 2023b) and the European Cyber Resilience Act (European Commission, 2023a). These aim at increasing the overall information security level within the economy.


In this context, the information security level of SMEs is therefore an important area to investigate in order to determine the current preparedness of companies. Knowledge about their information security, risk management and threat assessment to mitigate security threats is vital to determining the overall status, uncovering weaknesses and providing tailored support to these small and medium-sized enterprises. We herein define SMEs as companies with between 1 and 249 employees and turnover of up to 50 mil-

^a <https://orcid.org/0009-0008-7884-3100>

^b <https://orcid.org/0009-0009-9464-5080>

^c <https://orcid.org/0000-0002-5480-9521>

^d <https://orcid.org/0000-0003-3655-1376>

^e <https://orcid.org/0000-0003-0181-7648>

lion per year, based on the European Commission's definition (European Commission, 2020). The need for more and targeted research into information security in SMEs has also been echoed by the academic community (Melnik et al., 2022; Wilson et al., 2023; Sukumar et al., 2023; Pawar and Palivela, 2022; Chidukwani et al., 2022).

To address this issue and provide a foundation for future research, this paper examines the preparedness of SME in context of information security threats and risk management based on their basic information security controls. In doing so, we focus on the following three research questions: (RQ1) *What is the level of implementation of security controls within SMEs?*, (RQ2) *Which security controls are prioritised in SMEs?* and (RQ3) *Which security controls have a lower priority in SMEs?*.

To answer these research questions, we conducted an exploratory focus group discussion in the form of three workshops in Austria and Germany with 90 participants to determine which security controls are important and at what level of implementation they currently exist within SMEs. The workshops were held in German and lasted approximately 3 hours each. To this end, we used the well-established CIS Controls version 8 (Center for Internet Security, 2021) standard to suggest SME security controls within our workshop questionnaire. This way, we obtained 30 complete datasets from SMEs for analysis. Our findings show that the level of implementation of cybersecurity controls within SMEs is still very heterogeneous and that further action is needed to strengthen the cybersecurity of SMEs.

The remainder of this paper is structured as follows: In Section 2, we discuss related work on information security in SMEs and, in particular, surveys in this area. In Section 3, we outline the focus group research and the planning and execution of the survey. In Section 4, we present the results of our workshops and analyse and discuss them in relation to our research questions. Finally, in Section 5, we conclude our work and provide an outlook for future research.

2 RELATED WORK

While research on information security in the context of small and medium-sized enterprises has recently progressed in areas such as risk management (Virglerova et al., 2022; Sukumar et al., 2023; Zhang et al., 2020; Mantas et al., 2021) and security awareness (Georgsen and Kjøien, 2022; Lejaka et al., 2019; Chaudhary et al., 2022; Mayer and Volkamer, 2018; Wong et al., 2022; Uchendu et al., 2021; Rodríguez-

Corzo et al., 2018b). While there have been practical surveys in this area recently (Rae and Patel, 2020; Bisma et al., 2021; Aigbefo et al., 2022; Wilson et al., 2023; Heidenreich et al., 2022; Ncubukezi et al., 2020; Ahmed et al., 2020; Ncubukezi et al., 2020; Pawar and Palivela, 2022), these have not had the focus of practical implementation of security controls within SME. Rather, the focus for researchers seems to be surveys related to security behaviour and intentions regarding information security (Rae and Patel, 2020; Bisma et al., 2021; Aigbefo et al., 2022). A second area are studies investigating information security priorities, risks and threats (Wilson et al., 2023; Heidenreich et al., 2022; Ncubukezi et al., 2020). Further, a number of studies about related topics have been discovered. Ahmed et al.'s study (Ahmed et al., 2020) investigates the impact of virtualization within SMEs on their information security based on a set of ITIL controls. Heidenreich et al. (Heidenreich et al., 2022) propose an IT security measurement method for micro-enterprises and Pawar & Palivela (Pawar and Palivela, 2022) explore security standard adoption and frequencies of security awareness trainings within SMEs.

While the aforementioned surveys investigate and cover areas such as the behavioral approach to SME information security as well as general attitude and threat perception, there seems to be a distinctive lack of practical research surveys regarding SME security controls and their implementation in general. Too the best of our knowledge, no scientific surveys have investigated the practical implementation levels of security controls within SMEs.

3 APPLIED RESEARCH METHODOLOGY

The focus group methodology coupled with a quantitative survey approach has been used to investigate the research objective. To this end, the steps summarised by Kontio et al. (Kontio et al., 2008) have been used as the orientation. They are as follows: (a) Planning the research (b) Designing focus groups (c) Conducting the focus group sessions and (d) Analyzing the data and reporting the results. An overview of the research methodology can be seen in Figure 1. In total, three focus group sessions (workshops) were held between April and June 2023. One was held in Vilshofen, Bavaria, one in Innsbruck, Tyrol and one was held online.

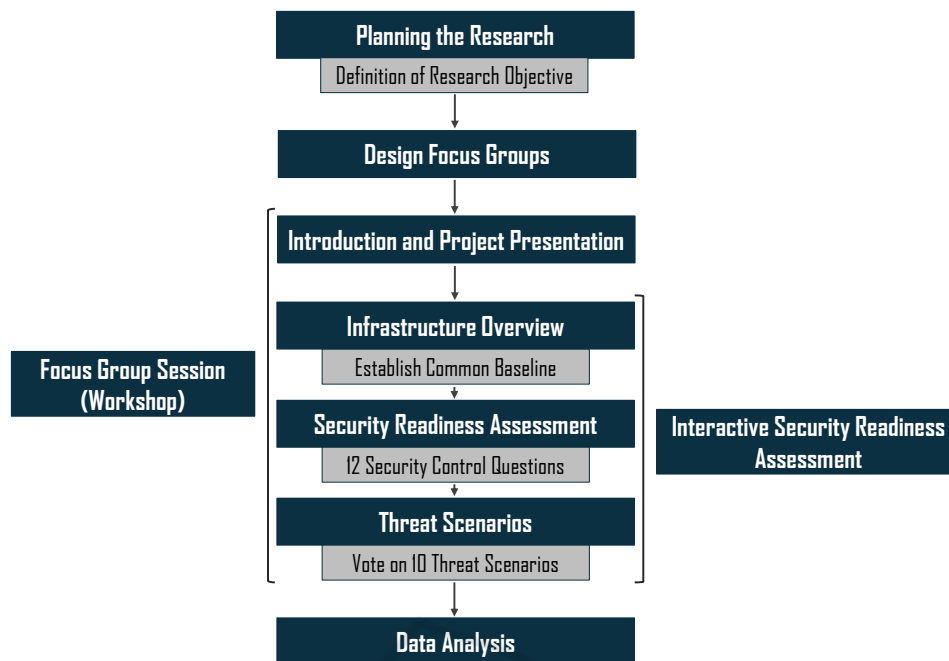


Figure 1: Research Methodology Overview.

3.1 Planning the Research

The research objective has been set based on discussion in the CySeReS-SME research group¹ as well as an extensive, systematic literature investigation on the topic. The research objective is to assess the cybersecurity readiness of SMEs in the DACH region, based on their use and implementation of security controls.

3.2 Design Focus Groups

Members for the focus groups in each workshop location (Bavaria, Tyrol and Online) have been recruited using social media posts, direct email contacting and public institutions (e.g. Chamber of Commerce Tirol²) as multipliers for the announcements to reach a large audience. The participation has been voluntary and free of charge. In order to recruit relevant participants each workshop title included the intended target group (people owning or employed in an SME) prominently. This way, the focus groups have been build based on participants signing up for the individual workshop sessions. Participants were asked to confirm their affiliation to an SME as part of the data collected during the workshops. Only responses from participating SMEs have been included in the research findings.

¹<https://cyseres-kmu.eu/>

²<https://www.wko.at/tirol>

3.3 Conducting the Focus Group Sessions

Each of the three focus group session has been hosted as a workshop in a different location. All workshops followed a systematic, similar structure and included a quantitative survey to capture the participants input. The general underlying concept of the workshops has been an interactive survey to allow the participating companies to partake. This enabled the direct review and discussion of live results during the workshops. Each session has been structured as follows: (a) *Introduction and Project Presentation*, (b) *Interactive Security Readiness Assessment* and finally (c) *Threat Scenarios*.

Introduction and Project Presentation - To start of each workshop, a short introductory section to introduce the project team, venue, agenda as well as the timeline has been given. This was followed by an introduction to the general topic of information security and the infrastructure and assets involved to consider when answering the questions posed in the interactive Security Readiness Assessment. The inclusion and discussion of this information ensured that all participants had the same understanding and level of knowledge to follow and answer the questions.

Interactive Security Readiness Assessment -

The interactive security readiness assessment presents the main part of the workshops. It has been structured into three areas: (1) *Infrastructure Overview* - here the participants received a short and concise overview of what information technology (IT), operational technology (OT) mostly production related, and supply chain infrastructure can look like in their companies. They were asked some general questions about their IT, OT and supply chain infrastructure as it relates to their business (e.g. *Does your company use digital technologies and networked systems to support internal processes, especially administrative processes?*). This has been done to supply all participants with a similar foundational overview of the topic, get them thinking about their companies infrastructure and therefore provide the basis to answer and discuss the questions in the next part. The questions have been designed as an interactive survey using the tool Mentimeter³. Mentimeter allows the workshop participants to access the survey and its questions using their mobile devices or laptops. They can respond to the questions in real time. The procedure in the workshop was to introduce and explain the question to the whole focus group, either gathered together in one of the workshop venues or in the online group session. Any ambiguities were clarified and the question was then put to a vote by the participants. After this overview of the infrastructure and what to consider for their own organisation, the workshop moved on to the security readiness assessment. (2) *Security Readiness Assessment* - This part includes the main questions to be answered by the participants. 12 questions regarding SME information security measures had to be answered. The questions are listed below. The survey questions regarding information security measures for SMEs have been systematically derived from the CIS controls V8.0 (Center for Internet Security, 2021) provided by the Center of Internet Security. The guideline has systematically been analyzed by two of the authors, relevant content for SMEs has been extracted and partly summarized to arrive at 12 concise survey questions. Each question can be answered with a 5 point likert scale regarding its implementation level in a company. The scale is defined as follows: Fully Implemented, Partially Implemented, Rather not Implemented, Not Implemented and Not Required. In this case, Partially Implemented and Rather Not Implemented differentiate the level of implementation and commitment to the area of the question. The category Partially Implemented suggests a higher level of commitment

to implementation and a possibly achieved level of implementation, while the category Rather Not Implemented implies a more rudimentary level of implementation, closer to the Not Implemented option. The questions are:

1. Are all of the company's sensitive/critical assets (hardware, software, databases) known and centrally listed, and are the records regularly updated?
2. Are hardware and software components in the company that are worth protecting configured with regard to their secure use?
3. Do you use policies and (automated) tools for authorisation management of user accounts, administrative access and service accounts with access to the company's sensitive infrastructure?
4. Does the company have organisational and/or technical measures in place to store, process and dispose of data in a controlled manner?
5. Do you make regular backups of your data? Do you have a procedure for restoring compromised data and systems and do you test it?
6. Do you regularly analyse vulnerabilities in your company's infrastructure and quickly eliminate new threats?
7. Do you prevent the installation and execution of malware within the company infrastructure?
8. Do you take measures to increase protection when using e-mail programs and web browsers?
9. Do you collect log information by default in the course of data processing and system usage?
10. Do you have a response plan for handling security incidents, including procedures, reporting processes and responsibilities?
11. Do you promote a basic knowledge and behavioral basis within the workforce on the subject of cybersecurity in order to sensitize them to the handling and potential dangers when dealing with information and systems?
12. Do you evaluate service providers before signing a contract and during the business relationship with regard to their security concepts and handling of confidential company data and systems?

To further structure the interactive survey, the questions have been distributed into 3 main categories. Question 1-5 belong to the main category Inventory and Safeguarding, 6-9 to Vulnerabilities and Prevention and the last three (10-12) to Culture and Organisation. Following the completion of each category during a workshop, the live results from

³<https://www.mentimeter.com/>

Mentimeter have been presented and discussed in the workshop group (focus group). (3) *Threat scenarios* - As a third step, the participants have been presented with 10 different, common threat scenarios derived from major governmental institutions (BSI⁴, NIST⁵) and asked to name their top 3 most critical. Each threat scenario has been briefly explained to provide a common understanding of each. The threat scenarios presented are: *Human Error and Sabotage, Infection with Malware via the Internet and Intranet, Social Engineering and Phishing, Access via Internet-connected Systems / Control Components, Infiltration of Malware via Removable Media / Mobile Systems, Software and Hardware Vulnerabilities in the Supply Chain, Technical Misconduct and Force Majeure, Intrusion via Remote Maintenance Access, Compromise of Extranet and Cloud Components and (Distributed) Denial of Service Attacks.*

3.4 Analyzing the Data and Reporting the Results

Following the completion of each workshop, the survey data has been exported from the Mentimeter tool and archived using Microsoft excel exports form Mentimeter. At the conclusion of the workshop series, the data has been consolidated, corrected and statistically analysed in Microsoft Excel based around their frequency distributions. The results are presented and discussed in the following chapters 4 & 5.

4 RESULTS & DISCUSSION

In this section, we present and discuss our findings based on our research questions (see Section 4.1 to 4.3) and discuss the limitations associated with our work (see Section 4.4).

Three workshops were held in 2023. The workshops were conducted in German. Table 1 shows the number of participants per workshop, the overall number of responses from each workshop and from SMEs in particular. Out of a total of 90 participants, 30 complete data sets were obtained from small and medium-sized enterprises. The remaining datasets were either incomplete or provided by organisations that exceeded the SME threshold and have been excluded from the analysis.

⁴<https://www.bsi.bund.de>

⁵<https://www.nist.gov/>

Table 2 provides further insights into the composition of the data set, namely the size and revenue of the surveyed SME population. It can be seen that the range of participating SMEs was very heterogeneous and spread across the entire inclusion range in terms of number of employees and turnover. The data set includes 9 SMEs with up to 9 employees, 9 small sized SMEs with up to 49 employees and 12 medium sized SMEs with up to 249 employees.

After data consolidation, including the removal of records from larger organisations and incomplete records, we based our analysis on these 30 complete records from SMEs. Our analytical design for the discussion was limited to the determination of frequencies, means and variances. We did not use inductive statistical methods such as significance tests as we did not take a random sample. The results of the analysis are presented and discussed below.

4.1 Implementation of Security Controls in SMEs

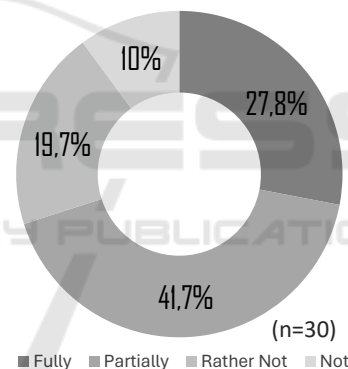


Figure 2: Implementation Categories Average Answers in Percent.

The distribution of mean scores per implementation category shown in Figure 2 gives an overall impression of how far the cluster of 30 SMEs surveyed during the workshop series have progressed in their information security. First of all, it is noticeable that the selection of security controls provided (in the form of the 12 questions) seems to meet the needs of SMEs, as only 0.8% of all company responses fell into the Not required category (not displayed in Figure 2). This means that at most one single company indicated that a particular security control question was not relevant in the context of their company, bringing the mean score of the Not Required category to 0.8%. According to the data acquired within our survey, the level of information security in SMEs is still uneven and very heterogeneous. While about 1/4 (27.7%)

Table 1: Participants & Data Samples.

	Participants	Complete Data Sets	SME Data Sets
Germany	24	14	12
Austria	14	3	3
Online	52	22	15
Σ	90	39	30

Table 2: SME Organisation Size and Revenue.

Size	Count
Up to 9 employees and revenue up to 2 million / year	9
Up to 49 employees and revenue up to 10 million / year	9
Up to 249 employees and revenue up to 50 million / year	12
Σ	30

of the responses confirmed that companies have fully implemented some of the security controls, the majority of responses (41.7%) are still within the partially implemented category. This indicates that organisations have started or are in the process of implementing the security controls, but are still on their way to achieving full implementation and therefore security benefits. Furthermore, when looking at the Rather Not Implemented and Not Implemented categories, which indicate that organisations have given little or no consideration to these security controls, it is clear that almost 1/3 (29.7%) of the responses fell into these combined categories. This highlights the need for future work in SME information security, as nearly 1/3 of the responses indicate that organisations have not considered some of the security controls.

4.2 Prioritising of Security Controls in SMEs

Figure 3 summarises our findings on the top performing security controls in terms of percentage of responses in the Fully Implemented category. The top four controls with 36.7% are Inventory of hardware, software and databases, Data backup and recovery, Malware protection measures and Cybersecurity culture and training. These four are closely followed by two other controls with just over 1/3 in the fully implemented category (33.3%): protection for email and web browsers and handling of security incidents. For all other security controls, the percentage of fully implemented ranged from 27% to as low as 10%. We have identified two main areas of controls, which seem to perform well in this regard. The human factor and rather technical security controls. Not surprisingly, cybersecurity culture and training received a lot of attention by companies and therefore a high score in the fully implemented area as well as the Par-

tially Implemented area (33,3%), as the human factor is considered one of the key aspects within SME information security (Pawar and Palivela, 2022; Chaudhary et al., 2022). This indicates that security training and culture efforts are being undertaken by nearly 70% of the companies surveyed, which we perceive as a sign of progress in the correct direction for SME information security. In addition, the handling of security incidents, which involves a lot of human interaction and awareness (in the form of incident reporting and clear responsibilities within the workforce as to who takes the lead in the event of an incident), appears to be an important issue for a large proportion of the organisations surveyed. Secondly, more technical controls such as data backup and recovery, malware protection and email and web browser protection appear to be a priority. Malware protection has also been stated as one of the most important controls by another security control survey conducted by Pawar et al. (Pawar and Palivela, 2022) in 2021.

4.3 Security Controls Less Prioritised in SMEs

On the flip side of the security controls that are performing well, we have also identified some areas of weaker performing controls within the SME population. These are summarised in Figure 4. Only 10%, or three companies, reported that they had fully implemented supplier and service provider management controls and were making good efforts in this area. However, over half of the companies surveyed (53.3%) indicated that they have Rather Not (33.3%) or Not (20%) taken effort to implement and manage this area. This is an alarming result, given that the supply chain in general and SMEs in particular are seen as vulnerabilities within it (Melnik et al., 2022; Georgsen and Kjøien, 2022). This is in line with the

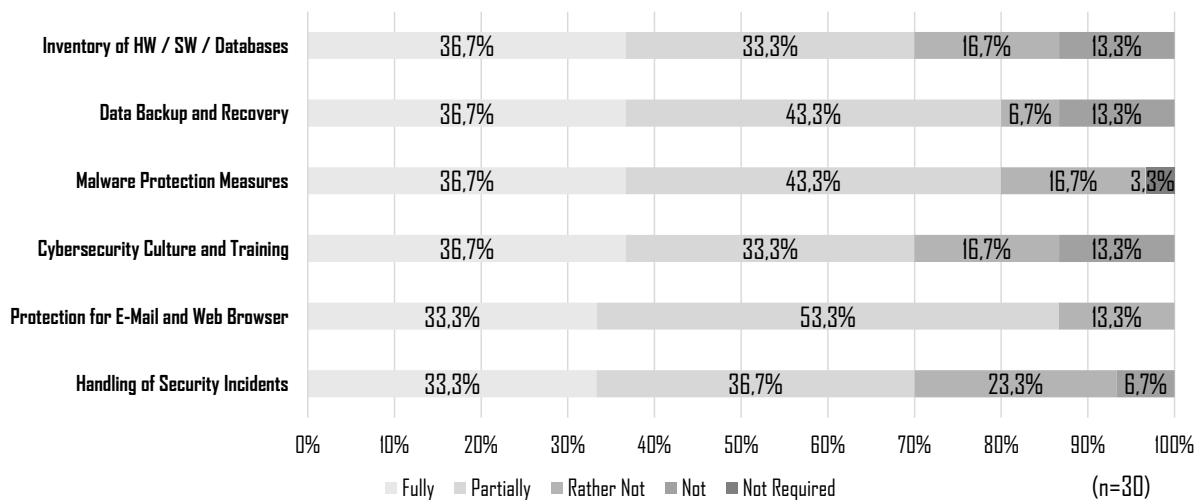


Figure 3: Highest Percentage Controls in the "Fully Implemented" Category.

call for further research and efforts in this area as called for in the academic community (Melnik et al., 2022; Durowoju et al., 2020). The next two controls which have received weak results are Set Up and Configuration of Log files and Regularly Analyse and Address Weak Points with 46,7% and 40% respectively in the combined categories of Rather Not and Not implemented, which clearly indicate, that companies have not taken sufficient efforts in these areas. The last 4 security controls shown in the figure 4 highlight a predicament identified in this research survey, as they contain three controls that have already been discussed with regard to their high scores in the Fully Implemented category (view Section 4.2). However, these three controls - Inventory of hardware/software and databases, Cybersecurity culture and Training and handling of security incidents - also received almost a third of responses (30%) within the combined categories of Rather Not Implemented and Not Implemented. This highlights the conflict that while some companies seem to prioritise these controls highly, nearly 1/3 seem to prioritise little to no effort in these areas. This is a worrying precedent, as in particular the handling of security incidents and the associated clarification of responsibilities in the event of an incident, as well as cybersecurity culture and training, are directly related to strengthening the response and awareness of the workforce regarding its information security posture. And in particular, the information security posture of the human workforce is consistently highlighted as the weakest link when it comes to information security threats, whether in the form of an insider threat or simply a lack of awareness (Pawar and Palivela, 2022; Chaudhary et al., 2022; de Bruijn and Janssen, 2017). The importance of the human workforce and their information security posture has

further been confirmed by the surveyed audience of the workshops themselves. They rated three threats highly related to the human workforce the highest out of the 10 presented threats for voting. These are Human Error and Sabotage in the top spot, Infection with malware via the Internet and Intranet in second and Social Engineering and Phishing third. These all target the human workforce in particular. The voting results for the top threats as perceived by SMEs are summarised in Figure 5.

Finally, it is surprising that the security control of inventorying hardware/software and databases received such low scores, with almost a third of companies stating that they have made little or no effort to inventory their critical corporate assets, as awareness and control of corporate assets is important to most, if not all, information security efforts within an organisation.

4.4 Limitations

The presented research may be limited by (i) low sample size, (ii) selection bias of participants, and (iii) authors selection bias. (i) The low sample size in our study can be explained by the difficulties in attracting and motivating SMEs, in particular, to attend and participate in cybersecurity activities (Wilson et al., 2023). To address this, we worked with public organisations such as the Austrian Chamber of Commerce Tirol⁶, Bayern Innovativ⁷ and Business Upper Austria⁸ to multiply the audience for our research. In addition, we enabled companies to provide well in-

⁶<https://www.wko.at/tirol>

⁷<https://www.bayern-innovativ.de/de>

⁸<https://www.biz-up.at/>

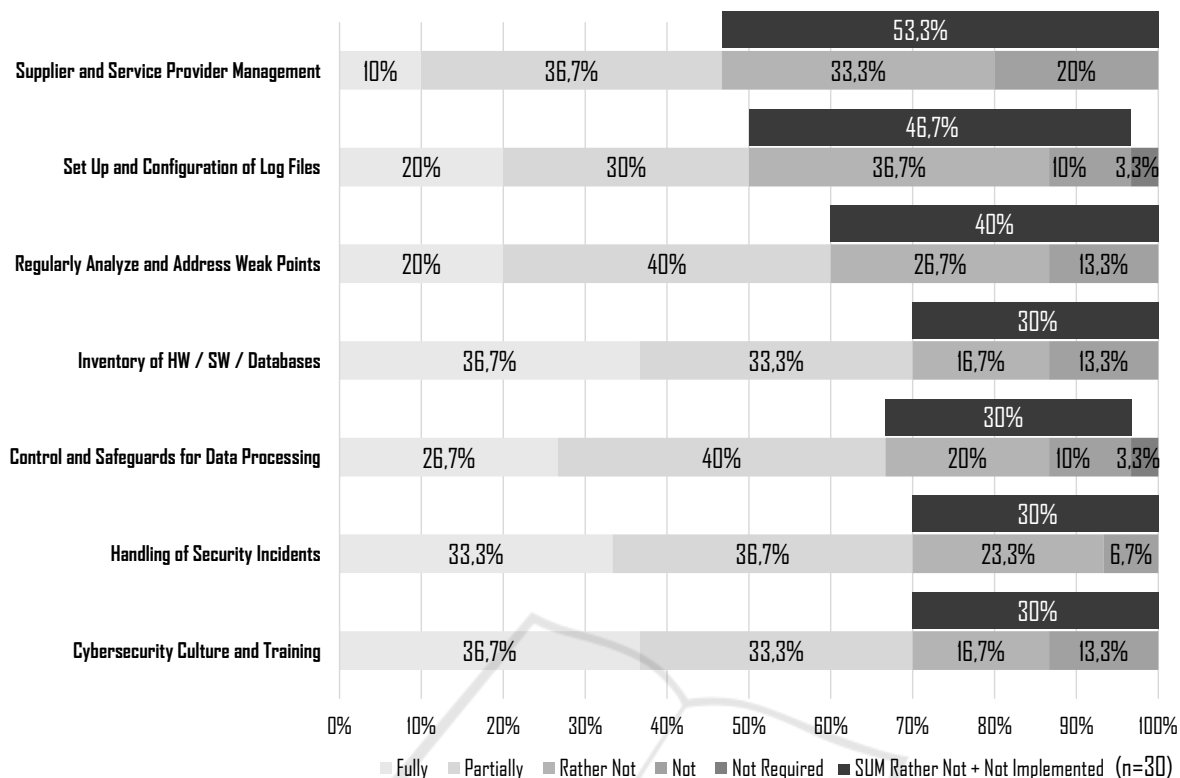


Figure 4: Weak Performing Controls (SUM of Rather Not and Not Implemented).

formed answers to the survey questions by providing an information summary in advance to each question and feedback on ambiguities during the workshop surveys. This way, we ensured that responses were not random and have been made as informed as possible. (ii) To counter selection bias of participants, we contacted a wide range of companies and used specialised organisations known for working with SMEs as multipliers for our invitations to the workshops to ensure the most relevant data samples. We thereby did not take a random sample. (iii) Our publication and methodology could be limited by author selection bias regarding the information provided, the security controls selected, and other elements of our research. To counter this, we reviewed and collaborated with at least two authors and usually the entire CySeReS-KMU project research team on each component and methodology of the focus group research. This way, we ensured that at minimum two people were involved in each design decision.

5 CONCLUSION

In this paper, we present an exploratory practical study of the overall level of information security

implementation within 30 small and medium-sized enterprises, using an integrated focus group research approach accompanied by a quantitative survey. In doing so, we identified the security controls that perform best in terms of achieving the full implementation level, as well as the flip side by highlighting information security control areas that still seem to lack the appropriate attention and effort. We further uncovered a predicament in that many of the well-performing information security controls have a fairly large proportion of companies that still appear to be neglecting them. This leads us to believe that the information security landscape of SMEs and the posture of individual companies appears to vary widely from security control to security control, and therefore from company to company. Summarising the best and worst performing security controls has led to the discovery of some important areas of strength, and in some cases weakness, in the overall information security posture of SMEs. The top three overall performing controls are: Data backup and recovery, malware protection measures, and email and web browser protection, followed by the three predicament controls. These appear to be prioritised by over a third of the SMEs surveyed, but at the same time neglected by almost another third of the SME

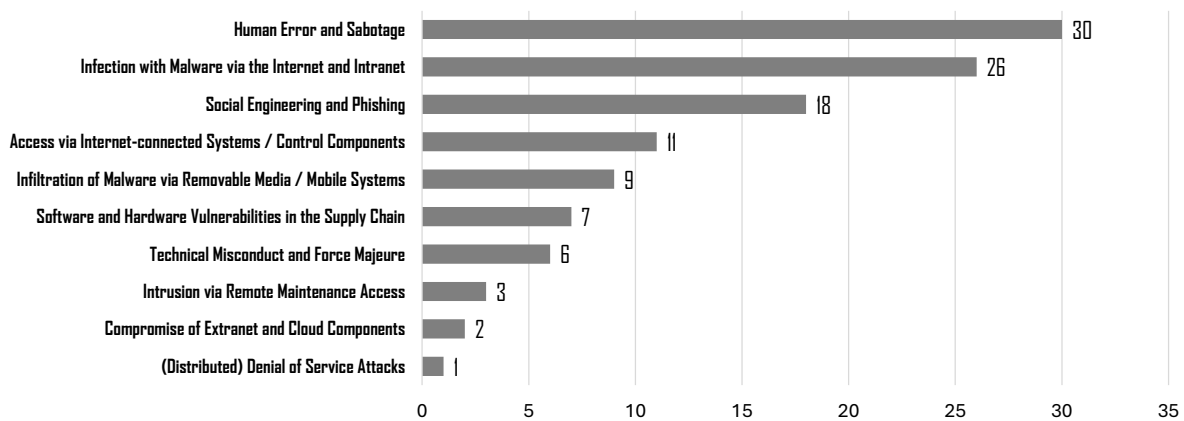


Figure 5: Number of Votes for Security Threats.

population. These controls are Inventory of hardware / software and databases, Cybersecurity culture and training and handling of security incidents. Finally, there are three security controls that between 40% and over 50% of companies do not seem to prioritise very highly, while at the same time stating that they do not consider them unnecessary for their business. These are: Supplier and service provider management, log file setup and configuration, and regularly analyse and address Weak Points. From these observations, we conclude that while efforts are clearly being made to strengthen information security in SMEs, there is still a significant need for further efforts by companies and future research in the academic community.

We therefore advocate for future research efforts in the following areas based on the outcome of our survey:

- (1) Supply chain management clearly needs to be studied in terms of its place and application within SMEs, as more than half of the SMEs surveyed did not implement this control adequately.
- (2) The use of log files as an information security control within SMEs should be evaluated on the basis of whether it is a value adding and practical security measure for companies of this size.
- (3) The information security processes and posture of SMEs in general should be examined and strengthened by appropriate frameworks and processes, as many process and personnel reliant information security areas, such as regular vulnerability analysis, inventory as one of the main foundations to establish and coordinate information security efforts within an organisation, and handling of security incidents, seem to be areas where a large proportion of SMEs are lacking. Especially the lack of a proper inventory

and therefore assessment of assets which might be critical to the company regarding its information security, should also be investigated.

(4) This extends to cybersecurity culture and training, which were identified as both performing well for some companies and neglected by others, while it was clearly identified both within literature (Pawar and Palivela, 2022; Chaudhary et al., 2022) and the threat assessment survey conducted within the workshops that human resources are one of the most important factors and threats in SME information security. Without adequately trained and aware personnel, any technical and procedural security control imposed by the company can be overridden by human error or misapplication.

(5) Finally, our call for more general and comprehensive research is driven by the fact that no security control significantly exceeded the margin of 1/3 of companies reaching full implementation, meaning that almost 2/3 of the surveyed companies are either in some stage of implementation or have completely neglected them. This suggests that organisations need further guidance on how to achieve an overall information security posture to strengthen their defences.

In conclusion, our findings clearly outline that the SME information security landscape is evolving, but still requires a great deal of work and research to achieve an adequate level of protection against the ever-increasing information security threats. Our study provides valuable information about the information security situation in SMEs, highlights key areas for future work, and serves as a guide for researchers and organisations alike as they navigate the field of SME information security.

ACKNOWLEDGEMENTS

This work is co-funded by the European Union through INTERREG VI-A Germany/Bavaria–Austria 2021–2027 – INTERREG VI-A Bayern–Österreich 2021–2027, as part of the Project “CySeReS-KMU: Cyber Security and Resilience in Supply Chains with focus on SMEs” (project number BA0100016).

REFERENCES

- Ahmed, F., Burney, A., and Malik, A. (2020). Security aspects of virtualization and its impact on business information security. In *2020 International Conference on Information Science and Communication Technology (ICISCT)*, pages 1–9. IEEE.
- Aigbefo, Q. A., Blount, Y., and Marrone, M. (2022). The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 41(6):1151–1170.
- Bisma, R., Winarto, S. R., and Puspita, Y. C. (2021). Investigating cyber security factors influencing the perception behavioral intention of small and medium enterprise. In *2021 Fourth International Conference on Vocational Education and Electrical Engineering (ICVEE)*, pages 1–7. IEEE.
- Center for Internet Security (2021). *Cis critical security controls v8*.
- Chaudhary, S., Gkioulos, V., and Goodman, D. (2022). cybersecurity awareness for small and medium-sized enterprises (smes): availability and scope of free and inexpensive awareness resources. In *European Symposium on Research in Computer Security*, pages 97–115. Springer.
- 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*, 10:85701–85719.
- de Bruijn, H. and Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1):1–7.
- Durowoju, O., Chan, H. K., and Wang, X. (2020). Investigation of the effect of e-platform information security breaches: a small and medium enterprise supply chain perspective. *IEEE Transactions on Engineering Management*, 69(6):3694–3709.
- European Commission (2020). *User guide to the sme definition*.
- European Commission (2023a). *Cyber resilience act*.
- European Commission (2023b). *Directive on measures for a high common level of cybersecurity across the union (nis2 directive)*.
- European Union Agency for Cybersecurity, ENISA (2023). *Enisa threat landscape 2023*.
- Georgsen, R. and Kjøien, G. M. (2022). Serious games with sysml: Gamifying threat modelling in a small business setting. In *INCOSE International Symposium*, volume 32, pages 119–132. Wiley Online Library.
- Heidenreich, M., Franczyk, B., and Johannsen, A. (2022). Evaluation study of an it security measurement method for micro-enterprises. In *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pages 1–7. IEEE.
- Kontio, J., Bragge, J., and Lehtola, L. (2008). The focus group method as an empirical tool in software engineering. In *Guide to advanced empirical software engineering*, pages 93–116. Springer.
- Lejaka, T. K., Da Veiga, A., and Looock, M. (2019). Cyber security awareness for small, medium and micro enterprises (smmes) in south africa. In *2019 Conference on Information Communications Technology and Society (ICTAS)*, pages 1–6. IEEE.
- Mantas, E., Papadopoulos, D., Fernández, C., Ortiz, N., Compastíe, M., Martínez, A. L., Pérez, M. G., Kourtis, A., Xylouris, G., Mlakar, I., et al. (2021). Practical autonomous cyberhealth for resilient micro, small and medium-sized enterprises. In *2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, pages 500–505. IEEE.
- Markakis, E., Nikoloudakis, Y., Mastorakis, G., Mavroumoustakis, C. X., Pallis, E., Sideris, A., Zotos, N., Antic, J., Cernivec, A., Fejzic, D., et al. (2019). Acceleration at the edge for supporting smes security: The fortika paradigm. *IEEE Communications Magazine*, 57(2):41–47.
- Mayer, P. and Volkamer, M. (2018). Addressing misconceptions about password security effectively. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, pages 16–27.
- Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., and Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, 60(1):162–183.
- National Institute of Standards and Technology, U.S. Department of Commerce (2016). *Small business information security: The fundamentals – nistir 7621 revision 1*.
- Ncubukezi, T., Mwansa, L., and Rocaries, F. (2020). A review of the current cyber hygiene in small and medium-sized businesses. In *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 1–6. IEEE.
- Pawar, S. and Palivela, H. (2022). Lcci: A framework for least cybersecurity controls to be implemented for small and medium enterprises (smes). *International Journal of Information Management Data Insights*, 2(1):100080.
- Rae, A. and Patel, A. (2020). Developing a security behavioural assessment approach for cyber rating uk msbs. In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–8. IEEE.
- Rodríguez-Corzo, J. A., Rojas, A. E., and Mejía-Moncayo, C. (2018a). Methodological model based on gophish to face phishing vulnerabilities in sme. In *2018 ICAI Workshops (ICAIW)*, pages 1–6. IEEE.

- Rodríguez-Corzo, J. A., Rojas, A. E., and Mejía-Moncayo, C. (2018b). Methodological model based on gophish to face phishing vulnerabilities in sme. In *2018 ICAI Workshops (ICAIW)*, pages 1–6. IEEE.
- Sukumar, A., Mahdiraji, H. A., and Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*.
- Uchendu, B., Nurse, J. R., Bada, M., and Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109:102387.
- Virglerova, Z., Panic, M., Voza, D., and Velickovic, M. (2022). Model of business risks and their impact on operational performance of smes. *Economic research-Ekonomska istraživanja*, 35(1):4047–4064.
- Wilson, M., McDonald, S., Button, D., and McGarry, K. (2023). It won't happen to me: Surveying sme attitudes to cyber-security. *Journal of Computer Information Systems*, 63(2):397–409.
- Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., and Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66:102520.
- World Bank Group (n.d.). Small and medium enterprises (smes) finance – improving smes' access to finance and finding innovative solutions to unlock sources of capital. Accessed on: 02/05/2024.
- World Economic Forum (2024). Global cybersecurity outlook 2024 – insight report.
- Zhang, X., Xie, H., Yang, H., Shao, H., and Zhu, M. (2020). A general framework to understand vulnerabilities in information systems. *IEEE Access*, 8:121858–121873.