A Comprehensive Review of Information Security Research regarding SMEs and Future Directions

Bjarne Lill[1,*], Clemens Sauerwein[1], Nico Mexis[2] and Karoline Langner[3]

[1]*Department of Computer Science, University of Innsbruck, ICT Building, Technikerstraße 21a, Innsbruck, A-6020, Austria*
[2]*Faculty of Computer Science and Mathematics, University of Passau, Innstraße 41, Passau, D-94032, Germany*
[3]*University of Applied Sciences Upper Austria, Campus Steyr, Logistikum, Wehrgrabengasse 1-3, Steyr, A-4400, Austria*
E-mail: Bjarne.Lill@uibk.ac.at; Clemens.Sauerwein@uibk.ac.at; nico.mexis@uni-passau.de; karoline.langner@fh-steyr.at
[*]*Corresponding Author*

Received 29 November 2024; Accepted 17 October 2025

Abstract

Information security is a critical concern for small and medium-sized enterprises (SMEs) in today's world. The increasing number of security incidents and their growing complexity and sophistication pose a serious threat to SMEs. They need to be able to understand information security risks and rely on tailored solutions and frameworks to establish an appropriate information security posture. In order to provide targeted assistance to these organisations in their security efforts, it is important to identify the areas of research that have already been considered in this context and highlight important avenues for future research open to the academic community. To address this challenge, the research objective of this publication is to provide a fundamental overview of the existing research in SME information security and the future

Journal of Cyber Security and Mobility, Vol. 14_5, 1245–1288.
doi: 10.13052/jcsm2245-1439.1459
© 2025 River Publishers

work that is yet to be done. In doing so, we aim to establish a baseline to guide future research in this area. We pursued this research objective by conducting a multi-vocal, systematic literature review within seven scientific databases and further consider grey literature on the topic. A total of 112 scientific publications and 16 grey literature sources were clustered to provide an adequate overview of existing research in SME information security. Furthermore, the publications have been reviewed for their implications for future directions of research. In doing so, we have provided an overview of research in the field of SME information security and provided the academic community with open research gaps to consider for future research efforts.

Keywords: Information security, cybersecurity, small and medium-sized enterprise, SME, MVLR, literature review, clustering, research gap.

1 Introduction

Information security is a widely discussed topic in today's world. The ever-increasing number of security incidents and breaches poses a serious threat to organisations and the economy as a whole. Security incidents are becoming increasingly sophisticated and complex [57, 86, 142]. This presents a serious problem, especially for small and medium-sized enterprises (SMEs), which often have limited resources and knowledge to build a strong information security posture [86, 103]. And yet they are often hit the hardest by a successful information security attack, as the consequences for these organisations can be as severe as complete bankruptcy [98, 111]. This vulnerability, coupled with their often weaker information security posture, makes them easy targets for attack [35, 103, 122]. This presents a problem for the global economy and SMEs themselves, as they account for approximately 90% of worldwide businesses [141]. We herein define SMEs as companies with between 1 and 249 employees and a turnover of up to EUR 50 million per year or a balance sheet total of up to EUR 43 million per year, based on the European Commission's definition [51]. As such, their information security represents a key challenge, as they play an important role in the global economy. The importance of this issue is underscored by various regulatory frameworks aimed at strengthening the information security of SMEs, such as the NIS2 Directive [53], the European Cyber Resilience Act [52], and the US Government's Executive Order 14028 on Improving the Nation's Cybersecurity [40]. These frameworks aim to improve the overall level of information security across the economic landscape. In order to address this

challenge, targeted research and solutions tailored to the needs of these small and medium-sized enterprises are needed to provide them with the knowledge and tools to build a strong information security posture and, by extension, strengthen the information security resilience of the global economy as a whole [35, 90, 103, 122, 139].

It is important to understand what information and research is available to SMEs today and what challenges remain for the future. In this context, it is crucial to comprehend the extent and sophistication of academic research on SME information security. Accordingly, the research objective for this publication is to establish a systematic overview of the body of knowledge in the field of information security of SMEs and outline implications for future research. This involves a comprehensive review and analysis of the existing academic knowledge base in the form of scientific literature and selected grey literature to provide an overview of existing research and implications for future research. To address the research objective, we conducted a multivocal literature review (MVLR) of scientific and selected grey literature on SME information security. We considered literature from seven leading academic databases and grey literature results from an extensive search engine query. We reviewed 317 academic sources and 25 grey literature documents. We further clustered the remaining 112 academic publications and 16 grey literature documents thematically to identify the most prominent areas of current research. In addition, we analysed and clustered the future research pathways suggested by the 112 scientific publications and presented them in a comprehensive and structured manner. Our findings include a comprehensive overview of the thematic structure and main research areas of SME information security research, as well as an overview of the most requested paths for future research in this area. In this way, we provide guidance on research to date and highlight open areas for future work for the research community.

The remainder of this publication is structured as follows: In Section 2, we discuss related work in the area of information security in small and medium-sized enterprises. In Section 3, we present our multivocal literature review methodology and our systematic approach to this comprehensive literature review. In Section 4, we present our results regarding the scientific literature, its general tendencies and its main thematic areas. The same is done for the grey literature in Section 5. We then present our results on the future work analysis in Section 6 and discuss these. We conclude our work with a short summary and outlook in Section 7.

2 Related Work

While there are some existing surveys in the area of information security in small and medium-sized enterprises in the direction of reviewing the existing literature [4, 35, 123], these studies do not go as far as to present a holistic systematisation of knowledge in this area. More often, they focus on a single information security aspect or geographical location. For example, Tam et al. [123] investigate small business cybersecurity with a geographical focus on Australia while Alahmari & Duncan [4] place a focus on information security within SMEs with a priority on risk management. The study by Chidukwani et al. [35] provides a broader, more extensive summary. They investigate the cybersecurity within SMEs and its related challenges, research focus and recommendations in the context of the NIST cybersecurity framework version 1.1 and its five functions: Identify, Protect, Detect, Respond and Recover [97]. However, while they present many valid insights into the most pressing information security topics and issues for SMEs, they seem to consider a rather small number of scientific publications up to the year 2021. Furthermore, they focus on clustering the publications into the five NIST functions rather than a thematic clustering. Therefore, we aim to extend their research efforts by considering a larger number and more recent publications. We want to focus exclusively on a systematisation of knowledge, including a thematic clustering, as well as the identification of research gaps specifically requested by the SME information security publications studied. Accordingly, to the best of our knowledge, no comprehensive and holistic systematisation of knowledge on SME information security has been identified and we aim to address this gap.

3 Methodology

In order to address the research objective posed in Section 1, we conducted a (1) systematic literature review based on the process proposed by Kitchenham [80]. In doing so, we identified the most relevant and recent scientific papers in the field of SME information and cybersecurity. In addition, we extended our methodology to include non-scientific literature by conducting a (2) multivocal literature review [65, 66]. The reviews for scientific literature and grey literature in their adapted form both include the following three phases: *Definition of Search Strategy*, *Publication Selection* and *Data Extraction*. The structure of the multivocal literature review is illustrated in Figure 1. The results of the multivocal literature review were clustered and used to identify the most prominent research areas within the current

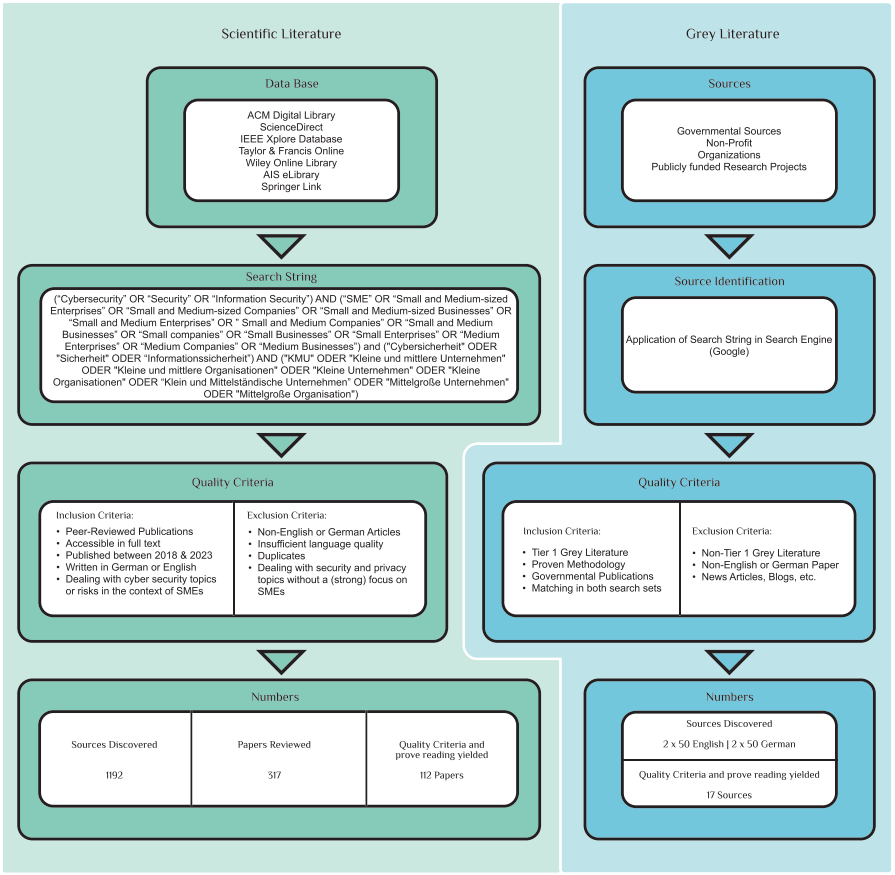

Figure 1 Multivocal literature review.

scientific and grey literature (see Section 4 and 5). As a final step, we examined and summarised the implications for future work and research within the scientific community on the topic of information security (see Section 6).

3.1 Scientific Literature

Definition of Search Strategy – The following seven databases were selected for the scientific database search: *ACM Digital Library, ScienceDirect, IEEE Xplore Database, Taylor & Francis Online, the Wiley Online Library, AIS eLibrary and Springer Link*. These databases were systematically searched

using predefined search strings. These search terms were developed on the basis of initial readings of reports (e.g. NIST publications, CIS controls, Enisa reports,...), which were conducted to skim the field of information security and to get a first impression of the overall topic. They were also discussed within the research group of authors contributing to this MVLR to build a consensus. Each search term includes both the phrases "information security" and "cybersecurity", as these two terms are often used synonymously in the literature [10, 117, 123]. The search term includes search phrases in the English and German language. As shown in Figure 1, the following search terms were used: *("Cybersecurity" OR "Security" OR "Information Security") AND ("SME" OR "Small and Medium-sized Enterprises" OR "Small and Medium-sized Companies" OR "Small and Medium-sized Businesses" OR "Small and Medium Enterprises" OR " Small and Medium Companies" OR "Small and Medium Businesses" OR "Small companies" OR "Small Businesses" OR "Small Enterprises" OR "Medium Enterprises" OR "Medium Companies" OR "Medium Businesses")* and *("Cybersicherheit" OR "Sicherheit" OR "Informationssicherheit") AND ("KMU" OR "Kleine und mittlere Unternehmen" OR "Kleine und mittlere Organisationen" OR "Kleine Unternehmen" OR "Kleine Organisationen" OR "Klein und Mittelständische Unternehmen" OR "Mittelgroße Unternehmen" OR "Mittelgroße Organisation")*. The structure of these search terms has been adapted to the respective method of input in each database without affecting the individual search terms. Our initial search yielded 1192 papers.

Publication Selection – In order to evaluate the relevance, timeliness, and quality of the identified publications, appropriate inclusion and exclusion criteria were applied to the initial search results. These can be seen in Figure 1. The following inclusion criteria were applied – *peer-reviewed, accessible in full text, published between 2018–2023, written in German or English and focusing on cybersecurity topics or risks in the context of SMEs*. The exclusion criteria were – *Non-English or German articles, insufficient language quality, duplicates and thematically dealing with security and privacy topics without a (strong) focus on SMEs*. After applying these quality criteria, the sources found were subjected to a relevance check based on their titles and abstracts. The remaining papers were then subjected to a thorough full-text review. Through this process, 112 scientific publications were identified as relevant to the topic of SME information security. The number of results per database can be seen in Table 1.

Data Extraction – The sources found to be relevant to the defined research objective were thoroughly reviewed by at least two authors working

in tandem. Whenever a contradiction was identified during the review and clustering process, the matter was discussed by at least two authors until a consensus was reached. They were grouped into 26 cluster categories. The cluster categories were developed by at least two authors who reviewed the publications. They were then checked by an additional author. They represent the core theme of a given publication. Cluster categories may overlap in scope. Each publication was assigned a maximum of three different cluster categories in order to identify the general topic of the publication and pursued research intend in the area of SME information security. The cluster categories and their respective sources are summarized in Section 4 and a comprehensive overview is given in Table 3.

Table 1 Composition of the scientific literature reviewed

Number of Results X Databases	AIS eLibrary	ACM	ScienceDirect	IEEE Xplore	Taylor & Francis	Wiley	Springer
Initial Hits	244	187	78	258	214	186	25
Filtered by Title	28	29	35	114	67	40	4
$\sum$ Reviewed Papers	317						
$\sum$ Included after Clustering	112						

3.2 Scientific Literature Research Gap

Following the thematic clustering of the scientific literature as described in Section 3.1 above, the identified literature was further analysed and clustered in terms of proposed future work and research gaps. This was done similarly to the thematic clustering. First, at least two authors identified the research gap(s) for each publication. Then, two or more authors categorized these gaps into cluster categories and a structured overview of the proposed future work as a whole (see Section 6 and Figure 4). In the event of a disagreement, the topic has been discussed by at least two or more of the authors until a consensus has been reached.

3.3 Grey Literature

Definition of Search Strategy – As shown in Figure 1, the search strategy for grey literature differs from the approach for scientific literature because it

is usually not listed in the common scientific databases [59]. Therefore, in order to include grey literature in this review, the first 50 results from the Google search engine for a predefined search string similar to the one used in the scientific literature were reviewed. The English search string – *("Cybersecurity" OR "Security" OR "Information Security") AND ("SME" OR "Small and Medium-sized Enterprises" OR "Small and Medium-sized Companies" OR "Small and Medium-sized Businesses" OR "Small and Medium Enterprises" OR "Small and Medium Companies" OR "Small and Medium Businesses" OR "Small companies" OR "Small Businesses" OR "Small Enterprises" OR "Medium Enterprises" OR "Medium Companies" OR "Medium Businesses")* and the German language search string – *("Cybersicherheit" OR "Sicherheit" OR "Informationssicherheit") AND ("KMU" OR "Kleine und mittlere Unternehmen" OR "Kleine und mittlere Organisationen" OR "Kleine Unternehmen" OR "Kleine Organisationen" OR "Klein und Mittelständische Unternehmen" OR "Mittelgroße Unternehmen" OR "Mittelgroße Organisation")* have been input by two authors from different geographical locations (Germany and Austria) on the same day. The resulting first 50 results were then documented by both authors. In order to identify the most relevant results, the 2×50 English language results and the 2×50 German language results from the search engine were compared, and only sources identified independently by both authors were included (see Table 2 for reference).

Table 2 Grey literature reviewed

	#English	#German
Google Search	2×50	2×50
Overlapping Publications	11	14
$\sum$ Reviewed Publications	25	
$\sum$ Included after Clustering	16	

Publication Selection – Only sources with a clearly identifiable document (PDF, etc.) on their website were included. Free text websites and their content were filtered out. This resulted in a total of 25 full-text sources. These sources have been subjected to a strict quality assessment similar to the scientific literature sources. The inclusion criteria for grey literature were – *Tier 1 grey literature, proven methodology, governmental publications, matching in both search sets (2 authors)* and the exclusion criteria were – *Non-Tier 1 grey literature, Non-English or German Publications and news articles, blogs, etc.* After applying the quality criteria, 16 sources were identified as containing SME information security content.

Data Extraction – These 16 grey literature sources were subjected to a thorough full-text review in order to cluster them in the same way as the scientific literature in Section 3.1. The thematic grey literature clustering can be found in Table 4. The grey literature has not been clustered in terms of future work requests, as future work is usually omitted from government publications.

4 Scientific Literature Results

This section summarises the results of the scientific part of the multivocal literature review. An overview of the composition of the included publications as well as their overall clustering is presented.

A total of 112 scientific publications relevant to information security in the context of SMEs were identified in the scientific literature review. An overview of the composition of the included literature is given in Figure 2. Of the 112 publications, 38 are journal publications, 69 belong to conferences and their proceedings, three are workshop publications and the last two are published tier 1 grey literature. The language of the literature considered is English, with the exception of one publication being in German.

In order to obtain a general overview of the literature considered and its focus prior to the clustering process, the papers were evaluated for their general focus on information technology (IT), operational technology (OT – production focused topics) and supply chain (SC) cybersecurity related topics. As can be seen in Figure 3, the overall focus of the scientific literature

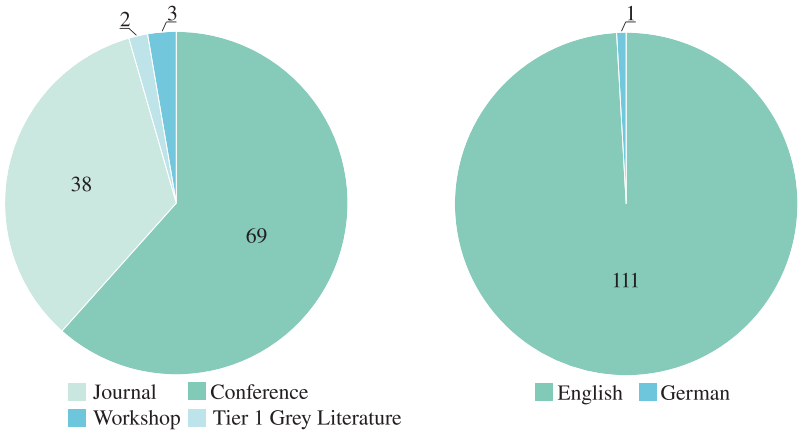

Figure 2 Publication characteristics.

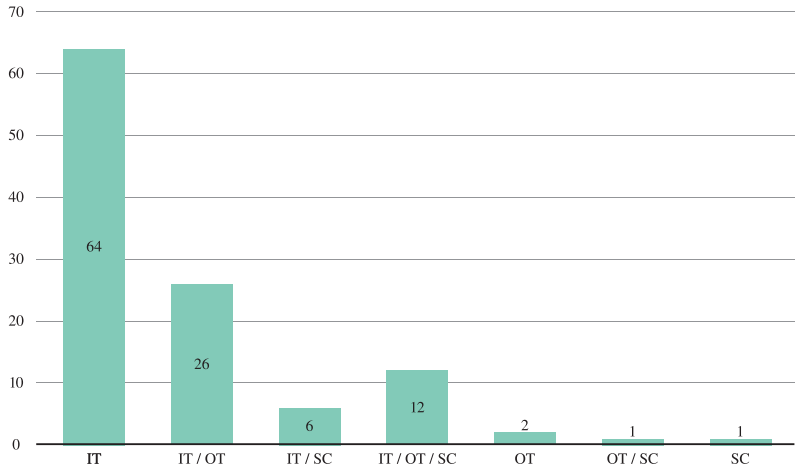

Figure 3 Publication focus.

on SME information security appears to be heavily oriented towards IT-related topics. 64 publications focus primarily on IT information security and a further 44 focus on IT in conjunction with either OT or SC-related topics or both (26 with a joint focus on IT and OT, 6 with a focus on IT and SC, and 12 covering all three evaluation criteria (IT/OT/SC)).

This shows that 108 out of 112 publications, or around 96%, have a primary focus on or include IT-related information security topics, which is a majority. On the other hand, publications that focus primarily on OT or SC information security in the context of SMEs seem to be rare in academic research on the subject. Only two publications have been marked down with a primary focus on OT, one with a shared focus between OT and SC and lastly a single one primarily focusing on SC information security. This suggests that operational technology and supply chain related information security issues may not (yet) be a focus of attention in the context of academic research on information security in SMEs.

4.1 Scientific Clustering

Following the general overview of the literature reviewed, the publications considered were clustered according to their overall focus on SME information security topics and risks. The publications were clustered into 26 cluster categories. Each publication has been assigned a maximum of 3 cluster categories in order to clearly reflect its overall thematic focus. The 26 cluster categories and their associated publication sources are summarised in Table 3.

Table 3 Clustering categories scientific literature – number of occurrences

Thematic Clustering Categories			
Category	Count	Category	Count
Framework	23	AI	8
[5, 19, 25, 27, 28, 37, 47, 50]		[25, 31, 39, 47, 60, 62, 110, 127]	
[79, 82, 85, 86, 90, 94, 95, 103]		Security Awareness	7
[106, 112, 118, 119, 135, 143, 144]		[32, 67, 82, 88, 111, 128, 140]	
Vulnerability / Threat Mgmt.	18	IoT Security	6
[8, 30, 39, 41, 60, 61, 67, 87, 95, 101]		[6, 15, 34, 45, 50, 84]	
[110, 111, 114, 116, 124, 127, 130, 144]		Security Governance	5
Risk Management	16	[16, 20, 75, 89, 119]	
[4, 12, 19, 20, 36, 61, 64, 78, 79]		Supply Chain Cybersecurity	4
[85, 94, 115, 122, 131, 134, 144]		[44, 90, 118, 140]	
Cybersecurity Assessment	16	Blockchain	4
[8, 11, 12, 14, 27, 43, 49, 70–72]		[69, 91, 102, 132]	
[78, 107, 115, 122, 131, 143]		Cybersecurity Advisory	4
Network Security	15	[11, 12, 43, 62]	
[1, 30, 31, 41, 47, 73, 81, 101]		Digital Transformation	2
[105, 114, 120, 126, 130, 133, 135]		[63, 75]	
Cybersecurity Survey	12	Operational Performance	2
[1, 2, 18, 35, 46, 48, 72]		[134, 135]	
[100, 103, 108, 129, 139]		Use of Private Devices	2
Legal Requirements	11	[3, 86]	
[16, 17, 26, 33, 34, 36, 42, 74]		Security Investments	2
[104, 113, 125]		[5, 87]	
Cloud	9	Cryptography	2
[9, 48, 68, 85, 86, 94, 101, 116, 133]		[68, 133]	
Security Controls	9	CS in Developing Countries	2
[13, 27, 28, 35, 37, 45, 103, 112, 124]		[3, 76]	
Industry 4.0	8	Cyber Insurance	1
[13, 15, 46, 63, 96, 102, 106, 121]		[76]	
User Behaviour	8	Secure Software Development	1
[2, 5, 14, 18, 77, 108, 110, 128]		[7]	

The degree of generalisation and the overall scope of the cluster categories vary. For example, the framework and risk management categories are very general and broad, while the blockchain and cryptography categories are more narrow and focused on specific technologies. The cluster categories

may overlap thematically to some extent due to the nature of closely related themes. The cluster categories are explained below:

- *Framework* – includes publications that approach a cybersecurity problem or strategy in a systematic and holistic way. As an example in this category, Skrodelis & Romanovs [118] discuss a framework for cyber-physical risk security in digital supply chains based on a basic risk management process. They outline the different steps and their implications within the different stages of the underlying risk management process and combine them into a digital supply chain framework.
- *Vulnerability / Threat Management* – includes publications that address topics related to identification, research and mitigation of specific vulnerabilities and threats in an information security scenario. As an example, Zhang et al. [144] present a general approach to understand vulnerabilities within SMEs, considering different vulnerability patterns and their performances.
- *Risk Management* – includes all information security risk related publications with a strong focus on risk management and mitigation. Sukumar et al. present a cyber risk assessment, which includes various risk categories. They presented these as part of a survey distributed to enterprises within the UK and establish a risk classification based on its results and expert considerations [122]. This publication, with its form of assessment of specific information security risks, is also part of the next thematic area of cybersecurity assessment.
- *Cybersecurity Assessment* – includes publications that focus on assessing specific information security measures, risks and the overall state of information security in organisations.
- *Network Security* – includes publications that focus on securing computer networks, particularly in the context of a production environment. For example, Chalvatzis et al. [30] present a technological approach to measuring system security through analysing and organizing attacks based on vulnerability scanning in computer networks to prevent system intrusion.
- *Cybersecurity Survey* – includes surveys, literature reviews and similar research methods to obtain data in the area of SME information security and related areas. An example is the paper by Chidukwani et al. [35], where they conduct a literature review of existing research mapped to the NIST Cybersecurity Framework functions and identify prominent security controls outlined in the literature.

- *Legal Requirements* – includes publications that address topics related to laws, regulations, and compliance standards governing information security practices. For example, Ryle et al. [113] discuss the US Federal Trade Commission's newly proposed regulatory changes to information security for financial SMEs in the US and the impact they could have on these firms in terms of time and resource expenditures.
- *Cloud* – includes publications that explore the security challenges, strategies, and solutions specific to cloud computing environments, covering aspects such as data protection and cloud-security awareness. Cloud computing and its adoption barriers and security risks for SMEs are a topic discussed in this thematic category by the authors Alsafi & Ran [9].
- *Security Controls* – includes publications that detail specific measures, practices, and technologies implemented to protect information systems and enhance the overall information security of an organisation. For example, Chidukwani et al. [35] conducted a literature review to identify common security measures described in the literature and suggested that more research was needed on the practical implementation of security controls.
- *Industry 4.0* – encompasses publications related to the security challenges and solutions in the context of Industry 4.0 solutions. As an example in this category, Stentoft et al. [121] discuss the drivers and barriers faced by manufacturing SMEs with respect to Industry 4.0 readiness and practices.
- *User Behaviour* – includes publications focusing on the human aspect of cybersecurity, exploring how user actions and behaviours impact security. An example of this is the publication by Kalhoro et al. [77] in which they examine the impact of personality traits on the information security behaviour of employees in SMEs.
- *AI* – covers publications that discuss the application of artificial intelligence in cybersecurity, including AI-driven threat detection, response mechanisms, and the use of machine learning algorithms to predict and mitigate cyber threats. For example, Chamou et al. [31] explore the use of deep learning techniques to detect information security threats such as malware attacks.
- *Security Awareness* – includes publications that focus on the importance of educating and training individuals about cybersecurity best practices, raising awareness of potential threats, and promoting a security-conscious culture within organisations. This category includes

publications such as Chaudhary et al. [32], who investigate the availability and scope of free and low-cost awareness resources in the context of SME information security.

- *IoT Security* – encompasses publications addressing the security challenges and solutions specific to Internet of Things (IoT) devices. For example, Alawadhi et al. [6] discuss the risks and challenges SMEs face when implementing an IoT system.
- *Security Governance* – covers publications that discuss the frameworks and policies governing cybersecurity practices on a high level within organisations. As an example publication, Maynard et al. [89] examine the governance process in SMEs at the organisational and employee level in relation to executive support and the overall security mission of the company.
- *Supply Chain Cybersecurity* – includes publications focused on securing the supply chain from cyber threats, discussing strategies for managing risks associated with third-party vendors and ensuring the integrity and security of supply chain operations. For example, Skrodelis & Romanovs [118] discuss a supply chain security framework based on a basic risk management process. They outline the different steps and their implications within the different stages of the underlying risk management process and aggregate them into a digital supply chain framework.
- *Blockchain* – encompasses publications that explore the use of blockchain technology in the context of SME information security. Gupta et al. [69] investigate the benefits of using blockchain technology to facilitate secure knowledge sharing and data transfer between SMEs and their supply chain partners.
- *Cybersecurity Advisory* – includes publications that provide expert advice and recommendations on improving cybersecurity postures. This can include strategic guidance, best practices, and consulting insights for organisations seeking to enhance their information security. For example, Franco et al. [62] propose a chat bot to support cybersecurity planning and management in SMEs.
- *Digital Transformation* – covers publications that discuss the cybersecurity implications of digital transformation initiatives, where businesses integrate digital technologies into all areas of operations, fundamentally changing how they operate and deliver value to customers. As an example in this category, Johannsen & Kant [75] discuss measures in IT governance, risk and compliance management to efficiently and securely manage the digital transformation of SMEs.

- *Operational Performance* – encompasses publications that examine the impact of cybersecurity measures on the operational performance of organisations. For example, Virglerova et al. [134] investigate business risks and their impact on the operational performance of SMEs.
- *Use of Private Devices* – includes publications that address the security challenges and strategies associated with the use of personal devices (BYOD – Bring Your Own Device) in the workplace. Akin & Kabanda [3] explore the practice of bringing your own devices to work in African SMEs and outline the security concerns associated with it.
- *Security Investments* – covers publications that discuss the financial aspects of cybersecurity and investing in it. As an example, Master et al. [87] assess the efficiency of security controls and discuss approaches to maximise the efficient use of the limited budget available for information security in SMEs.
- *Cryptography* – encompasses publications that delve into the science of encryption and secure communication. Vedeshin et al. [133] explore a cryptographic approach for home-based personal manufacturing based on a key and byte-less encryption method.
- *CS in Developing Countries* – includes publications that explore the unique cybersecurity challenges and strategies in developing countries. For example, Kabanda et al. [76] explore the cybersecurity challenges of SMEs specifically in the context of developing countries.

The last two cluster categories contain only one publication each, but the authors felt that these publications were so exclusively concerned with this area of research that they should be included in this thematic overview.

- *Cyber Insurance* – covers publications discussing the role of insurance in managing and mitigating cyber risk around information security incidents and breaches for organisations. Lemnitzer [83] investigates the lack of proper information security practices and discusses the introduction of mandatory information security insurance within SMEs and its potential benefits.
- *Secure Software Development* – encompasses publications that focus on integrating security into the software development lifecycle. Alghamdi et al. [7] explore factors associated with the adoption of information security measures in the development of custom-made software within SMEs.

As can be seen in Table 3, there are a number of cluster categories that seem to receive more attention from researchers than others. In general, these seem to be the more general and broadly defined categories rather

than the more specific and sometimes technology-focused ones. Examples are the 6 clusters which have been identified most often: *Framework (23), Vulnerability / Threat Management (18), Risk Management (16), Cybersecurity Assessment (16), Network Security (15) and Cybersecurity Survey (12)*, which all address a rather general problem area or method of data gathering within SME information security. These are accompanied by a number of other, also more frequently identified categories in the areas of legal research (*Legal Requirements* (11)), research related to specific technologies (*Cloud* (9), *Industry 4.0* (8), *AI* (8), *IoT Security* (6) and *Blockchain* (4)) and the human factor (*User Behaviour* (8) and *Security Awareness* (7)). Another often identified category with 9 specific occurrences is the research on *Security Controls* (9). Furthermore, research into *Security Governance* (5), *Supply Chain Cybersecurity* (4) and *Cybersecurity Advisory* (4) has received some attention. The thematic clustering is completed by a number of clusters that appear to have received little attention, with 2 or fewer publications addressing the area. This includes general areas such as *Digital Transformation* (2), *Operational Performance* (2), *Security Investments* (2) and *Cyber Insurance* (1) as well as some more specific research topics such as *Cryptography* (2), *Use of Private Devices* (2), *Cybersecurity in Developing Countries* (2) and *Secure Software Development* (1). Overall, this clustering outlines, that especially some more generally oriented areas which seem to be part of many information security efforts (Risk Management, Vulnerability / Threat Management, Frameworks, Cybersecurity Assessment, Security Controls) have received more research attention coupled with research into specific applications and restrictions of selected technologies (Cloud, Industry 4.0, AI, IoT Security, Blockchain). It seems noteworthy that the human factor in particular, related to information security culture and staff training, seems to be rather thinly represented, even though it is considered highly relevant to all information security efforts [32, 103]. Finally, there appear to be a number of clusters that have received only little attention from the research community, but may also be highly relevant, as some authors have focused almost exclusively on these areas in their publications.

5 Grey Literature Results

The grey literature review identified 16 relevant publications / documents on the topic. These were clustered in the same way as the scientific literature presented above. Table 4 outlines the clustering categories and their associated sources. An additional cluster category was identified in relation to

Table 4 Clustering categories grey literature – number of occurrences

Thematic Clustering Categories	
Category	Count
Cybersecurity Advisory [22–24, 29, 38, 54–56, 58, 92, 99, 136]	12
Security Controls [22, 24, 29, 38, 54, 56, 58, 99]	8
Framework [22, 29, 38, 54, 56]	5
Cybersecurity Survey [55, 136–138]	4
Vulnerability / Threat Mgmt. [21, 24, 55, 92]	4
Security Governance [93]	1
Incident Response [23]	1

the scientific clustering categories. This is the *Incident Response* category. This category has not specifically been identified as the focus of a publication within the scientific literature, but the grey literature publication [23] nearly exclusively focuses on the topic.

Looking at the summary from Table 4, the most prominent category within the 16 grey literature documents is *Cybersecurity Advisory* with 12 occurrences. This is followed by work on *Security Controls* (8), the *Framework* category (5), Cybersecurity Survey (4) and Vulnerability / Threat Management (4). Finally, there was a single publication focused on *Security Governance* (1) and *Incident Response* (1), respectively. It is evident that grey literature publications seem to have a strong focus on cybersecurity consulting and security controls. This is not surprising, as most of the publications are guidelines provided by government institutions to provide practical guidance in the area of SME cybersecurity. An observation made by the authors has been, that grey literature publications often provide more holistic recommendations and practical advice than could be identified in academic publications. This view seems to be confirmed by the identification of research gaps in the scientific literature (see Section 6 and Figure 4). The most prominent future work paths identified within the academic community are the extension and implementation of scientific frameworks and solutions

in practical scenarios, as well as the call for more tailored SME frameworks and solutions in general.

6 Discussion and Implications for Future Work

The following section summarises and discusses the identified research gaps and possible directions for future research efforts according to the analysed literature from the multi-vocal literature review. It highlights the most prominent areas suggested by the authors from the scientific publications and presents them in an easily understandable and clustered manner. The main findings from the scientific literature can be seen in Figure 4. The figure shows the identified research gaps together with the number of publications that included the research gap. All research clusters outlined by 5 or more publications were considered as leading research directions, and research areas with a total of 4 or fewer occurrences were thematically clustered as further specifications within the leading categories.

6.1 Academic Literature Proposed Future Work

Firstly, of the 112 scientific publications considered in this analysis of future work, 33 did not contain specific recommendations for future work in relation to SMEs. These have been excluded from the future work clusters shown in Figure 4. Next, 7 future work clusters outlined by more than 5 authors have been identified as leading research directions for future work. These are:

(1) *General Extension of Research* with 36 occurrences, which includes all publications that suggest more future work in general and regarding their own proposed frameworks and solutions in practical scenarios. This includes extending the proposed solutions with more real-world data and implementing the proposed frameworks and guidelines in real-world scenarios, such as deploying them in organisations to collect more performance data, observing organisational and user behaviour, or simply extending the baseline data for the research in a quantitative way. [3,8,12,19,20,25,27,28,31,36,39,41,44,47,48,50,62,70,72,78,79,81,86–89,95,102,104,107,110,114–116,130,131]

(2) *Tailored SME Frameworks and Solutions* with 31 occurrences, which includes the call for more tailored frameworks and solutions specifically adapted to the needs and constraints of small and medium-sized enterprises. This includes many sub-calls for specific areas of tailored frameworks and solutions for general research and specific research on technology-related

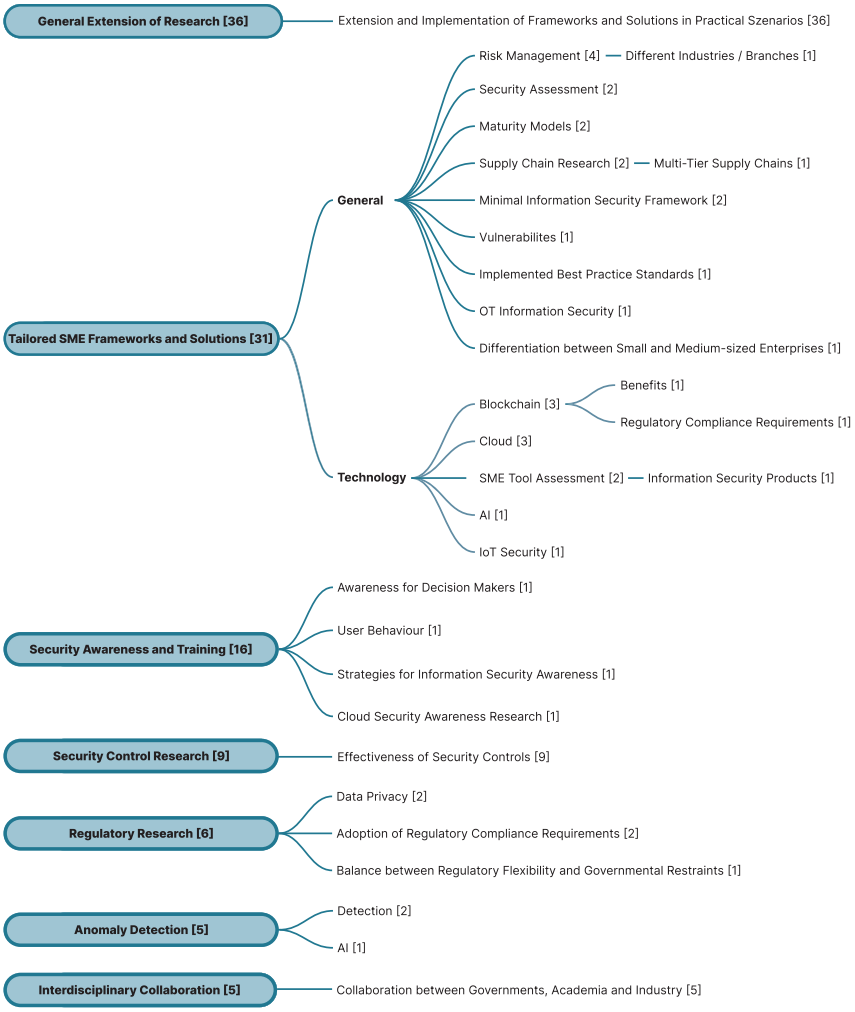

Figure 4 Scientific literature research gaps.

topics. These are discussed later in this section. [5, 6, 25, 31–34, 42, 63, 68, 69, 75, 82, 83, 87, 89–91, 94, 96, 103, 106, 109, 116, 122, 125, 134, 135, 139, 143, 144]

(3) *Security Awareness and Training* with 16 occurrences, which includes all publications with future calls for work related to information security awareness, how to establish and maintain an information security culture in organisations, and specifics on user behaviour and security training. [2, 5, 17, 26, 32, 35, 46, 47, 77, 82, 83, 94, 108, 116, 122, 128]

(4) *Security Control Research* with 9 occurrences, which includes all publications that deal with the specific evaluation, analysis, discussion and performance measurement of specific information security measures to increase overall information security within an organisation or to address specific threats and vulnerabilities. [2, 13, 26, 34, 35, 60, 101, 125, 133]

(5) *Regulatory Research* with 6 occurrences, which includes all publications that deal with regulatory issues related to government mandates such as privacy regulations, the adoption of regulatory compliance requirements such as laws, regulations, etc. by government bodies and organisations, and the balance between regulatory mandates and economic flexibility. [17, 33, 42, 74, 106, 113]

(6) *Anomaly Detection* with 5 occurrences, which includes publications dealing with the field and technology of anomaly detection in the context of information security efforts and proposing countermeasures. [25,87,105,110,126], and finally

(7) *Interdisciplinary Collaboration* with 5 occurrences, which includes publications that call for more interdisciplinary collaboration and cooperation regarding the pooling of resources for information security efforts between governments, the academic research community and industry players. [34, 42, 82, 83, 132]

These lead categories outline a clear need for more general and specific research for small and medium-sized enterprises. Furthermore, the prominent theme of security awareness and training, which is primarily concerned with research into the human factor in information security, appears to be another frequently requested area of research. This is in line with a general opinion in the literature that the human factor can be a valuable asset, but also one of the greatest threats within information security [32, 103]. This makes the proper establishment of a security culture and information security training for the workforce a much sought after research topic. In addition, the detailed study of security controls and measures to address security threats and vulnerabilities, research on regulatory issues related to government directives, laws, etc., anomaly detection and the call for more interdisciplinary collaboration between governments, academia and industry partners underline the need for future SME-related research in a broad variety of areas. These prominent research areas are complemented by a number of less frequent, but not necessarily less important, requests for future work on various topics. In order to provide a better overview of the research streams requested in the literature, these have been grouped thematically under the main categories.

6.2 Presentation of Subtopics

The first lead category, *General Extension of Research*, as shown in Figure 4, has no subcategories because it includes those publications that called for general extension and practical testing of their own proposed work in order to extend research data, gain practical insights and thus refine their work. They have not outlined other general and specific areas of research to be pursued. This is different for the publications and authors clustered in the second category, *Tailored SME Frameworks and Solutions*. The literature clustered in this lead category contained many additional requested future work subcategories. Therefore, two main subcategories, *General* research and *Technology* research, were created to better outline the research directions in this category. The *General* research category covers the broader themes of future work, and the *Technology* research category covers all future research requests related to specific technologies and their development and application. These have been used to better structure the subtopics related to this main category. The subcategories for *Tailored SME Frameworks and Solutions* in the *General* Research area are as follows (overview in Figure 4): *Risk Management* in general has been outlined as a future area of work by 4 publications [5, 25, 134, 139] as an area where tailored solutions and research for SMEs are still lacking and desired. [134] specifically outlined the need to investigate SME information security risk management in the context of different industries and sectors to assess its value and efficiency. *Security Assessment* as an area of future work has been outlined by two publications [109,139]. They call for more research into information security assessments to better understand security risks and assessments in SMEs, and to lower the barrier to entry into security assessments for individuals with less information security background. In addition, *Maturity Models* research has been requested by two authors [106, 143]. They call for more research regarding tailored SME specific maturity models and their application. Further, future research regarding a *Minimal Information Security Framework* has been requested by [83, 103]. Additionally, *Supply Chain Research* is outlined as a future research field by [44,90]. The latter paper outlines supply chain information security, particularly in multi-tier supply chains beyond tier 1 as possible future work to assess and evaluate information security throughout the entire SME supply chain. Furthermore, research areas under the General category, each requested in a single publication, are: Research on *Vulnerabilities* [144] within SMEs, *Implemented Best Practice Standards* [89], where the authors request the study of implemented best practice standards within SMEs and their practical implications, research focused on

production environments and enterprises (around their specific information security in operational technology (*OT Information Security*)) [135], and finally the study of the *Differentiation between Small and Medium-sized Enterprises* [75], where the authors propose to divide research for SMEs into research for small enterprises and research for medium enterprises to investigate differences in information security practices and risk mitigation.

The subcategories under the *Technology* branch of the main category *Tailored SME Frameworks and Solutions*, on the other hand, are (overview in Figure 4): Future research on *Blockchain* technology in the context of SME has been requested in three publications [33, 69, 91], with [69] focusing on exploring the potential benefits of using blockchain technology in information security and [33] on adopting regulatory compliance requirements related to blockchain. Another popular technology branch with three publications proposing future work is research on *Cloud* technology related to information security efforts within SME [68, 94, 116]. Further technology related research branches are an *SME Tool Assessment* [63,87] on information security tools and products for SME, research into the use of *AI* [31] for information security purposes and the topic of *IoT Security* requested by [6].

The lead category *Security Awareness and Training* also includes four associated subtopics in different research directions. [5] calls for research specifically related to the security behaviour and *Awareness for Decision Makers*, [128] suggests further investigation of *User Behaviour*, [82] calls for future research into *Strategies for Information Security Awareness*, and [116] outlines the importance of specifically *Cloud Security Awareness Research*. The lead category *Security Control Research* does not have any subcategories associated. It focuses on research regarding the efficiency and application of information security measures.

Next, the lead category *Regulatory Research* has three associated subcategories. First, *Data Privacy* as a research area related to government policies and legislation is requested by [74,106]. Secondly, research into the *Adoption of Regulatory Compliance Requirements* is outlined as future work by [33,42] and finally, investigation regarding a *Balance between Regulatory Flexibility and Governmental Restraints* and how this can effect SME is called for by [113].

To conclude the presentation of the subcategories, the lead category *Anomaly Detection* has two associated sub-directions for research, namely research into *Detection* methods [87, 105] and the investigation of *AI* [126] technology in relation to anomaly detection. Finally, the last lead category *Interdisciplinary Collaboration* calls for greater *Collaboration between*

Governments, Academia and Industry partners on SME information security research, policies and measures and has no associated subcategories.

6.3 Grey Literature

While the grey literature analysed in the multi-vocal literature review was clustered thematically in the same way as the academic literature (see Section 5), it was not clustered according to proposed research gaps and future work. This is due to the fact that grey literature published by not-for-profit organisations and governments tends to omit gaps in the research and directions for future work efforts.

It can be seen that many of the scientific research avenues requested match the thematic clustering of existing lines of work identified in Section 4.1, which is not surprising given that the authors requesting the future research are also responsible for the research already conducted and included in the thematic clustering. However, it is interesting to note that many of the areas that have already received a lot of attention according to the thematic clustering in Table 3 still seem to be highly requested areas for future research. For example, areas such as research into tailored and holistic frameworks and risk management, both of which have already received considerable attention in the existing work, are still highly and specifically requested avenues of research in future work. The same can be said for more focused research, for example on the scope and effectiveness of security controls for SMEs or blockchain technology, which remain much requested avenues of research in future work alongside many others. These facts, and the sheer number and variety of future avenues of work called for in the area of SME information security, paint a clear picture that much more research and practical application of concepts seems necessary to strengthen SME information security overall and in the long term.

6.4 Limitations

Our work may be limited by certain threats to validity, which we present and discuss below, along with appropriate countermeasures. These are (i) authors selection bias, (ii) clustering bias, (iii) low number of sources and (iv) language bias. (i) The first threat to validity is a biased selection of relevant publications within our research. To overcome this bias, we relied on a carefully structured and thorough methodology, including specific search terms, the use of relevant databases, and the involvement of at least two authors in every decision, from the development of the methodology, to

the establishment of appropriate inclusion and exclusion criteria, and finally the selection of a publication for inclusion. In addition, the entire process was documented in a research protocol to ensure scientific transparency. (ii) Another threat could be the biased establishment of cluster categories and/or identified path of future work. To circumvent this, at least two authors were involved in these processes at all times. In case of ambiguity, a discussion was held between the authors and a consensus was reached to resolve ambiguous decisions. (iii) A third risk to the validity of our research could be that the selection of sources considered is too limited to provide a holistic and comprehensive overview of the research area. To address this, we considered seven different databases in two different languages (German and English) to broaden the inclusion of potentially relevant sources. In addition, grey literature available on the topic was included to further broaden the literature review and provide a second perspective on the topic. A significant number of sources were considered for inclusion (1192 original scientific sources and 200 grey literature sources) in order to address this threat to the best of our ability. (iv) The language bias of only considering English and German papers in this review could be a threat to validity, as the team of authors are only fluent in these two languages to consider publications in a scientific research setting.

7 Conclusion & Future Work

In accordance with our research objectives and questions, we reviewed the academic and grey literature on SME information security to provide a baseline overview of the field. In doing so, we identified and quantitatively ranked the most prominent and common research paths within the field. We have also examined the grey literature on the topic and outlined an apparent difference in focus between the academic literature and the grey literature in this area. We have examined the future research pathways proposed by the academic community and clustered them in a structured and easily understandable way. In doing so, we have provided a clear overview and directions for future work that we would like to encourage the academic community to follow. It is clear that much more research is possible and seems necessary to strengthen SME information security in order to help these enterprises to establish an appropriate information security posture. We will continue on this research path by focusing on the highlighted future work streams to provide tailored frameworks and solutions for SMEs, coupled with more specific research on security controls in this context and a focus on practical validation of

our research. This involves the practical validation and assessment of a tailored SME information security framework we have developed, the in-depth discussion of the associated security controls and their practical application with our industry partners. Ultimately, we aimed for this work to empower SMEs by helping them to better understand their security posture, to provide researchers with a clear roadmap for future work and to assist policymakers in developing supportive and effective security frameworks by having identified research gaps.

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

[1] Fawad Ahmed, Aqil Burney, and Ahsan Malik. 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, 2020. doi:10.1109/ICISCT 49550.2020.9080029.

[2] Queen A Aigbefo, Yvette Blount, and Mauricio Marrone. The influence of hardiness and habit on security behaviour intention. *Behaviour & Information Technology*, 41(6):1151–1170, 2022. doi:10.1080/0144929X.2020.1856928.

[3] Adedolapo Akin-Adetoro and Salah Kabanda. Factors affecting the adoption of byod in south african small and medium enterprises. *The Electronic Journal of Information Systems in Developing Countries*, 87(6):e12185, 2021. doi:10.1002/isd2.12185.

[4] Abdulmajeed Alahmari and Bob Duncan. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pages 1–5. IEEE, 2020. doi:10.1109/CyberSA49311.2020.9139638.

[5] Abdulmajeed Abdullah Alahmari and Robert Anderson Duncan. Towards cybersecurity risk management investment: A proposed encouragement factors framework for smes. In *2021 IEEE International Conference on Computing (ICOCO)*, pages 115–121. IEEE, 2021. doi:10.1109/ICOCO53166.2021.9673554.

[6] Jenan Alawadhi, Amna Murad AlJanabi, Moaiad Ahmad Khder, Basel JA Ali, and Riyad F Al-Shalabi. Internet of things (iot) security risks: Challenges for business. In *2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, pages 450–456. IEEE, 2022. doi:10.1109/ICETSIS55481.2022.9888930.

[7] Fatimah Alghamdi, Nermin Hamza, and Moutasm Tamimi. Factors that influence the adoption of information security on requirement phase for custom-made software at smes. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pages 1–6. IEEE, 2019. doi:10.1109/CAIS.2019.8769519.

[8] Adnan Bin Amanat Ali, Ramesh Kumar Ayyasamy, Rehan Akbar, Vasaki Ap Ponnusamy, and Lim Ean Heng. Cybersecurity infrastructure adoption model for malware mitigation in small medium enterprises (sme). In *2022 IEEE 5th International Symposium in Robotics and Manufacturing Automation (ROMA)*, pages 1–6. IEEE, 2022. doi:10.1109/ROMA55875.2022.9915696.

[9] Tariq Alsafi and Ip-Shing Fan. Cloud computing adoption barriers faced by saudi manufacturing smes. In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6. IEEE, 2020. doi:10.23919/CISTI49556.2020.9140940.

[10] Abraham Althonayan and Alina Andronache. Shifting from information security towards a cybersecurity paradigm. In *Proceedings of the 2018 10th International Conference on Information Management and Engineering*, pages 68–79, 2018. doi:10.1145/3285957.3285971.

[11] Mário Antunes, Marisa Maximiano, and Ricardo Gomes. A customizable web platform to manage standards compliance of information security and cybersecurity auditing. *Procedia Computer Science*, 196:36–43, 2022. doi:10.1016/j.procs.2021.11.070.

[12] Laura Arenda and Oliver Popov. A conceptual model of an intelligent platform for security risk assessment in smes. In *2019 IEEE 13th International Conference on Application of Information and Communication Technologies (AICT)*, pages 1–8. IEEE, 2019. doi:10.1109/AICT47866.2019.8981796.

[13] Halldor Arnarson, Faraz Safarpour Kanafi, Tero Kaarlela, Ulrich Seldeslachts, and Roel Pieters. Evaluation of cyber security in agile manufacturing: Maturity of technologies and applications. In *2022 IEEE/SICE International Symposium on System Integration (SII)*, pages 784–789. IEEE, 2022. doi:10.1109/SII52469.2022.9708888.

[14] Liudmila Astakhova and Nikita Muravyov. A data collection and analysis system for managing the vulnerabilities of users of an information system in a small business. In *2019 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, pages 193–196. IEEE, 2019. doi:10.1109/USBEREIT.2019.8736583.

[15] Lukas Auer, Christian Skubich, and Matthias Hiller. A security architecture for risc-v based iot devices. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1154–1159. IEEE, 2019. doi:10.23919/DATE.2019.8714822.

[16] Bruno Azinheira, Mário Antunes, Marisa Maximiano, and Ricardo Gomes. A methodology for mapping cybersecurity standards into governance guidelines for sme in portugal. *Procedia Computer Science*, 219:121–128, 2023. doi:10.1016/j.procs.2023.01.272.

[17] Benjamin Bartlett. Government as facilitator: how japan is building its cybersecurity market. *Journal of Cyber Policy*, 3(3):327–343, 2018. doi:10.1080/23738871.2018.1550522.

[18] Rahadian Bisma, Septian Reri Winarto, and Yuanita Candra Puspita. 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, 2021. doi:10.1109/ICVEE54186.2021.9649719.

[19] Nefeli Bountouni, Sotiris Koussouris, Alexandros Vasileiou, and Stylianos A Kazazis. A holistic framework for safeguarding of smes: A case study. In *2023 19th International Conference on the Design of Reliable Communication Networks (DRCN)*, pages 1–5. IEEE, 2023. doi:10.1109/DRCN57075.2023.10108247.

[20] Michael Brunner, Andrea Mussmann, and Ruth Breu. Introduction of a tool-based continuous information security management system: An exploratory case study. In *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pages 483–490. IEEE, 2018. doi:10.1109/QRS-C.2018.00088.

[21] Bundesamt für Sicherheit in der Informationstechnik, BSI. Fortschrittliche angriffe – neue qualität aktueller angriffe und prognose, 2021. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Managementabstract-Angriffe.pdf?__blob=publicationFile&v=2.

[22] Bundesamt für Sicherheit in der Informationstechnik, BSI. Cybersicherheit für kmu – die top 14 fragen, 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_KMU.pdf?__blob=publicationFile&v=10.

[23] Bundesamt für Sicherheit in der Informationstechnik, BSI. Erste hilfe bei einem schweren it-sicherheitsvorfall, 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html.

[24] Bundesamt für Sicherheit in der Informationstechnik, BSI. Maßnahmenkatalog ransomware, 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Massnahmenkatalog.html.

[25] Eko Budi Cahyono, Suriani Binti Mohd Sam, Noor Hafizah Binti Hassan, Norliza Mohamed, Norulhusna Ahmad, and Yusnaidi Yusuf. A review on cyber resilience model in small and medium enterprises. In *2022 4th International Conference on Smart Sensors and Application (ICSSA)*, pages 114–119. IEEE, 2022. doi:10.1109/ICSSA54161.2022.9870952.

[26] Antonio Calcara and Raffaele Marchetti. State-industry relations and cybersecurity governance in europe. *Review of International Political Economy*, 29(4):1237–1262, 2022. doi:10.1080/09692290.2021.1913438.

[27] Juan Francisco Carías, Saioa Arrizabalaga, Leire Labaka, and Josune Hernantes. Cyber resilience self-assessment tool (cr-sat) for smes. *IEEE Access*, 9:80741–80762, 2021. doi:10.1109/ACCESS.2021.3085530.

[28] Juan Francisco Carías, Marcos RS Borges, Leire Labaka, Saioa Arrizabalaga, and Josune Hernantes. Systematic approach to cyber resilience operationalization in smes. *IEEE access*, 8:174200–174221, 2020. doi:10.1109/ACCESS.2020.3026063.

[29] Center for Cyber Security Belgium. Cyber security guide for sme / belgium, 2022. URL: https://www.cybersecuritycoalition.be/resource/cyber-security-guide-sme/.

[30] Ilias Chalvatzis, Dimitrios A Karras, and Rallis C Papademetriou. Using nasl based superscripts to measure system security through analyzing and organizing attacks. In *2019 27th Telecommunications Forum (TELFOR)*, pages 1–4. IEEE, 2019. doi:10.1109/TELFOR 48224.2019.8971211.

[31] Dimitra Chamou, Petros Toupas, Eleni Ketzaki, Stavros Papadopoulos, Konstantinos M Giannoutakis, Anastasios Drosou, and Dimitrios Tzovaras. Intrusion detection system based on network traffic using deep neural networks. In *2019 IEEE 24th international workshop on computer aided modeling and design of communication links and networks (CAMAD)*, pages 1–6. IEEE, 2019. doi:10.1109/CAMAD.2019.8858475.

[32] Sunil Chaudhary, Vasileios Gkioulos, and David Goodman. 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, 2022. doi:10.1007/978-3-031-25460-4_6.

[33] Yan Chen. Information security management: compliance challenges and new directions, 2022. doi:10.1080/15228053.2022.2148979.

[34] Pier Giorgio Chiara. The iot and the new eu cybersecurity regulatory landscape. *International Review of Law, Computers & Technology*, 36(2):118–137, 2022. doi:10.1080/13600869.2022.2060468.

[35] Alladean Chidukwani, Sebastian Zander, and Polychronis Koutsakis. A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, 10:85701–85719, 2022. doi:10.1109/ACCESS.2022.3197899.

[36] Chih-Chieh Chiu, Pang-Wei Tsai, and Chu-Sing Yang. Pids: an essential personal information detection system for small business enterprise. In *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pages 01–06. IEEE, 2021. doi:10.1109/ICECCME52200.2021.959 0950.

[37] Carlos F Cruzado, Liset S Rodriguez-Baca, Lizeth G Huanca-López, and Erika I Acuña-Salinas. Reference framework "hogo" for cybersecurity in smes based on iso 27002 and 27032. In *2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pages 35–40. IEEE, 2022. doi:10.1109/Confluence52989.2022.9734116.

[38] CSA Singapore. Cybersecurity toolkit for sme owners, 2021. URL: https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-toolkits/enterprise-leaders-and-sme-owners.

[39] Jordi Cucurull, Christos Tselios, Carolina Rueda, Noemi Folch, Fady Copty, Reda Igbaria, Manos Athanatos, Antonios Krithinakis, Sotiris Ioannidis, Jose Francisco Ruiz, et al. Integration of an online voting solution with the smesec security framework. In *2020 IEEE international systems conference (SysCon)*, pages 1–8. IEEE, 2020. doi:10.1109/SysCon47679.2020.9275838.

[40] Cybersecurity & Infrastructure Security Agency. Executive order on improving the nation's cybersecurity, 2021. Accessed on: 08/12/2024. URL: https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity.

[41] Jose Emmanuel Cruz de la Cruz, Christian Augusto Romero Goyzueta, and Cristian Delgado Cahuana. Intrusion detection and prevention system for production supervision in small businesses based on raspberry pi and snort. In *2020 IEEE XXVII International Conference on Electronics, Electrical Engineering and Computing (INTERCON)*, pages 1–4. IEEE, 2020. doi:10.1109/INTERCON50315.2020.9220240.

[42] Danilo D'elia. Industrial policy: the holy grail of french cybersecurity strategy? *Journal of Cyber Policy*, 3(3):385–406, 2018. doi:10.1080/23738871.2018.1553988.

[43] Petr Douchek, Lea Nedomova, Ladislav Luc, and Lubek Novak. Information security: The glory and penury of smes in the czech and slovak republics. In *2020 International Conference on Engineering Management of Communication and Technology (EMCTECH)*, pages 1–7. IEEE, 2020. doi:10.1109/EMCTECH49634.2020.9261506.

[44] Olatunde Durowoju, Hing Kai Chan, and Xiaojun Wang. 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, 2020. doi:10.1109/TEM.2020.3008827.

[45] Ife Olalekan Ebo, Olorunjube James Falana, Olutosin Taiwo, and Bamidele Alaba Olumuyiwa. An enhanced secured iot model for enterprise architecture. In *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*, pages 1–6. IEEE, 2020. doi:10.1109/ICMCECS47690.2020.247112.

[46] Marco Ehrlich, Henning Trsek, Lukasz Wisniewski, and Jürgen Jasperneite. Survey of security standards for an automated industrie 4.0 compatible manufacturing. In *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society*, volume 1, pages 2849–2854. IEEE, 2019. doi:10.1109/IECON.2019.8927559.

[47] Ogerta Elezaj, Sule Yildirim Yayilgan, Mohamed Abomhara, Prosper Yeng, and Javed Ahmed. Data-driven intrusion detection system for small and medium enterprises. In *2019 IEEE 24th international workshop on computer aided modeling and design of communication links and networks (CAMAD)*, pages 1–7. IEEE, 2019. doi:10.1109/CAMAD.2019.8858166.

[48] Carsten Ellwein, Oliver Riedel, Olga Meyer, and Daniel Schel. Rent'n'produce: A secure cloud manufacturing platform for small and medium enterprises. In *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, pages 1–6. IEEE, 2018. doi:10.1109/ICE.2018.8436332.

[49] Asja Emer, Marco Unterhofer, and Erwin Rauch. A cybersecurity assessment model for small and medium-sized enterprises. *IEEE Engineering Management Review*, 49(2):98–109, 2021. doi:10.1109/EMR.2021.3078077.

[50] Philip Empl and Günther Pernul. A flexible security analytics service for the industrial iot. In *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, New York, NY, USA, 2021. Association for Computing Machinery. doi:10.1145/3445969.3450427.

[51] European Commission. User guide to the sme definition, 2020. doi:10.2873/255862.

[52] European Commission. Cyber resilience act, 2023. URL: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[53] European Commission. Directive on measures for a high common level of cybersecurity across the union (nis2 directive), 2023. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[54] European Digital SME Alliance. Small business standards – sme guide on information security controls, 2022. URL: https://www.digitalsme.eu/new-sme-guide-on-information-security-controls/.

[55] European Union Agency for Cybersecurity, Enisa. Cybersecurity for smes – challenges and recommentations, 2021. doi:10.2824/770352.

[56] European Union Agency for Cybersecurity, Enisa. Cybersecurity guide for smes – 12 steps – to securing your business, 2021. URL: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes.

[57] European Union Agency for Cybersecurity, ENISA. Enisa threat landscape 2023, 2023. doi:10.2824/782573.

[58] European Union Agency for Cybersecurity, Enisa; Cert-EU. Boosting your organisation's cyber resilience, 2022. URL: https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience.

[59] Dominic J Farace and Joachim Schöpfel. *Grey literature in library and information studies*. KG Saur, 2010. doi:10.1515/9783598441493.

[60] Ignacio Fernandez De Arroyabe and Juan Carlos Fernandez de Arroyabe. The severity and effects of cyber-breaches in smes: a machine learning approach. *Enterprise Information Systems*, 17(3):1942997, 2023. doi:10.1080/17517575.2021.1942997.

[61] Pedro Tubío Figueira, Cristina López Bravo, and José Luis Rivas López. Improving information security risk analysis by including threat-occurrence predictive models. *Computers & Security*, 88:101609, 2020. doi:10.1016/j.cose.2019.101609.

[62] Muriel Figueredo Franco, Bruno Rodrigues, Eder John Scheid, Arthur Jacobs, Christian Killer, Lisandro Zambenedetti Granville, and Burkhard Stiller. Secbot: a business-driven conversational agent for cybersecurity planning and management. In *2020 16th international conference on network and service management (CNSM)*, pages 1–7. IEEE, 2020. doi:10.23919/CNSM50824.2020.9269037.

[63] Sébastien Gamache, Georges Abdul-Nour, and Chantal Baril. Evaluation of the influence parameters of industry 4.0 and their impact on the quebec manufacturing smes: The first findings. *Cogent Engineering*, 7(1):1771818, 2020. doi:10.1080/23311916.2020.1771818.

[64] Chris García-Porras, Sarita Huamani-Pastor, and Jimmy Armas-Aguirre. Information security risk management model for peruvian smes. In *2018 IEEE Sciences and Humanities International Research Conference (SHIRCON)*, pages 1–5. IEEE, 2018. doi:10.1109/SHIRCON.2018.8592994.

[65] Vahid Garousi, Michael Felderer, and Mika V Mäntylä. The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature. In *Proceedings of the 20th international conference on evaluation and assessment in software engineering*, pages 1–6, 2016. doi:10.1145/2915970.2916008.

[66] Vahid Garousi, Michael Felderer, and Mika V Mäntylä. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology*, 106:101–121, 2019. doi:10.1016/j.infsof.2018.09.006.

[67] R.E. Georgsen and G. Myrdahl Køien. Serious games with sysml: Gamifying threat modelling in a small business setting. In *INCOSE International Symposium*, volume 32, pages 119–132. Wiley Online Library, 2022. doi:10.1002/iis2.12902.

[68] Mani Goyal and Avinash Sharma. Enhancing hybrid encryption techniques for secured data processing for small medium enterprises in cloud. In *2021 IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES)*, pages 1–5. IEEE, 2021. doi:10.1109/TRIBES52498.2021.9751621.

[69] Chetna Gupta, Varun Gupta, and Jose Maria Fernandez-Crehuet. A blockchain-enabled solution to improve intra-inter organizational innovation processes in software small medium enterprises. *Engineering Reports*, 5(7):e12674, 2023. doi:10.1002/eng2.12674.

[70] Michael Heidenreich. Conceptualization of a measurement method proposal for the assessment of it security in the status quo of micro-enterprises. In *2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, pages 187–192. IEEE, 2019. doi:10.1109/iCCECE46942.2019.8941688.

[71] Michael Heidenreich. Implementation of an it security measurement method for the evaluation of it security in micro-enterprises. In *2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, pages 92–97. IEEE, 2020. doi:10.1109/iCCECE49321.2020.9231113.

[72] Michael Heidenreich, Bogdan Franczyk, and Andreas Johannsen. 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, 2022. doi:10.1109/ICECET55527.2022.9873487.

[73] Blake Iyamuremye and Hisato Shima. Network security testing tools for smes (small and medium enterprises). In *2018 IEEE International Conference on Applied System Invention (ICASI)*, pages 414–417. IEEE, 2018. doi:10.1109/ICASI.2018.8394272.

[74] Marko Jäntti. Studying data privacy management in small and medium-sized it companies. In *2020 14th International Conference*

on Innovations in Information Technology (IIT), pages 57–62. IEEE, 2020. doi:10.1109/IIT50501.2020.9299050.

[75] Andreas Johannsen and Daniel Kant. It-governance-, risiko-und compliance-management (it-grc)–ein kompetenzorientierter ansatz für kmu. In *Faktor Mensch*, pages 275–294. Springer, 2022. doi:10.1365/s40702-020-00625-8.

[76] Salah Kabanda, Maureen Tanner, and Cameron Kent. Exploring sme cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3):269–282, 2018. doi:10.1080/10919392.2018.1484598.

[77] Shadab Kalhoro, Ramesh Kumar Ayyasamy, AbdulKarim Kanaan Jebna, Anam Kalhoro, Kesavan Krishnan, and Suresh Nodeson. How personality traits impacts on cyber security behaviors of smes employees. In *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, pages 635–641. IEEE, 2022. doi:10.1109/3ICT56508.2022.9990621.

[78] Evangelia Kavakli, Pericles Loucopoulos, and Yannis Skourtis. Capability oriented re for cybersecurity and personal data protection: Meeting the challenges of smes. In *2022 IEEE 30th International Requirements Engineering Conference Workshops (REW)*, pages 244–249. IEEE, 2022. doi:10.1109/REW56159.2022.00053.

[79] Bong-Jae Kim and Seok-Won Lee. Understanding and recommending security requirements from problem domain ontology: A cognitive three-layered approach. *Journal of Systems and Software*, 169:110695, 2020. doi:10.1016/j.jss.2020.110695.

[80] Barbara Kitchenham. Procedures for performing systematic reviews. Joint Technical Report TR/SE-0401, Keele University, Keele, UK, July 2004. URL: https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf.

[81] Sushil Kumar et al. Botnet detection techniques and research challenges. In *2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC)*, pages 1–6. IEEE, 2019. doi:10.1109/ICRAECC43874.2019.8995028.

[82] Tebogo Kesetse Lejaka, Adéle Da Veiga, and Marianne Loock. 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, 2019. doi:10.1109/ICTAS.2019.8703609.

[83] Jan Martin Lemnitzer. Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, 6(2):118–136, 2021. doi:10.1080/23738871.2021.1880609.

[84] John Lindström, Jens Eliasson, Anders Hermansson, Fredrik Blomstedt, and Petter Kyösti. Cybersecurity level in ips2: A case study of two industrial internet-based sme offerings. *Procedia CIRP*, 73:222–227, 2018. doi:10.1016/j.procir.2018.03.302.

[85] Evangelos Mantas, Dimitris Papadopoulos, Carolina Fernández, Nil Ortiz, Maxime Compastié, Antonio López Martínez, Manuel Gil Pérez, Akis Kourtis, George Xylouris, Izidor Mlakar, et al. 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, 2021. doi:10.1109/MeditCom49071.2021.9647609.

[86] Evangelos Markakis, Yannis Nikoloudakis, George Mastorakis, Constandinos X Mavromoustakis, Evangelos Pallis, Anargyros Sideris, Nikolaos Zotos, Jan Antic, Ales Cernivec, Diana Fejzic, et al. Acceleration at the edge for supporting smes security: The fortika paradigm. *IEEE Communications Magazine*, 57(2):41–47, 2019. doi:10.1109/MCOM.2019.1800506.

[87] Alexander Master, George Hamilton, and J Eric Dietz. Optimizing cybersecurity budgets with attacksimulation. In *2022 IEEE International Symposium on Technologies for Homeland Security (HST)*, pages 1–7. IEEE, 2022. doi:10.1109/HST56032.2022.10024984.

[88] Peter Mayer and Melanie Volkamer. Addressing misconceptions about password security effectively. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, pages 16–27, 2018. doi:10.1145/3167996.3167998.

[89] Sean Maynard, Terrence Tan, Atif Ahmad, and Tobias Ruighaver. Towards a framework for strategic security context in information security governance. *Pacific Asia Journal of the Association for Information Systems*, 10(4):4, 2018. doi:10.17705/1PAIS.10403.

[90] Steven A Melnyk, Tobias Schoenherr, Cheri Speier-Pero, Chris Peters, Jeff F Chang, and Derek Friday. New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, 60(1):162–183, 2022. doi:10.1080/00207543.2021.1984606.

[91] Suneetha Merugula, G Dinesh, M Kathiravan, Gourab Das, Praful Nandankar, and Santoshachandra Rao Karanam. Study of blockchain technology in empowering the sme. In *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, pages 758–765. IEEE, 2021. doi:10.1109/ICAIS50930.2021.9395831.

[92] Mittelstand Digital. Gegen cyberattacken gewappnet – sechs einfallstore für cyberangriffe bei kleineren und mittelständischen unternehmen, 2020. URL: https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/it-sicherheitsrisiko-gegen-cyberatacken.pdf?__blob=publicationFile&v=1.

[93] Mittelstand Digital. Iso 27001 – ein leitfaden zum interformationssicherheitsmanagement, 2021. URL: https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/it-sicherheit-leitfaden-Informationssicherheitsmanagememt.pdf?__blob=publicationFile&v=3.

[94] Izidor Mlakar, Primož Jeran, Valentino Šafran, and Vangelis Logothetis. A cost-effective security framework to protect micro enterprises: Palantir e-commerce use case. In *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6. IEEE, 2021. doi:10.1109/ISDFS52919.2021.9486359.

[95] Megat Muazzam Abdul Mutalib, Zuraini Zainol, and Mohd Hazali Mohamed Halip. Mitigating malware threats at small medium enterprise (sme) organisation: A review and framework. In *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, volume 6, pages 1–6. IEEE, 2021. doi:10.1109/ICRAIE52900.2021.9703991.

[96] Vaibhav S Narwane, Rakesh D Raut, Bhaskar B Gardas, Balkrishna E Narkhede, and Anjali Awasthi. Examining smart manufacturing challenges in the context of micro, small and medium enterprises. *International Journal of Computer Integrated Manufacturing*, 35(12):1395–1412, 2022. doi:10.1080/0951192X.2022.2078508.

[97] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity – version 1.1, 2018. doi:10.6028/NIST.CSWP.04162018.

[98] National Institute of Standards and Technology, U.S. Department of Commerce. Small business information security: The fundamentals – nistir 7621 revision 1, 2016. doi:10.6028/NIST.IR.7621r1.

[99] Nationales Zentrum für Cybersicherheit NCSC – Schweizerische Eidgenossenschaft. Merkblatt informationssicherheit für kmus, 2020. URL: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html.

[100] Tabisa Ncubukezi, Laban Mwansa, and Francois Rocaries. 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, 2020. doi:10.23919/ICITST51030.2020.9351339.

[101] Rohit Negi, S Venkatesan, and Sandeep K Shukla. *Implementing Enterprise Cyber Security with Open-Source Software and Standard Architecture: Volume II*, chapter Implementation of an Intrusion Detection System and Deception Technologies using Open Source Tools for Small Businesses, pages 151–192. River Publishers, 2023. doi:10.1201/9781003426134-10.

[102] Alessandra Neri, Marta Negri, Enrico Cagno, Simone Franzò, Vikas Kumar, Tommaso Lampertico, and Carlo Andrea Bassani. The role of digital technologies in supporting the implementation of circular economy practices by industrial small and medium enterprises. *Business Strategy and the Environment*, 32(7):4693–4718, 2023. doi:10.1002/bse.3388.

[103] Shekhar Pawar and Hemant Palivela. 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, 2022. doi:10.1016/j.jjimei.2022.100080.

[104] Luís M Pedroso, Virgínia M Araújo, Manuel Perez Cota, and João Paulo Magalhães. How can gdpr fines help smes ensuring the privacy and protection of processed personal data. In *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6. IEEE, 2021. doi:10.23919/CISTI52073.2021.9476620.

[105] HMDGV Perera, KM Samarasekara, IUK Hewamanna, DNW Kasthuriarachchi, Kavinga Yapa Abeywardena, and Kanishka Yapa. Netbot-an automated router hardening solution for small to medium enterprises. In *2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0015–0021. IEEE, 2021. doi:10.1109/IEMCON53756.2021.9623186.

[106] Jean-Rémi Piat, Christophe Danjou, Bruno Agard, and Robert Beauchemin. A guideline to implement a cps architecture in an sme. *Production & Manufacturing Research*, 11(1):2218910, 2023. doi:10.1080/21693277.2023.2218910.

[107] Christophe Ponsard, Philippe Massonet, Jeremy Grandclaudon, and Nicolas Point. From lightweight cybersecurity assessment to sme certification scheme in belgium. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 75–78. IEEE, 2020. doi:10.1109/EuroSPW51379.2020.00019.

[108] Andrew Rae and Asma Patel. 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, 2020. doi:10.1109/CyberSecurity 49315.2020.9138893.

[109] Simona Ramanauskaite, Jogaile Raslanaite, Laima Kaupadiene, et al. Information integrity estimation model for small and medium enterprise. In *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, pages 1–6. IEEE, 2018. doi:10.1109/AIEEE.2018.8592443.

[110] Fatema Rashid and Ali Miri. User and event behavior analytics on differentially private data for anomaly detection. In *2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 81–86. IEEE, 2021. doi:10.1109/BigDataSecurity HPSCIDS52275.2021.00025.

[111] Julio Alexander Rodríguez-Corzo, Alix E Rojas, and Camilo Mejía-Moncayo. Methodological model based on gophish to face phishing vulnerabilities in sme. In *2018 ICAI Workshops (ICAIW)*, pages 1–6. IEEE, 2018. doi:10.1109/ICAIW.2018.8555006.

[112] Nair Rubio, Lurdes Chavarria, and David Mauricio. Security architecture for the protection of digital assets in smes. In *2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, pages 1–6. IEEE, 2020. doi:10.1109/ICECCE49384.2020.9179422.

[113] Patrick Ryle, Jie Yan, and Lorraine R Gardiner. Gramm-leach-bliley gets a systems upgrade: What the ftc's proposed safeguards rule changes mean for small and medium american financial institutions. *EDPACS*, 65(2):6–17, 2022. doi:10.1080/07366981.2021.1911387.

[114] S Sarath, A Asif, and P Aravind. Low-cost security solution for micro, small and medium enterprises. In *2020 IEEE International Conference for Innovation in Technology (INOCON)*, pages 1–9. IEEE, 2020. doi:10.1109/INOCON50539.2020.9298273.

[115] Christopher Schmitz and Sebastian Pape. Lisra: Lightweight security risk assessment for decision support in information security. *Computers & Security*, 90:101656, 2020. doi:10.1016/j.cose.2019.101656.

[116] Ahmad Zia Sharifi, Hashmatullah Zaheer, Mohammad Fahim Azizi, and Jamilurahman Faizi. Detection and prevention of distributed

denial of service attacks in smes: the case of cloudplus. In *2019 Sixteenth International Conference on Wireless and Optical Communication Networks (WOCN)*, pages 1–4. IEEE, 2019. doi:10.1109/WOCN45266.2019.8995022.

[117] Erik Silfversten, Erik Frinking, Nathan Ryan, and Marina Favaro. Cybersecurity – a state-of-the-art review – executive summary, 2019. URL: https://repository.wodc.nl/bitstream/handle/20.500.12832/2423/2956_Summary_tcm28-397365.pdf?sequence=1&isAllowed=y.

[118] Heinrihs Kristians Skrodelis and Andrejs Romanovs. Cyber-physical risk security framework development in digital supply chains. In *2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, pages 1–5. IEEE, 2021. doi:10.1109/ITMS52826.2021.9615305.

[119] Heinrihs Kristians Skrodelis, Julija Strebko, and Andrejs Romanovs. The information system security governance tasks in small and medium enterprises. In *2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, pages 1–4. IEEE, 2020. doi:10.1109/ITMS51158.2020.9259305.

[120] Olena Starkova, Kostiantyn Herasymenko, Sergii M Korotin, Volodymyr Afanasiev, and Anastasiia Lisnyk. Development of recommendations for ensuring security in a corporate network. In *2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, pages 111–115. IEEE, 2019. doi:10.1109/ATIT49449.2019.9030470.

[121] Jan Stentoft, Kent Adsbøll Wickstrøm, Kristian Philipsen, and Anders Haug. Drivers and barriers for industry 4.0 readiness and practice: empirical evidence from small and medium-sized manufacturers. *Production Planning & Control*, 32(10):811–828, 2021. doi:10.1080/09537287.2020.1768318.

[122] Arun Sukumar, Hannan Amoozad Mahdiraji, and Vahid Jafari-Sadeghi. Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*, 43(10):2082–2098, 2023. doi:10.1111/risa.14092.

[123] Tracy Tam, Asha Rao, and Joanne Hall. The good, the bad and the missing: A narrative review of cyber-security implications for australian small businesses. *Computers & Security*, 109:102385, 2021. doi:10.1016/j.cose.2021.102385.

[124] Haydar Teymourlouei and Vareva Harris. Effective methods to monitor it infrastructure security for small business. In *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 7–13. IEEE, 2019. doi:10.1109/CSCI49370.2019.00009.

[125] Paul Timmers. The european union's cybersecurity industrial policy. *Journal of Cyber Policy*, 3(3):363–384, 2018. doi:10.1080/23738871.2018.1562560.

[126] Thomas Toublanc, Romain Bévan, Florent de Lamotte, and Pascal Berruet. Assisting the configuration of intelligent safety gateway. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pages 5875–5880. IEEE, 2018. doi:10.1109/IECON.2018.8591155.

[127] Khaizuran Aqhar Ubaidillah, Syifak Izhar Hisham, Ferda Ernawan, Gran Badshah, and Edy Suharto. Intrusion detection system using autoencoder based deep neural network for sme cybersecurity. In *2021 5th International Conference on Informatics and Computational Sciences (ICICoS)*, pages 210–215. IEEE, 2021. doi:10.1109/ICICoS53627.2021.9651851.

[128] Betsy Uchendu, Jason RC Nurse, Maria Bada, and Steven Furnell. Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109:102387, 2021. doi:10.1016/j.cose.2021.102387.

[129] Patrick Ulrich, Vanessa Frank, and Alice Timmermann. The dark side of data science-an empirical study of cyber risks in german smes. *Procedia Computer Science*, 176:2615–2624, 2020. doi:10.1016/j.procs.2020.09.307.

[130] Nikolaos Vakakis, Odysseas Nikolis, Dimosthenis Ioannidis, Konstantinos Votis, and Dimitrios Tzovaras. Cybersecurity in smes: The smart-home/office use case. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–7. IEEE, 2019. doi:10.1109/CAMAD.2019.8858471.

[131] Max Van Haastrecht, Injy Sarhan, Alireza Shojaifar, Louis Baumgartner, Wissam Mallouli, and Marco Spruit. A threat-based cybersecurity risk assessment approach addressing sme needs. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, pages 1–12, 2021. doi:10.1145/3465481.3469199.

[132] Srinidhi Vasudevan. Defi: A risky business or silver bullet for smes? In *2022 International Conference on Cyber Resilience (ICCR)*, pages 1–5. IEEE, 2022. doi:10.1109/ICCR56254.2022.9995866.

[133] Anton Vedeshin, John Mehmet Ulgar Dogru, Innar Liiv, Sadok Ben Yahia, and Dirk Draheim. A secure data infrastructure for personal manufacturing based on a novel key-less, byte-less encryption method. *IEEE Access*, 8:40039–40056, 2019. doi:10.1109/ACCESS.2019.2946730.

[134] Zuzana Virglerova, Marija Panic, Danijela Voza, and Milica Velickovic. Model of business risks and their impact on operational performance of smes. *Economic research-Ekonomska istraživanja*, 35(1):4047–4064, 2022. doi:10.1080/1331677X.2021.2010111.

[135] Patrick Wagner, Gerhard Hansch, Christoph Konrad, Karl-Heinz John, Jochen Bauer, and Jörg Franke. Applicability of security standards for operational technology by smes and large enterprises. In *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, pages 1544–1551. IEEE, 2020. doi:10.1109/ETFA46521.2020.9212126.

[136] Wik – Wirtschaftliches Institut für Infrastruktur und Kommunikationsdienste. Aktuelle lage der it-sicherheit in kmu, 2017. URL: https://www.wik.org/fileadmin/files/_migrated/news_files/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf.

[137] Wik – Wirtschaftliches Institut für Infrastruktur und Kommunikationsdienste. Current it security situation in smes – summary of representative survey results, 2017. URL: https://www.wik.org/fileadmin/files/_migrated/news_files/Current_IT_Security_Situation_in_SME_WIK_en__2_.pdf.

[138] Wik – Wirtschaftliches Institut für Infrastruktur und Kommunikationsdienste. Digitales handwerk unterschätzt it-risiken, 2023. URL: https://www.wik.org/fileadmin/files/_migrated/news_files/Infoblatt_Handwerk_-_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_-_WIK_2017.pdf.

[139] Martin Wilson, Sharon McDonald, Dominic Button, and Kenneth McGarry. It won't happen to me: surveying sme attitudes to cybersecurity. *Journal of Computer Information Systems*, 63(2):397–409, 2023. doi:10.1080/08874417.2022.2067791.

[140] Lai-Wan Wong, Voon-Hsien Lee, Garry Wei-Han Tan, Keng-Boon Ooi, and Amrik Sohal. The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66:102520, 2022. doi:10.1016/j.ijinfomgt.2022.102520.

[141] World Bank Group. Small and medium enterprises (smes) finance – improving smes‘ access to finance and finding innovative solutions to unlock sources of capital, 2019. Accessed on: 05/15/2024. URL: https://www.worldbank.org/en/topic/smefinance.

[142] World Economic Forum. Global cybersecurity outlook 2024 – insight report, 2024. URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

[143] Bilge Yigit Ozkan and Marco Spruit. Adaptable security maturity assessment and standardization for digital smes. *Journal of Computer Information Systems*, 63(4):965–987, 2023. doi:10.1080/08874417.2022.2119442.

[144] Xiong Zhang, Haoran Xie, Hao Yang, Hongkai Shao, and Minghao Zhu. A general framework to understand vulnerabilities in information systems. *IEEE Access*, 8:121858–121873, 2020. doi:10.1109/ACCESS.2020.3006361.

Biographies

Bjarne Lill. Bjarne Lill is a Ph.D. student and researcher at the Department of Computer Science at the University of Innsbruck, Austria. His research interests include information security, risk management and applied information security, assessment and implementation in the context of small and medium-sized enterprises. He works in close cooperation with industry partners and other research institutions as part of research projects.

Clemens Sauerwein. Clemens Sauerwein is Assistant Professor at the Department of Computer Science at the University of Innsbruck, Austria. His research interests include information security risk management, cyber threat intelligence sharing, empirical studies in the field of information security and information systems. He works in close collaboration with industry and transfers his results into practice as a consultant and member of several security interest groups.

Nico Mexis. Nico Mexis was born in Bad Reichenhall, Bavaria, Germany, in 1999. He received two B.Sc. degrees in computer science and mathematics and the M.Sc. degree in computer science from the University of Passau, Passau, Bavaria, Germany, in 2021, 2022, and 2023, respectively. As a student assistant, he has also published several articles in the framework of the DFG PUFMem and NANOSEC projects between 2019 and 2023. Since 2023, he is working as a research assistant at the Chair of Computer Engineering at the University of Passau under the supervision of Prof. Dr. Stefan Katzenbeisser. His current research project is CySeReS-KMU, in which he is researching new security technologies for small and medium-sized enterprises in supply chains. Mr. Mexis is a member of IEEE, ACM, and GI. For more information, see https://nmexis.me.

Karoline Langner. Karoline Langner received her Master's degree in Supply Chain Management from the University of Applied Sciences Upper Austria, Campus Steyr, in 2023. Since 2023, she has been involved as a research project manager in Austrian and European projects on supply chain risk management, resilience, and cybersecurity, including SOPHIE, CySeReS-KMU, and Resistant. Her current research includes supply chain resilience, cybersecurity, and the prevention of cascading effects in critical networks.