Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity

CARLOS ROMBALDO JUNIOR, INGOLF BECKER, and SHANE JOHNSON, University College of London, United Kingdom

Small and Medium Enterprises (SMEs) are pivotal in the global economy, accounting for over 90% of businesses and 60% of employment worldwide. Despite their significance, SMEs have been disregarded from cybersecurity initiatives, rendering them ill-equipped to deal with the growing frequency, sophistication, and destructiveness of cyber-attacks. We systematically reviewed the cybersecurity literature on SMEs published between 2017 and 2023. We focus on research discussing cyber threats, adopted controls, challenges, and constraints SMEs face in pursuing cybersecurity resilience. Our search yielded 916 studies that we narrowed to 77 relevant papers. We identified 44 unique themes and categorised them as novel findings or established knowledge. This distinction revealed that research on SMEs is shallow and has made little progress in understanding SMEs' roles, threats, and needs. Studies often repeated early discoveries without replicating or offering new insights. The existing research indicates that the main challenges to attaining cybersecurity resilience of SMEs are a lack of awareness of the cybersecurity risks, limited cybersecurity literacy and constrained financial resources. However, resource availability varied between developed and developing countries. Our analysis indicated a relationship among these themes, suggesting that limited literacy is the root cause of awareness and resource constraint issues.

CCS Concepts: • General and reference → Surveys and overviews; • Applied computing → Business-IT alignment; IT governance; • Security and privacy → Social aspects of security and privacy; Systems security; • Social and professional topics → Computing literacy.

Additional Key Words and Phrases: CyberSecurity, Cyber Security, Small and Medium Business, Small and Medium Enterprises, SMB, SME, Cyber Resilience

ACM Reference Format:

Authors' address: Carlos Rombaldo Junior, jr.rombaldo@gmail.com; Ingolf Becker, i.becker@ucl.ac.uk; Shane Johnson, shane.johnson@ucl.ac.uk, University College of London, Gower Street, London, United Kingdom.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2023 Copyright held by the owner/author(s).

Manuscript submitted to ACM

1 INTRODUCTION

More than ever, services are digitalised, and systems are interconnected. While this has clear benefits, the recent boom of internet-based business has led to an alarming rise in cybercrime [54]. In the early 2000s, cyberattacks mostly involved the distribution of viruses and worms with destructive intentions. However, in the past decade, attacks have evolved into large-scale data breaches and ransomware campaigns motivated by financial gains [54, 108]. More recently, we have observed a surge in sophisticated cyber threats from organised crime groups and nation-states [26, 55, 65, 79], making it more challenging for organisations to defend against such resourceful adversaries. As cyber-attacks increase in scale, attackers have shifted their attention from well-protected large organisations to Small and Medium Enterprises (SME) with less resilient defences [5, 52, 70, 85, 107].

This research synthesises knowledge from the expanding literature concerning SME cybersecurity, identifies gaps in this knowledge, and informs understandings of what might be done to bolster SME cybersecurity. It consolidates the challenges and constraints SMEs encounter, current cybersecurity measures they use and their efficacy, risks they face, and possible solutions to address those risks.

Reports have been showing increases in the number of successful cyber-attacks against SMEs [4, 5, 59, 107]. For example, according to the Verizon report, 58% of the attacks registered in 2019 targeted SMEs [60], and 43% of breaches had SMEs as victims [109]. The UK Federation of Small Business reported a daily rate of 10,000 attacks against SMEs based in the UK [28]. While these numbers are unsettling, the reality is expected to be worse as SMEs typically do not report suffered cyber-attacks [6, 56, 70]. Although the number of breaches and financial losses continues to soar, recent surveys suggest that SMEs remain unprepared [20, 57, 73, 111]. For example, a 2022 cybersecurity survey across UK businesses revealed that only 17% of its businesses undertook vulnerability audits [67]. Research suggests that the lack of preparedness amongst SMEs is due to their lack of awareness of the threats faced [55, 63, 65, 77, 94]. Conversely, researchers believe the problem lies in low-risk perception and prioritisation [4, 35, 60]. Other researchers attribute the problem to insufficient investments in cybersecurity [62, 73, 81] and poor cybersecurity literacy to establish defensive programs [5, 88].

Some readers might be wondering what SMEs are, and why should their cybersecurity should be researched in particular. To answer the first part, there is no globally adopted definition of what an SME is. Instead, researchers have been using various definitions, which makes comparison troublesome (see, section 4). This research employs the European Commission's version, which defines SMEs as any enterprise with up to 250 employees and EUR 50 million in revenue [27]. As for their importance, according to the World Bank, SMEs play a major role in global economies, representing 90% of worldwide business, over 50% of global employment and 40% of average national incomes [100]. In the US, they represented 99.9% of the country's 32.5 million businesses and accounted for 43.5% of the country's GDP (Gross Domestic Product) in 2020 [104]. The statistical office of the European Union [39] reported that in 2022, 99.8% of all enterprises in the 27 EU states were SMEs, with 90% being micro businesses (less than ten employees). SMEs employed 83 million people, the equivalent of 64% of total employment in the block, and were responsible for over half of regional turnover. Considering that SME development is a high priority for many governments, the World Bank estimates they will create 600 million new jobs by 2030. In developing countries, SMEs are responsible for 7 out of 10 job creations, yet they face greater financial challenges than those in developed countries.

Many governments and industries have launched initiatives to bolster SME cybersecurity. For example, the UK government issued the 'Small Business Cybersecurity Guide' [23]. Along the same lines, US agencies released manuals to instruct SMEs on how to improve cybersecurity practices [25, 40, 66]. The European Commission too has invested [36] in projects to foster the creation of cost-effective cybersecurity solutions and the creation of SME cybersecurity best practices [37]. These include as Geiger [45], which is a lightweight Cybersecurity framework tailored for SMEs [95]. The OECD (Organisation for Economic Cooperation and Development) issued a digital transformation manual for SMEs with an emphasis on cybersecurity [78], while the Global Cyber Alliance collates SMEs' cybersecurity best practices [47]. In 2017, The Europe Digital SME alliance designed the SME cybersecurity strategy to foster SME cybersecurity initiatives [38]. While promising, we found no evidence that any of these frameworks and guidelines have been implemented. Moreover, studies that have evaluated the applicability of existing practices and frameworks (including ISO-27001, ITIL, COBIT, and NIST CSF) have concluded that they remain unsuitable for SMEs [18, 21, 24, 33, 44, 51, 60, 81, 83].

For decades, the literature has focused on more prominent (large) businesses and provides extensive coverage of existing risks and mitigations. Yet, little is known about SME-specific threats and how they differ from those directed at larger organisations [20, 33, 52, 57]. Only in recent years has the study of SMEs become a field of inquiry. Figure 1 illustrates the rapid and intensified growth of research published in this field, an increase of over 800% in the past five years.

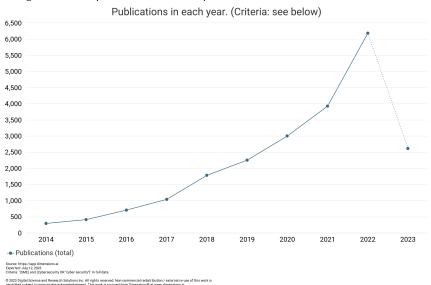


Fig. 1. Volume of published studies in the past decade. Data extracted from Dimensions.Al

Given the above, this study performs a systematic review (SR) of the literature to address the following research questions:

RQ1: What are the cybersecurity threats experienced by SMEs?

RQ2: What awareness do SMEs have about the threats they face?

RQ3: What is the uptake of cybersecurity controls by SMEs?

RQ4: Which cybersecurity frameworks apply to or can be tailored to SMEs?

RQ5: What challenges do SMEs face in adhering to existing cybersecurity frameworks and solutions?

This approach has several advantages over alternative strategies for synthesising existing literature, such as ad-hoc reviews. Conventional review methods are biased toward studies produced by authors known in the field or aligned with researchers' expectations. Systematic reviews have emerged as solutions to these problems [53, 101]. They rely on a transparent and reproducible protocol designed and agreed upon before data collection begins. This protocol describes the search terms to be used, the data sources to be searched and the steps involved in the extraction and synthesis of findings. As a result, the approach minimises authors' biases in selecting or prioritising studies that confirm their beliefs or interests [16, 53]. In principle, any two researchers following the same protocol should identify the same studies and arrive at the same conclusions when applying this method. SRs are commonly used in the field of medicine to synthesise experimental evidence on 'what works' to address a given problem [110]. However, they have also proven effective in synthesising evidence on emerging topics and dealing with diverse domains [15, 101].

This paper is structured as follows. The next section describes the protocol devised and subsequently presents the synthesised results. The final section discusses the implications of the findings, further research opportunities and limitations of the study.

2 METHODOLOGY

This section discusses the Systematic Review (SR) methodology employed. The method adheres to PRISMA-P [74] and Cochrane [53] frameworks, which are well-established standards for the conduct of systematic reviews. This methodology commences with the elaboration of the research questions (see introduction) using the PICO (Problem, Innervation, Comparison and Outcome) format [92]. This is followed by a description of the electronic databases to be searched, the specification of the search terms used, and the eligibility criteria employed to inform the selection of studies. Next, the data extraction and approach to evidence synthesis are detailed. Figure 2 provides an overview of the research method, while the subsections expand on each step.

2.1 Data Sources

Literature was searched for in computer science-focused search engines (ACM Digital and IEEE Xplore Digital) and more general academic search engines (ProQuest, Scopus, and Web of Science). To minimise the danger of publication bias, we included Google Scholar as a source for grey literature and research produced outside of traditional publishing and distribution channels. Examples of grey literature are industry reports, working papers, newsletters, government documents, and white papers [1]. Further details on content indexed by the databases used can be found in table 1.

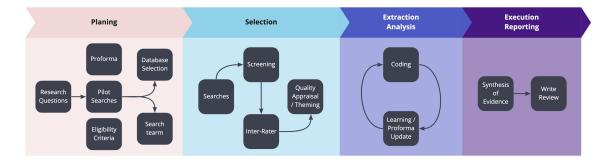


Fig. 2. Research Method Overview

Table 1. Database used to source studies

Specific academic	ACM digital library: a comprehensive database of full-text articles and bibliographic literature cover-			
databases	ing computing and information technology from Association for Computing Machinery publications			
	IEEE Xplore Digital Library: indexed articles and papers on computer science, electrical engineering,			
	and electronics from the Institute of Electrical and Electronics Engineers (IEEE) and the Institution of			
	Engineering and Technology			
Generic academic databases	ProQuest: Databases covered: Library & Information Science Abstracts (LISA), ProQuest Central			
	(Criminal Justice Database, Computing Database, Library Science Database, Science Database, Social			
	Science Database, Psychology Database and databases covering technology and social sciences,			
	ProQuest Dissertations & Theses Global			
	Scopus: Elsevier's abstract and citation database - Content on Scopus comes from over 5,000 publishers			
	and must be reviewed and selected by an independent Content Selection and Advisory Board (CSAB)			
	to be, and continue to be, indexed on Scopus			
	Web of Science: Conference Proceedings Citation Index, Science Citation Index Expanded, Social			
	Sciences Citation Index, Arts & Humanities Citation Index, and Book Citation Index			
Grey Literature	Google Scholar: articles, theses, books, abstracts and court opinions from academic publishers,			
	professional societies, online repositories, universities and other websites.			

2.2 Search strategy

The search query comprised two parts, both refined through pilot searches. The first was used to identify studies related to cybersecurity, while the second located studies with an emphasis on SMEs. Pilot searches returned many irrelevant studies when the cybersecurity and SME terms were searched independently. The best results were found when both terms appeared up to a few words apart. In other words, when searching for the co-occurrence of these terms rather than just their appearance. For this reason, the operator 'NEAR/8' was used to specify that both terms must appear up to eight words apart. Question marks were used to determine a single unknown character and match variations such as 'cyber-security', 'cybersecurity', and 'cyber security'. The following example illustrates the search query used:

```
( 'cyber?security' OR 'information security' OR
  'digital security' OR 'threat' OR 'cyber?threat' OR
  'cyber resilience' OR 'it security' OR 'data security' )
NEAR/8
```

```
( ('SME' OR 'SMME' OR 'SMB') OR
  ('small' OR 'medium' or 'micro') NEAR/2
  ('business' OR 'enterprise' OR 'organi?ation') )
```

The defined search query had to be modified to accommodate the syntax supported by each database search engine. For example, the ACM Digital library offers no support for the operator NEAR, which had to be replaced by the 'AND' operator. Moreover, as is typical with systematic reviews, the query had to be limited to titles and abstracts; otherwise, it would have returned hundreds of thousands of additional (irrelevant) studies. Similarly, the ProQuest query leveraged the 'Not Full Text' (NFT) operator to match everything except the full text. The Scopus search engine did not support the operator NEAR. Instead, a similar 'PRE' function was used. Web of Science could not parse '?' so the query had to be modified to include term variations manually. Google Scholar results were limited to the first fifteen pages as subsequent pages no longer provided results relevant to the topic.

2.3 Eligibility criteria

The screening phase was divided into two parts. The first involved the assessment of study titles and abstracts, while the second involved a full-text review. The following criteria informed eligibility decisions based on title and abstracts.

- (1) To ensure the relevance of the literature reviewed to today's SMEs' technological context, articles had to be published on or after January 1st, 2017. This threshold was selected as it coincided with the growth in cloud adoption [96, 97] and the forced digitalisation and BYOD deployments propelled by the Covid-19 pandemic [41, 48, 90]. Combined with a surge of publications in 2017 (figure 1) and the expectation that research is cumulative, we judged the last five years to be an adequate time frame.
- (2) Only literature that was either publicly available or could be obtained via UCL's (University College London) library was included.
- (3) Only literature published in English was included.

To measure personal bias and coder drift, we calculated the Inter-Rater Reliability (IRR) using the Prevalence Adjusted Bias Adjusted Kappa (PABAK) statistic [19]. Two researchers independently screened a random sample (n=52) of the titles and abstract results [89]. Outcomes were compared, and any differences (n=4) were afterwards discussed and resolved. The IRR coefficient was 0.846, which indicates 'almost perfect agreement' according to the PABAK formula [19].

For each study that met the inclusion criteria during the title and abstract screening, the full text was obtained, read and assessed based on its methodological and thematic focus. Studies were included if they met the following eligibility criteria:

(1) Several cybersecurity studies mentioned SMEs; however, only those that explicitly discussed SME cybersecurity were included in the review.

- (2) Studies must have thematic relevance. This is, studies must mention cybersecurity threats, controls or solutions to qualify. Themes emerged from pilot searches and were updated during the screening. Namely: Cybersecurity Awareness, Behaviour or Knowledge Gap; Data Security and Privacy; Cybersecurity Incidents and Response; Information Security Management Frameworks (ISMF); IT Security, including Bring Your Own Device (BYOD), Internet of Things (IoT), Cloud, Infrastructure and Network Security; Risks Assessment & Management; Supply-chain Security; Threat Intelligence and Cyber Resilience.
- (3) Studies had to present a clear and detailed methodology section that would enable an objective assessment of their conclusions.

2.4 Data Collection

All matching studies were exported into Research Information Systems (RIS) format files and subsequently imported into Rayyan [80], a specialised platform for systematic literature reviews, where the initial screening took place. As Google Scholar does not include abstracts when exporting results, its bibliography had to be imported on Mendeley for metadata lookup and then imported into Rayyan. None of the database exports contained the full texts. As such, studies filtered in the first screening stage were exported from Rayyan into Zotero [114], which facilitated retrieval of the full-text PDFs. Abstract and title screening was managed using Rayyan, while full-text screening was completed using Zotero. Not all full texts were available under open-access licences or through UCL's library; consequently, these studies were excluded. Further details on the volume of included and excluded studies are discussed in the results section. Studies were read and assessed using the eligibility criteria. Finally, results were exported into NVIVO using the RIS format, with content PDF and theme labels. At this point, we discovered that whenever a study contained multiple labels (themes), Zotero merged all labels into one, compromising the thematic assignment. To overcome this limitation, we developed an ad-hoc script [22] to split merged labels. The extracted data and the full-text PDF were exported, using the RIS format, into NVIVO, where the full-text coding took place. Codes were initially based on, but not limited to, a Proforma, detailed in the next section.

2.5 Data extraction and synthesis

A Proforma was produced from pilot searches and sampled studies to assist with data extraction. It consisted of a predefined set of relevant information to be extracted from each study, as follows:

- (1) Year of publication
- (2) Theme (as per inclusion criteria)
- (3) Study type (case study, systematic review, empirical, quantitative/qualitative, design proposal, industry report, etc.)
- (4) Data collection method (observation, surveys, or experimentation)
- (5) Size of sampled data (individuals and organisations)
- (6) Coverage (geographic, industry and socio-economic)
- (7) Discussion of existing cybersecurity frameworks

- (8) What motivated the study
- (9) Conclusions and recommendations
- (10) Limitations, as stated by the authors

We found only a limited number of studies providing quantitative data. Therefore, we opted for a qualitative approach to synthesis, combining elements of content and thematic analysis. Content analysis consists of the categorisation and classification of data according to its objective meaning and measurable attributes. In contrast, thematic analysis represents a more subjective approach, with an emphasis on the interpretation and context of the data, making it a more subjective and nuanced approach [16, 105]. Qualitative analysis identifies patterns in two ways: inductively (bottom-up) or deductively (top-down). With the deductive method, data are coded according to a predefined set of themes/codes to answer already established research questions. Conversely, with an inductive approach, research questions and themes emerge during the coding process. The deductive method provides in-depth knowledge of existing themes, whilst the inductive offers breadth by allowing themes to emerge during data analysis. Here, we applied a mixture of inductive and deductive methodologies, referred to by Braun and Clarke as theoretical thematic analysis [16]. To do so, a predefined set of themes was derived through an initial literature search. During the data extraction process, existing codes evolved from arising patterns and new codes were added in an iterative style until theoretical saturation was reached (i.e., no new themes emerged). The first author conducted the data extraction, which was subsequently reviewed and discussed by all authors. This led to a well-defined code book with clear agreed definitions. We do not report inter-rater agreement scores, as they are inappropriate in thematic analysis [17].

3 RESULTS

Searches were carried out in September 2022 and returned 916 records. Of these, 243 were duplicates, and five were unavailable in English; therefore, both were excluded. The title and abstract screening resulted in the inclusion of 358 studies and the exclusion of 310 that did not match the eligibility criteria. Furthermore, 38 results were excluded because their content was unavailable through the UCL institutional library. From the 275 studies that made it to content screening, 198 were excluded based on the eligibility criteria due to inadequate research or reporting standards (a point we discuss later). Consequently, 77 studies were included in the final scope for data extraction. Figure 3 illustrates the number of studies involved at each review stage.

The data extraction and thematic analysis resulted in the identification of 44 high-level themes. Each theme has a series of sub-themes representing more specific discoveries within the subject. Some of these topics (themes) have been continuously discussed in the literature with little to no evidence of new research being conducted to test their studies (e.g. within the last five years). To identify these perpetuating topics, we subdivided themes into driver and conclusion classes. Driver themes refer to knowledge from previous literature that motivated, justified, or drove the study but that were not tested in a particular study. Conclusion themes are those which studies have investigated and (re)tested the topic, advancing the state of knowledge. This classification was deemed important because behaviour and technologies have changed over time, and it should not be assumed that older discoveries have the same relevance in modern contexts.

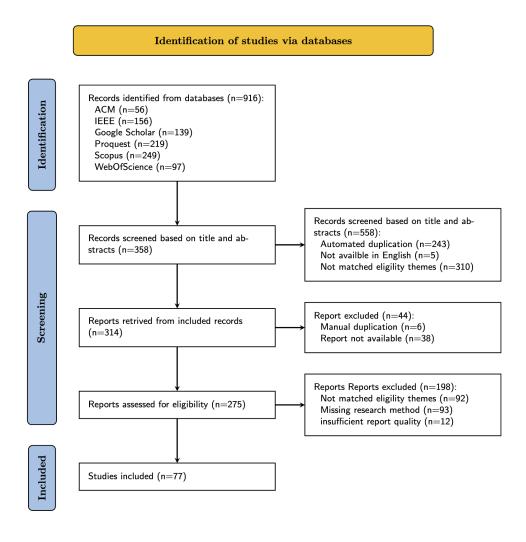


Fig. 3. PRISMA chart depicting stages and results

Many of the 44 themes had only a few mentions in the literature. To concentrate on more significant discoveries, in this article, we focus on the themes that occurred in at least ten studies. Table 2 lists the high-level themes and their frequency of occurrence (number of studies) for drivers, conclusions, and citations to the studies that discussed them. The cells of the table are shaded based on the number of studies from which each theme emerged. The higher the frequency, the darker the colour. A complete table, including sub-level themes and themes with lower frequency, is available in our open science folder (https://osf.io/ps7xy/).

Table 2. Synthesised Themes

Synthesised Theme	Drivers	Studies (Driver)	Concl.	Studies (Conclusion)	Total
Lack of awareness	23	[4] [8] [9] [10] [11] [21] [32] [35] [44] [56] [59] [60] [63] [64] [73] [76] [81] [85] [87] [86] [94] [111] [113]	19	[4] [5] [6] [10] [51] [52] [55] [60] [62] [75] [77] [79] [85] [87] [86] [99] [102] [111] [113]	34
Limited literacy	20	[4] [5] [8] [9] [10] [12] [13] [18] [24] [29] [44] [51] [59] [64] [70] [87] [86] [88] [111] [112]	11	[6] [32] [52] [73] [75] [79] [85] [98] [102] [111] [113]	30
Under-funded and resource- constrained cybersecurity programs	19	[4] [10] [12] [13] [21] [24] [35] [51] [52] [64] [71] [73] [81] [82] [85] [87] [86] [111] [112]	12	[5] [6] [32] [51] [52] [59] [60] [62] [79] [98] [102] [107]	29
Literature overlooked SMEs specific needs	21	[4] [5] [6] [8] [12] [20] [31] [32] [51] [52] [56] [58] [73] [76] [79] [81] [84] [87] [86] [107] [113]	7	[5] [6] [10] [18] [60] [83] [98]	26
Lack of tailored solutions and frameworks	20	[4] [7] [12] [21] [20] [24] [51] [59] [61] [70] [71] [76] [79] [81] [82] [83] [85] [87] [86] [107]	9	[51] [60] [63] [81] [83] [87] [98] [107] [113]	24
Low risk perception	14	[4] [6] [12] [35] [44] [56] [58] [60] [71] [87] [86] [94] [112] [113]	15	[4] [6] [9] [32] [52] [60] [62] [73] [79] [87] [86] [93] [94] [102] [113]	22
Rising cyberattacks against SME	19	[4] [5] [8] [12] [13] [20] [32] [52] [56] [59] [64] [70] [73] [81] [94] [98] [107] [111] [113]	2	[29] [94]	20
Overwhelmed sparse or non-existent cybersecurity leadership	10	[3] [5] [10] [13] [24] [44] [64] [69] [70] [73]	13	[6] [13] [21] [32] [52] [62] [69] [73] [79] [85] [94] [98] [111]	20
Increasing financial loss due to cyberattacks	15	[4] [5] [6] [9] [31] [32] [35] [52] [55] [70] [73] [83] [88] [99] [102]	2	[5] [86]	16
Cloud adoption minimises cybersecurity challenges	9	[21] [32] [41] [58] [59] [70] [73] [82] [93]	6	[3] [4] [5] [6] [41] [111]	14
Poor security operations	6	[6] [51] [58] [90] [102] [113]	8	[21] [30] [32] [56] [77] [87] [98] [113]	13
Risk awareness improve cybersecurity behaviour	2	[85] [88]	9	[5] [52] [62] [75] [84] [85] [88] [94] [107]	9
Legislation and informative content improve cybersecurity	5	[10] [35] [44] [56] [94]	5	[5] [20] [55] [88] [94]	9

The following sub-sections provide a discussion of each theme. Discussions begin with an overview of the topic and a comparison of driver and conclusions themes, followed by details of how the theme emerged from studies.

3.1 Lack of awareness of cybersecurity risks

The *lack of awareness of cybersecurity risks* emerged as the most frequent theme in the literature. It was discussed in 23 studies as a motivation (driver) for research, while 19 studies presented novel findings (conclusion) regarding this theme, both further discussed later in this section. This profile shows that recent studies continue to suggest that SMEs lack awareness of cybersecurity threats. While there is consensus in the literature about a *lack of awareness of cybersecurity* being a problem, a comparison of how driver and conclusion themes evolved made it evident that discoveries changed over time. For instance, research concerned with decision-maker awareness has declined: it emerged as a driver in five studies [4, 11, 64, 94, 113], but was a conclusion in only two [6, 62]. At the same time, research concerned with employees appears to have remained stable, being discussed as motivation in three studies [35, 59, 64] and with original findings being presented in three different studies [10, 55, 102].

Several studies concluded that employees were aware of cybersecurity dangers, but because their leadership was not, cybersecurity initiatives were not prioritised or were ignored [4, 6, 62, 64, 94, 113]. Conversely, five empirical studies [35, 55, 59, 64, 102] concluded that only leadership and tech departments had awareness and that this was not propagated to the remainder of the organisation. Of these studies, one article suggested (as a conclusion theme) that this situation made SMEs more vulnerable to phishing attacks [55].

A *lack of awareness of existing solutions* has also gained attention in the literature. It emerged as a motivation in one study [81] and as a conclusion in five others [5, 52, 86, 87, 99]. Each of these studies suggested that SMEs could not establish effective cybersecurity defences because they did not employ available solutions and that this was because they were simply unaware of them.

A *lack of awareness of digital assets* (e.g. infrastructure, customer data or digital monies) surfaced only as a finding, suggesting that it is a recent discovery. Three studies revealed that SMEs were aware of such threats, but because they underestimated their asset value, they perceived themselves as unlikely targets of cyber-attacks and considered their primary defences 'good enough' [79, 102, 111]. A *lack of awareness of regulatory cybersecurity requirements* (a.k.a. compliance) emerged as a driver in two studies [76, 87]. However, no research was identified that provided new findings regarding this topic. In addition to digital attack vectors, a *lack of awareness of non-technical threats* emerged solely as a conclusion in one study [75]. According to this research, humans became one of the main vectors for data breaches, because attention was focused on technological controls against cyber threats at the cost of disregarding human errors.

Various studies that surveyed SMEs revealed that increasing cybersecurity awareness amongst employees increases the likelihood of adopting appropriate security behaviours (self-reported and measured), thereby improving the organisation's cybersecurity posture [5, 52, 62, 75, 85, 88, 94, 107]. A systematic review by Van Haastrecht et al. summarises this nicely: 'Furthering human knowledge and improving the technical cybersecurity posture of an SME go hand-in-hand' [107].

It is worth noting that multiple studies have suggested that SMEs are not fully aware of the cybersecurity risks they face [4, 6, 10, 51, 55, 60, 62, 77, 79, 85, 102, 113], or the solutions available to them [5, 52, 86, 87, 99]. However, many of these studies failed to enumerate and specify the risks, threats, or solutions they referred to.

Instead, they often grouped various classes of risks (e.g., internal threats, ransomware, phishing attacks) under the umbrella term 'cybersecurity risks'. Similarly, solutions were broadly labelled as 'cybersecurity solutions' (see discussion section 4).

3.2 Limited Cybersecurity Literacy

To clarify the terminology employed between *lack of cybersecurity awareness* and *limited cybersecurity literacy*: the former is about not knowing of the existence of cyber-risks and -threats, while the latter is concerned with one's competence and domain knowledge in cybersecurity.

Limited cybersecurity literacy too emerged as a recurring theme in the literature; it surfaced as a motivation in a quarter of the articles reviewed (n=20) and was corroborated in 11 studies. Despite being frequently discussed, most studies mentioned it generically, failing to pinpoint which cybersecurity domain knowledge was missing and to specify which roles were illiterate. Consequently, only a few sub-themes emerged within this subject, highlighting the need for more comprehensive and targeted research to investigate shortfalls in this type of literacy.

Research motivated by this theme referred to previous discoveries suggesting that SME leaders and decision-makers were the ones presenting limited literacy on cybersecurity [4, 12, 13]. One study referenced previous research which suggested that insufficient cybersecurity proficiency among SME leadership has led to inefficient strategies and scarce investments in cybersecurity initiatives [4]. Studies indicated that SMEs' limited cybersecurity literacy resulted from unprepared cybersecurity professionals who failed to engage with other employees. This lack of preparedness resulted from a combination of a lack of higher education and available training curricula not matching industry needs. This emerged in the conclusion of one study [102] and as a motivation for another two studies [29, 63].

Research using interviews to investigate levels of cybersecurity awareness across SMEs in the North American medical industry reported that SME personnel literacy was directly related to the organisation's financial capacity; the more prosperous the SME, the higher its overall literacy level [32].

3.3 Under-Funded and Resource-Constrained Cybersecurity Programs

The under-invested and resourced-constrained cybersecurity programs theme emerged as a barrier to effective SME cybersecurity defences in 29 studies. This theme surfaced more frequently in the introduction of studies (n=19), but original findings were reported in a substantial body of literature (n=12), indicating that this issue is still being researched. Nonetheless, discussions were often quite generic, resulting in a lack of detail and a small number of sub-themes compared to other themes; a situation that is further discussed in section 4.11.

In their study, motivated by previous research, Rae and Patel argued that SMEs only funded cybersecurity activities after they suffered a cyber-attack [86]. In introducing their work, two other studies argued that previous work has suggested that SMEs often have financial resources but fail to allocate them to cybersecurity functions [13, Manuscript submitted to ACM

73]. Another study introduction implied that a shortage of funds restricted SMEs' access to cybersecurity solutions and external support [13]. Although the mentions above emerged as driver themes, they are consistent with the findings of Heidt et al.'s survey of UK-based SMEs. This study found that SMEs' cybersecurity functions were underfunded due to inadequate budget planning and unawareness of available financial subsidies from governments and external parties. This same study reported that SMEs invested less than £1,000 a month on cybersecurity, despite recognising their unpreparedness against cyber threats [52]. Another UK study of SMEs found (through interviews) that cybersecurity investments did not scale with company size and investments were capped at £10,000 per annum [79]. Continuing with empirical research conclusions, an investigation of SMEs in developing countries attributed the under-investment problem to the intangible benefits and unclear returns (of investments) aspects of cybersecurity functions [60]. This discovery relates to the *leadership limited cybersecurity literacy* theme, discussed in section 3.2.

Despite the literature uniformly recognising under-investment in cybersecurity as an endemic pitfall for SMEs, only one study [4] emphasised the need for guidance to inform on adequate levels of financial allocation. In other words, the literature often claims SME cybersecurity to be underfunded but does not provide recommendations on what sufficient levels of investment look like.

3.4 Literature Overlooked SMEs' Specific Needs

Many studies (n=26) claimed gaps in the cybersecurity literature lacked focus on SMEs. *Literature gaps* emerged in the introduction of 21 studies and were discussed in the conclusion of seven studies. Novel findings surfaced from two perspectives: areas requiring further exploration and deficiencies related to reporting standards. The discussion section delves into the latter perspective.

Six studies' introductions cited previous work suggesting that existing recommendations were not actionable by SMEs due to being either theoretical or too complex for short and low-literate SME cybersecurity personnel [4, 20, 56, 87, 107, 113]. Additionally, one of the papers mentioned in its introduction that the literature remained impractical and lacked sufficient evidence to support conclusions drawn [56]. In introducing their work, other studies highlighted gaps in the literature pertaining to topics including unclear implications of cybersecurity breaches [31]; data privacy management for SMEs [58]; specific challenges faced by SMEs based in developing countries [76, 113]; existing research focused on IT (Information Technology) but did not explore IoT [113]; Inadequate attention to human factors in SME cybersecurity [32, 86, 87]; exploring supply-chain effect particular to SMEs [31]; investigating cyber-risk management requirements and challenges for SMEs [5, 6, 113]; and, a lack of coverage on Information Security Management Frameworks (ISMF) in the context of SMEs [84].

As for novel findings, research surveying UK SMEs urged for existing solutions to offer more adaptability and lightweight versions that are sensitive to the constraints faced by SMEs [107]. This same study also reported that SME leadership had little interest in participating in surveys, which limits research development in the field. For instance, low responses (<1%) limited the possibility of quantitative research.

A systematic review concluded that the recommendations provided were not actionable by SMEs [10]. A survey of SMEs and large corporations reported an unmet need for a cybersecurity measurement framework specially

Manuscript submitted to ACM

focused on SMEs [83]. Three empirical studies confirmed the need to investigate the specific needs and challenges of SMEs in developing countries [5, 6, 60]; a point that also emerged in the introductions of two papers [76, 113]. Combined, all five studies implied that the existing literature focused predominantly on developed countries, and their findings were inapplicable to SMEs in developing countries. Research from Chandra and Sadikin suggested that challenges faced by SMEs in developing countries were intensified by limited access to funds, government support, cybersecurity literacy, and the cost of solutions [24].

3.5 Lack of Tailored Solutions and Frameworks

The literature frequently suggests that existing cybersecurity solutions are not suitable for SMEs. However, while many studies (n=20) highlighted this point to motivate their research, novel findings were only reported in nine papers.

The studies that motivated their research on this issue (but did not report novel findings) disagreed on the challenges and reasons for a lack of tailored solutions and frameworks. For example, Alghamdi et al. quoted previous research attributing the problem to resource-intensive implementation requirements of existing solutions [7]. Four studies presented more details on their motivation, stating that existing solutions were overly complicated for SMEs' constrained resources (human, financial, and silicon) [7, 12, 20, 61]. Only one study collected data and reported findings that supported this conclusion [87]. According to all of these studies, solutions were designed to address the needs of larger organisations, and given the different requirements and capabilities of SMEs, solutions were considered unfit.

In their study, Chandra and Sadikin findings suggest that SMEs must overcome many barriers, such as domain knowledge, solution complexity, infrastructure requirements, organisational changes, and financial costs [24]. Furthermore, studies concluded that challenges were intensified in developing countries due to a lack of adequate technological infrastructure, lower levels of literacy, and higher costs of acquiring new technologies [24, 60, 76].

Two additional studies reported that the SMEs they studied insisted on implementing unsuitable solutions, which caused more problems than they solved [107, 113]. These failed implementations led to the inefficient use of resources (human, financial and silicon), loss of confidence and the further de-prioritisation of cybersecurity initiatives. A contrasting position emerged from Tam et al. findings. They suggested that solutions have become suitable for SMEs. However, their deployment and operation remained unsuccessful due to SME employees' limited literacy and unsuited priorities [98]. Similarly, Van Haastrecht et al. conclude that instead of creating new solutions, the industry should focus on tailoring existing ones to make them suitable for SMEs [107]. However, it should be noted that this latter conclusion was not supported by empirical data.

3.6 Low Perception of Cybersecurity Risks

Perception and awareness may have overlapping meanings, and to mitigate this confusion, we employed the following definition. Lack of awareness is about not knowing a topic's existence. In contrast, low perception involves understanding its existence but not paying enough attention.

The theme *low perception of cybersecurity risks* served as motivation for research in 14 studies, and for novel findings in 15. This consistent emergence of drivers and conclusion classes (re)confirms the relevance of this theme in the literature.

This theme emerged from distinct perspectives. In the first perspective, many studies suggested that SMEs did not pay attention to cybersecurity risks due to the misconception that they as businesses are too small and irrelevant to be targeted by cyber-attackers. This argument was used to introduce eight studies [4, 6, 32, 35, 60, 73, 94, 112] and emerged from the findings of six empirical studies [32, 60, 73, 79, 86, 94]. These findings suggested that SMEs believed attacks were concentrated on larger organisations and that their defences were adequate. The second perspective taken was that SMEs paid limited attention to cybersecurity because of a low perception of the benefits of defence [87]. Another (third) perspective was that SMEs overlooked cybersecurity because they underestimated the monetary value of their digital assets (data and infrastructure) [102]. A fourth perspective surfaced in the introduction of three studies [6, 58, 113] which cited reports that SME leadership exhibited lower levels of perception of cybersecurity risk, which impacted upon their subordinates [6, 58, 113]. Similar arguments emerged in the conclusions of five studies, which suggested that low perceptions of risk amongst decision-makers result in the inadequate prioritisation of cybersecurity defences [6, 52, 58, 62, 73, 94, 113]. They recommended that cybersecurity initiatives should begin from top management; otherwise, employees would not prioritise it. Moreover, without leadership prioritisation, cybersecurity functions depended on small and often unrelated teams and were generally downplayed. A fifth perspective materialised from a survey of SMEs in the UK. In this study, it was reported that 75% of organisations did not accurately perceive how (un)prepared their cybersecurity defences were. The same study indicated a sharply rising cost for SMEs to recover from cyber-attacks. Yet, the perception gap remains significant compared with larger entities [86]. A sixth perception was that SMEs perceived fewer cybersecurity risks when operating on cloud infrastructure. This discovery was observed in the conclusions of two studies [86, 93]. Finally, the seventh perspective stemmed from Ahmed and Nanath suggestion that the reasons behind the perception problem remain unknown in the literature [4] and consequently require further research.

3.7 Overwhelmed, Sparse or Non-existent Cybersecurity Leadership

More studies reported original results on this topic (n=13) than introduced it as a motivation for their research (n=10). These all concurred that the absence of a specialised and dedicated cybersecurity unit represented a barrier to SME cyber defences. As a result, cybersecurity responsibilities were delegated to other departments that already had other priorities and often had limited cybersecurity expertise.

Although twenty studies discussed this topic, only a few examined it in-depth. As a result, only two subthemes have emerged. The first, *competing priorities*, emerged from the motivations and conclusions of a single study [69] and the findings of another [62]. Both suggested that cybersecurity functions were carried out by unrelated teams with competing priorities. Building up to this argument, additional research indicated that allocating cybersecurity functions to leaders of unrelated domains resulted in overwhelmed managers with the accumulation of too many functions. This finding was discussed in the introductions of some studies [5, 24, 64] but also tested in empirical investigations [6, 13, 52, 58, 62, 94]. Moreover, Heidt et al. findings suggest that

under-literate cybersecurity managers required more time (than literate ones) to develop the function effectively. It is suggested in the literature that this combination of additional time requirements and competing priorities led to the further de-prioritisation of cybersecurity activities [52]. In one study, the analysis of interviews suggested that a conflict of interest was another reason for downplaying cybersecurity [79]. To explain, researchers concluded that the effectiveness of cybersecurity relied on the ability of the organisation to restrict insecure practices. However, the decision to implement such restrictions is compromised when the same manager owns both the security control and the function or practice considered insecure. For example, the same manager is responsible for restricting access to sensitive data, and at the same time, his team is the one accessing this same data. The second sub-theme emerged from the findings of a single paper [21]. In that study, the authors indicated that the success of cybersecurity initiatives depended on, among other factors, leaders' ability to propagate awareness, commitment and engagement with cybersecurity with their subordinates. This same study suggested that cybersecurity activities should be led by SME management teams. This finding correlates with the theme low cybersecurity risk perception.

3.8 Cloud Adoption Minimises Cybersecurity Challenges

While our search did not explicitly focus on cybersecurity risks associated with the Cloud, this theme emerged from 14 studies. It was observed as a motivator in the introduction sections of nine studies, and in the results and conclusion sections of six. In general, these studies found that SMEs perceive cloud adoption as an enabler in their cybersecurity journey.

For example, findings from an interview-based investigation of the UK SMEs' cybersecurity preparedness [111] and a survey of cyber threat perception across Hungarian SMEs [41] suggest that SMEs perceived fewer cybersecurity risks when operating in the cloud. In both studies, respondents felt that risks were taken care of by the cloud provider. This same argument was also used to introduce another two studies [32, 82]. At the same time, research suggested that while cloud adoption did address some of the risks, it introduced new ones, thereby shifting the cyber threat landscape. This issue was discussed in the introductory sections of three studies [41, 58, 59], and novel findings concerning this notion were presented in three others [4–6]. Alahmari and Duncan, who authored two of these studies [5, 6], suggested that SMEs perceived fewer risks because: a) they misunderstood the shared responsibility model, mistakenly assuming that risks were addressed by their cloud provider; and, b) they could not see the new risks introduced by outsourcing their infrastructure.

An interview-based study, this time investigating the impacts of computing virtualisation on SMEs, reported that cloud adoption improved systems availability and resulted in less frequent and shorter periods of outages [3]. Meanwhile, [93] cited previous research indicating that cloud adoption had increased SMEs' access to solutions and technologies. While none of the literature reviewed fully supported these hypotheses, a complementary view was brought by Ahmed et al. conclusion that SMEs reduced costs associated with infrastructure and cybersecurity by migrating their services to the cloud [3]. Equivalent statements were used to introduce another three studies [21, 70, 73], and a partially contrasting point emerged in the introduction to one study [113], which referred to previous research to indicate that cloud infrastructure was not affordable for SMEs in developing countries.

Moreover, other research suggests that SMEs still resist cloud adoption [59, 113]. One of these studies cited previous research showing that German SMEs have not yet adopted cloud-based technologies because of concerns about the cybersecurity readiness of these services [59]. In their survey of Middle Eastern SMEs' cybersecurity posture, Ahmed and Nanath reported a similar pattern of adoption but for different reasons. They found that 50% of respondents were still planning or not interested in using cloud computing [4].

3.9 Poor Security Operations

Thirteen studies suggested that SMEs have weaker cybersecurity defences than larger organisations. According to these studies, this is because SMEs often struggle to build robust and efficient security operations. Six of these studies were motivated by this theme, while eight provided new data about it.

To introduce their study, Rawindaran et al. quoted previous studies suggesting that SMEs put themselves at risk by deploying open-source software in an uncontrolled manner [90]. Analogous discoveries were used to introduce five studies, that SMEs were at risk due to uncontrolled deployments of IoT (Internet of Things) and personal devices (BYOD - Bring Your Own Device) [6, 51, 58, 102, 113]. Support for these concerns was supplied in three interview studies, which provided empirical findings to show that these devices (IoT and BYOD) were deployed without effective cybersecurity posture assessment and monitoring, creating exploitable paths to corporate networks and sensitive data held by the organisations [56, 77, 98]. Furthermore, one of these studies reported that SMEs used mobile phones as employees' primary computing devices [56]. The findings of another three studies indicated that SMEs struggled to maintain up-to-date inventories of their data and computing devices. This creates suboptimal cybersecurity as enterprises need a clear understanding of what they need to protect [21, 30, 113].

Finally, two other empirical studies reported that SMEs used outdated software without the necessary controls to detect and update patches [32, 113], while Douchek et al. found that SMEs stumble with cybersecurity because they fail to monitor the security posture of their digital assets (servers, systems and data) [30].

3.10 Risk Awareness Improves Cybersecurity Behaviour

As discussed in section 3.1, a *lack of awareness of cyber risks* has been recognised as a major hindrance to SMEs achieving adequate cybersecurity. However, this theme, *risk awareness improves cybersecurity behaviours*, emerged with an enhanced view of the awareness problem. It surfaced from the conclusions of nine studies and in the motivation of two of these studies. It is worth noting that although studies provided novel findings, they were limited in scope.

When investigating the success of SMEs' information security management programs, research concluded that the top priority should be given to initiatives focused on improving the organisation's cybersecurity awareness [5]. As per Alahmari and Duncan's words: 'Creating the best possible awareness programme might help to reduce the potential risks to acceptable levels. The threat to cybersecurity has been recognised as the main risk for SMEs; addressing

this challenge with protective measures is not enough. Importantly, what is required is increasing the awareness needed to develop suitable measures for these organisations'.

Mijnhardt et al. further suggest that augmenting knowledge sharing within the organisation is crucial to cybersecurity posture improvements. This suggestion entails comprehending the vital connection between cybersecurity and business processes. The absence of this understanding has been a consistent barrier to SME cybersecurity programs [72]. However, it is important to note that the research reviewed employed an interview methodology or used self-report surveys to estimate the effect of interventions intended to improve awareness on cybersecurity. As none used an experimental design, this limits the extent to which causal inferences can be made.

3.11 Legislation and Informative Content Improve Cybersecurity

The introductions of seven studies stressed the importance of region- and industry-specific legislation such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) to foster cybersecurity initiatives among SMEs. According to the cited research, the benefits of these regulations were more about their informative aspects than punitive directives. Specifically, the studies suggested that the existence of the regulations (as opposed to the content of them) promoted knowledge sharing between service providers and SMEs, which led to increased awareness and improved cybersecurity practices [44, 56, 59, 87]. Empirical support for this conclusion was provided in two studies [30, 113]. The ratio of studies that discussed these ideas (n=7) to those that provided recent empirical findings (n=2), however, suggests a gap in the literature that warrants further exploration.

Despite the benefits discussed, surveys of cybersecurity practices and the challenges encountered by SMEs from Indonesia [113] and Czech & Slovak Republics [30] suggest that the regulations themselves could be better tailored to SMEs by (for example) taking into account the limited resources available to these organisations.

The introduction to Rae et al.'s study quoted government initiatives that promoted cybersecurity standards for SMEs. These initiatives provided SMEs with the opportunity to offer services in the public sector on the condition that they established at least baseline cybersecurity practices. As an example of how governments are incentivising this, the UK government set a target for 2022 to procure at least 33% of all their contracts from SMEs [87]. A contrasting position emerged from a survey (conclusion) of SMEs in developing countries. Their findings suggested that compliance-driven efforts can negatively impact SME cybersecurity as baseline requirements may not be sufficient to protect the organisation, but they overshadow the need for more robust practices [60].

3.12 Remaining Themes

So far, this section explored the most commonly discussed themes in the literature, from which two themes remain to be addressed: the *rise in cyber-attacks against SMEs* and the *increasing financial losses due to cyber-attacks*. The discussion of these themes was mainly observed in the introductions to articles. Moreover, when they were Manuscript submitted to ACM

mentioned in the conclusion sections of studies, they were not based on new empirical findings. To illustrate, The former theme was discussed in the introduction sections of 21 studies, but empirical findings were only presented in a single article. The latter theme was discussed in the introduction sections of 19 studies, and novel findings were presented in only two articles.

4 DISCUSSION

This section begins by answering the research questions posed in the introduction of this article based on the findings that emerged in the review. It then provides a discussion of the state of research on SME cybersecurity, providing a holistic view of its maturity and a consideration of reporting standards, gaps, and knowledge that is perpetuated within the literature without new empirical support.

4.1 Cybersecurity Threats Experienced by SMEs

The first question, 'RQ1: What are the cybersecurity threats experienced by SMEs?', was not fully answered in the reviewed literature. Instead of focusing on threats, studies often focused on challenges that SMEs encounter in establishing cybersecurity defences. They suggested that SMEs were unaware of the threats and that existing solutions did not address SMEs' needs. Yet, none investigated or enumerated the threats faced by SMEs. Nor did they consider if and how they differ from those faced by larger organisations.

The search of grey literature identified a number of industry reports that focused on data breaches and which often attempted to forecast upcoming threats. However, it is important to note that these reports primarily concentrated on larger organisations and made no distinction between the threats faced by these organisations and SMEs. The grey literature also highlighted a class of services called *threat intelligence*, whereby companies monitor cyber-attacks happening in various industries and regions. This information is then aggregated to produce reports (behind paywalls) on attackers' motivations and techniques. This type of service is well described by the Gartner research institute: 'Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets' [43]. To our surprise, the systematic search did not identify any studies that discussed threat intelligence for SMEs in particular. However, a more specific search that focused on threat intelligence and SMEs identified a single study that advocated for an approach to threat intelligence that is tailored to SMEs [106]. In short, the review indicates a need for research concerning threats and threat intelligence in the context of SMEs.

4.2 SME Awareness of Cyber Threats

As for the second research question, 'RQ2: What awareness do SMEs have about the threats they face?' As just discussed, the literature on actual cybersecurity threats to SMEs is limited. Nevertheless, there is a substantial amount of research that has explored SMEs' level of awareness of the cybersecurity threats that they might face and the need to invest in reducing their risk.

As discussed in the theme *Lack of awareness*, 34 studies found that SMEs have insufficient levels of cybersecurity awareness, and this issue was widespread from employees to leadership. An additional nine studies reported a positive relationship between the levels of awareness expressed by employees of SMEs and their behaviour in terms of cybersecurity (see theme, *Risk Awareness Improve Cybersecurity Behaviour*). While most studies agreed that levels of awareness were inadequate, five studies presented a contradictory picture, suggesting that SMEs had awareness but that their approach to cybersecurity fell short for reasons including resource constraints and limited cybersecurity literacy [21, 32, 79, 85, 102]. While this alternative perspective was only explicitly discussed in a small number of studies, it is also supported by a larger number of studies that discussed issues associated with *Limited Cybersecurity Literacy* and *Under-Funded and Resource-Constrained Cybersecurity Programs* in general.

To summarise, nearly half (44%) of the studies reviewed discussed inadequate levels of awareness as a deterrent to cybersecurity in the context of SMEs. At the same time, there was a small number of studies which implied that limited literacy and resource constraints were the underlying problem (instead of awareness). Our view is that further investigation is required to understand the correlation between awareness, literacy and resource availability issues. These three themes were the most commonly occurring themes in the literature, yet the relationship between them is poorly understood. This situation is further discussed in section 4.5.

4.3 Cybersecurity Controls Practised

The third question, namely 'RQ3: What is the uptake of cybersecurity controls by SMEs?', was partially addressed in the literature. Many studies (n=52) surveyed SMEs, but their primary focus was the identification of challenges rather than cybersecurity practices. Consequently, their reports emphasised what SMEs lacked but not what they had done. Not a single study was found to investigate and report existing SMEs' cybersecurity controls. Notwithstanding this, we were able to identify some insights regarding SMEs' controls, at least the inefficient ones. Studies discussed in the themes Poor Security Operations and Overwhelmed, Sparse or Non-existent Cybersecurity Leadership highlighted issues associated with disorderly deployments of open-source software and insecure devices, and how these initiatives lacked dedicated ownership. However, these insights were limited, and it is evident that there is a need for further investigation into the uptake of cybersecurity controls by SMEs and how this differs from larger organisations.

4.4 Availability of Cybersecurity Solutions

In relation to the fourth and fifth research questions, 'RQ4: Which cybersecurity frameworks apply to or can be tailored to SMEs?' and 'RQ5: What challenges do SMEs face in adhering to existing cybersecurity frameworks and solutions?' respectively, we found 20 studies that investigated how existing solutions catered to SME needs. These studies unanimously concluded that existing solutions remain unfit. However, despite the substantial research that looked at this topic, none of the reports provided a list of existing solutions nor did they outline specifically how SMEs' needs were unmet. Instead, we encountered generic statements and sometimes theoretical assessments. Therefore, RQ4 remains unanswered, and there remains a knowledge gap regarding what changes are expected from solutions.

However, more insight was provided regarding RQ5. The same mentioned studies reported that SMEs struggled to implement solutions due to the requirement for highly-specialised domain knowledge, infrastructure requirements, organisational changes, solution complexity and increased financial costs. The literature also suggests that these challenges are intensified in developing countries due to further limitations associated with cybersecurity literacy and financial resources.

Moreover, about one-third (n=23) of the studies reviewed proposed custom solutions, tailored to SMEs [4, 18, 21, 26, 31, 35, 41, 42, 51, 52, 59, 61, 63, 70, 75, 82, 83, 86, 87, 99, 107, 112]. However, all of these proposals were either entirely theoretical or had not progressed past a limited initial feasibility study. No usable deliverables (documentation, software, source code, etc.) were made available, which severely limits the ability of others to take these ideas forward.

4.5 Overall model of SME cybersecurity dependencies

The themes discussed are not mutually exclusive, and the synthesis conducted during the review process enabled us to identify relationships between them. These connections are visualised in figure 4.

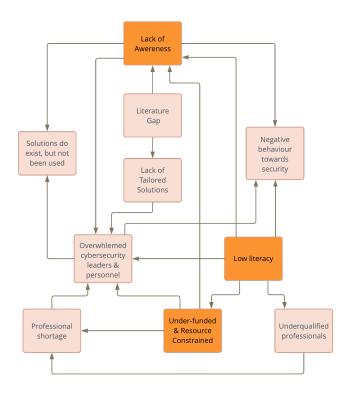


Fig. 4. Potential dependencies of emerged themes

The majority of papers concluded that a *lack of awareness* was the main reason for SMEs having ineffective cybersecurity initiatives. Our analysis however suggests that in many cases the source of the problems, including awareness, was *limited literacy in cybersecurity* and *constrained resources*. A few studies suggested that the *constrained resources* issue itself appears to be the result of *limited literacy*, as the necessary resources did exist, but they were just not allocated to cybersecurity [13, 52, 73]. We believe the issue of resourcing is quite complex and depends on many other factors, such as government support, the availability of subsidies, the geopolitical region and the industry the SME operates within, which is further discussed in an upcoming section.

As a consequence of the relationship between the *lack of awareness*, *limited literacy*, and *constrained resources* being poorly understood in the literature, research and interventions may have been misdirected by approaching these issues in isolation. For example, studies have investigated interventions to raise awareness among SME personnel, without considering whether resources (staff, tooling, time and finances) are available to allow them to address shortcomings in cybersecurity, should attempts at raising awareness be effective. Such a situation could lead to an increase in anxiety as staff are more aware but not supported in solving the newfound issues. More generally, raising awareness alone may be insufficient (and too simplistic) in the absence of adequate provisions regarding education, adequate time and investment. Being aware of risks is one thing, knowing how and having the means to address them is another. Research has been focused on the former, but without the latter, SMEs' cybersecurity initiatives remain unsuccessful.

Considering the aforementioned points, here we articulate a number of future research questions: Does raising awareness alone lead to improved cybersecurity? What is required to translate awareness into action? To what extent do resource constraints impact awareness? For instance, studies suggested that SME employees were overwhelmed and did not have adequate time to perform cybersecurity functions. Does giving them more time or fewer tasks improve cybersecurity performance in these SMEs? Can those involved learn from project management resource allocation? If more time is not the solution, how can we provide more structure to improve security task performance? Lastly, Is limited literacy the fundamental shortcoming of SME personnel? Can we state that awareness issues have resulted from a poor understanding of cybersecurity threats and their consequences?

4.6 Developed versus Developing countries

Many studies claimed that the literature was limited to SMEs situated in developed countries [5, 6, 60, 76, 113]. To examine this, we coded studies based on the geographic coverage of the SMEs studied, and our results unveiled a contradictory position. The reviewed literature covered 63 countries which are shown in figure 5. Studies targeted SMEs based in African, Asian, European, and Oceania developing countries, whereas American (Central, South, and North) SMEs remained unexplored. The highest coverage was in Germany and the UK (nine studies each), followed by Saudi Arabia (seven studies) and Indonesia (five studies).

To conclude, our data revealed the existence of substantial research pertaining to developing countries, thereby rejecting the hypothesis that studies are limited to developed nations. Nonetheless, certain developing regions, including South America, have yet to be investigated in the literature. Considering the unique geopolitical Manuscript submitted to ACM

characteristics of these regions, further research is required to understand if and how the challenges faced by SMEs in these locations differ from those in other developing regions.



Fig. 5. A heat map gauging the geographic region covered by reviewed literature. This data is available at (https://osf.io/ps7xy/).

4.7 Defining SMEs

To synthesise evidence for a particular type of organisation, it is important that there exists a clear and widely adopted definition of what that type of organisation is. Unfortunately, different definitions of SMEs were found throughout the literature.

Most studies relied on definitions provided by local governments and regional entities. However, these definitions varied. For instance, the Saudi Arabia Small Business Administration (SBA) and Census Bureau defined SMEs as any organisation with less than 500 employees [9]. At the same time, the South African Business Act classified an SME as any organisation with up to 200 employees, with no more than ZAR 10 million invested in assets and a turnover of up to ZAR 64 million, equivalent to 0.54 and 3.3 million dollars, respectively [75]. In comparison, the US Business Association categorised SMEs as organisations with up to 500 employees and a turnover between 7 and 250 million dollars, depending on the industry [104]. The European Commission [27] and the UK [50, 91] government categorise organisations with up to 10 employees or 2 million euros as micro businesses, while those with 50 employees or 10 million euros turnover and 250 employees or 50 million euros classified as small and medium enterprises, respectively. More global definitions were encountered, unfortunately, with no evidence of use. For example, the United Nations [103], IMF (International Monetary Fund) [14], and the OECD (Organisation for Economic Cooperation and Development) [78] defined micro organisations as those with up to 9 employees, while those with 49 and 249 employees were considered small and medium. These are just examples of how established definitions varied. In addition, we discovered studies that applied their own definitions. For instance, research investigating small German organisations defined SMEs as any business with up to 100 employees [102].

Differences in the definition are important beyond conceptual concerns. For example, when considering financial constraints, these are likely to vary for businesses with a turnover of USD 250 million and those with EUR 50 million or ZAR 64 (USD 3.3) million. The same applies to the number of employees.

4.8 Costs to recover from cyber-attacks

While there was a consensus in the literature regarding the increasing number of cyber-attacks against SMEs and associated recovery costs, estimates of the expenses varied substantially. For instance, Tam et al. suggested that micro SMEs lost an average of 14,000 dollars per year with data breaches [98], while White et al. estimated that 229,000 dollars were required to recover from a single attack [111], and Carías et al. reported that recovery costs were between 16.4 and 14.1 million euros [21] per attack. These numbers also differ from industry reports. For example, IBM publishes an annual cyber breach survey with businesses of all sizes. In the 2022 edition, they reported that it costs an estimated 4.35 million dollars for an SME to recover from a data breach. Smaller figures were reported in the 2023 edition of the UK (annual) cyber breaches survey, which estimated that recovery costs ranged between one and five thousand pounds, equivalent to 1.3 and 6.5 thousand dollars, respectively [68].

As previously mentioned, SME definitions portray turnovers substantially lower than some of the estimated costs required to recover from cyber-attacks. This disparity can be enough to put SMEs out of business, and they often do. In fact, according to the National Cyber Security Alliance (NCSA) [2], 60% of SMEs go out of business within six months of a breach. At the same time, Raineri and Resig reported that 43% of SMEs suffered at least one data breach in 2019, from which 60% went out of business in the following semester [88]. Similar findings are reported by Carías et al., who found that 66% of the 250 SMEs they surveyed closed after a successful cyber-attack [21]. The UK cyber breach survey reported that 32% of micro and 59% of medium organisations suffered at least one breach within the past 12 months of the report [68].

In summary, the literature presented consistent numbers regarding the frequency of cyber breaches experienced by SMEs. However, there was a noticeable disparity in estimates of recovery costs. This divergence could be attributed to several factors. Firstly, variable sample sizes and sample distributions among reports were noteworthy. Academic research investigated a smaller number (tens) of businesses, while industry and government surveys encompassed thousands or even tens of thousands of organisations. Secondly, apart from the UK cyber breach survey [68], most government and industry reports combined SMEs and larger organisation data; consequently, their insights can be misrepresented. Thirdly, as pointed out by Alahmari and Duncan, Gafni and Pavel, Ikuero and Zeng, Ikuero and Zeng, McLilly and Qu, White et al., SMEs under-report cyber-attacks which impacts estimates of costs as well as prevalence [6, 44, 56, 56, 70, 111].

In our view, there is a clear need for more precise estimates of the impact of cyber-attacks and the costs associated with recovery, in the context of SMEs. Better estimates would likely help to raise awareness of the importance of cybersecurity for SMEs.

4.9 Standards of Reporting in the Literature

Variability in what was reported and how it was reported in the cybersecurity literature posed one of the biggest challenges to extracting findings for this review (see also [56, 84, 98]). For example, two-thirds (n=51) of reviewed studies employed interviews and surveys in their research. However, these studies invariably failed to report important information, such as the approach used to sample SMEs, characteristics of the employees interviewed (e.g. role and tenure), and the data collection method used (e.g. structured or open questionnaires). Without such details, it becomes difficult (or impossible) to replicate these studies or to assess the validity/generalisability of their findings. This contrasts with more mature domains, such as the medical sciences, which have developed formal standards for reporting findings from empirical studies. For instance, the Consolidated Standards of Reporting Trials (CONSORT) defines a minimally acceptable standard for studies employing trials [34]. Consort was established in 1995 and has evolved over the years. The current version (2010) has been adopted by the leading journals of medical science [46].

In the absence of a dedicated reporting standard in the cybersecurity field, we adopted some aspects of CONSORT to inform the inclusion criteria applied for this review. For example, studies were excluded if they did not include a comprehensive description of the research methods employed. As outlined in figure 3, 275 studies were initially included based on content relevance. However, 38% (105) were excluded for not describing the research methodology in detail. This substantial number of exclusions highlights the necessity for reporting standards in the field. Similar observations have been made by others. For example, researchers have raised problems with unbalanced samples, missing data points, untested findings and variable reporting standards [56, 84, 98]. For the field to advance, this needs to change.

4.10 Variable definition of cybersecurity solutions

Cybersecurity is a diverse domain, and solutions developed to address different problems invariably get grouped under the term 'cybersecurity solutions'. This generalisation creates the false impression that studies were referring to the same class of solutions, when those that they have in mind could be quite different. For instance, many studies (n=24) suggested that existing 'cybersecurity solutions' were unsuitable for SMEs, while others (n=23) proposed new 'cybersecurity solutions'. While they all employed the same terminology, they touched on entirely different kinds of solutions. For example, some discussed information security management and risk management solutions [4–6, 81]; others cybersecurity maturity measurement frameworks [59, 82]; others cybersecurity awareness assessment [63]; others cybersecurity resilience frameworks [20]; others cybersecurity assurance and self-measurement framework [20, 51, 59]; while others discussed automation and the standardisation of cybersecurity incident response capabilities [70].

Despite the generalisation and unrelated usage of the terminology, studies unanimously concluded that existing solutions are still unsuitable for SMEs. Osborn and Simpson suggested this was because the literature and industry mistakenly assumed that large and small organisations always shared the same requirements [79]. However, in our view, it is likely that the cybersecurity industry and researchers alike overstate the impact of new technologies and understate the effort to tailor solutions to smaller businesses.

4.11 Lack of progress in SME research

The approach of distinguishing between novel contributions in the literature (conclusions) and discussions of prior literature that motivated a study (drivers) allowed us to evaluate the progress made on these themes over time. This differentiation revealed that recent research has introduced only a few novel findings, but that authors repeat and propagate many early discoveries without empirically replicating or offering new insights about them. Unfortunately, and perhaps ironically, many empirical studies came to the same conclusions as existing research, but authors were often seemingly unaware of previous work on the topic.

We see a few potential factors that may explain this situation. First, researchers often appeared to perform superficial literature reviews, neglecting the exploration of fundamental research that could have informed their investigations. Second, the absence of standardised research methodologies (and reporting standards) in the cybersecurity field has created space for opportunistic practices (e.g. interviews with small numbers of SMEs that were known to the researchers as opposed to the random sampling of SMEs using a sampling frame), potentially overshadowing the use of more rigorous research methods that are the expectation in more established fields of enquiry. Third, reviewed academic papers were scattered across many journals and venues. To illustrate, the 59 peer-reviewed academic studies considered here were published across 46 different journals and venues. Some of these were unrelated to computer systems; for instance, articles appeared in titles such as 'Entrepreneurship and Sustainability Issues', 'Business Excellence and Management', 'Journal of Applied Business and Economics' and 'Journal of Intellectual Capital'. Finally, in addition to the variable reporting standards discussed in section 4.9, the validity and reliability of some cybersecurity literature have been questioned by other researchers. For instance, Groß assessed the quality of 114 quantitative studies related to cybersecurity (from 2006 to 2016). Gross suggested that two-thirds of the papers delivered incomplete data, and about one-quarter presented findings based on erroneous calculations and inconsistent data. This research also concluded that reliability decreased over time he found more errors in newer studies [49].

Therefore, the standard of (SME) cybersecurity literature would appear to be a more widespread issue, and solving it is not easy. It requires coordinated initiatives and effort from researchers, reviewers, funders and stakeholders. Our recommendation starts with the need for a definition/adoption of sound and rigorous research and reporting standards, as have been established in other fields (e.g. medicine, see [34, 53, 74]), followed by more stringent reviewing processes prior to publication.

4.12 Limitations

As with any research, this review is not without limitations. For instance, we only considered studies written in English, which could create a language bias and result in a lack of representation from certain regions, especially developing countries. To ensure that the information we included was not outdated, we excluded studies published before January 2017. By doing so, we may have missed important information not subsequently discussed in the literature. Similarly, we may have missed information by excluding studies that did not explicitly describe the research methods used. Nonetheless, we accepted this risk in favour of relying on findings from studies for which it was clear how data were collected and analysed (which is a rather basic requirement). Lastly, Manuscript submitted to ACM

qualitative research inherently has an element of subjectivity. This research was carried out by three authors who met regularly to review and discuss the findings. Efforts were made to maintain objectivity, but biases can never be eliminated - only acknowledged and attempts made to mitigate them.

5 CONCLUSION

Despite SMEs being the backbone of the global economy, cybersecurity efforts remain focused on larger organisations. Perhaps because of this, the number of cyber-attacks and resulting financial losses SMEs face are skyrocketing. Nonetheless, there is a growing number of initiatives and research projects concerning SME cybersecurity. Here, we provide a systematic review of recent literature, applying qualitative methods to identify and synthesise the existing knowledge. We differentiated between knowledge that is perpetuated throughout the literature without new empirical findings, and those findings that are based on the generation of new evidence. We discussed the most frequently emerging themes and their potential relationship. Our discussion included observations and recommendations concerning the variability of reporting standards across studies and the staleness and reliability of the literature.

Notwithstanding our reservations about the quality of some of the literature, three significant barriers to cybersecurity for SMEs emerged: a lack of awareness of threats faced, resource constraints (human, digital and financial) and limited cybersecurity literacy among SME personnel. While there appears to be a cause-and-consequence relationship between these factors, research is required to comprehend the mechanisms through which they affect each other. Our hope is that the findings of this review will inform the future research agenda and help industry and governments deliver initiatives tailored to SME needs.

REFERENCES

- [1] Jean Adams, Frances C. Hillier-Brown, Helen J. Moore, Amelia A. Lake, Vera Araujo-Soares, Martin White, and Carolyn Summerbell. 2016. Searching and synthesising 'grey literature' and 'grey information' in public health: Critical reflections on three case studies. Systematic Reviews 5, 1 (9 2016), 1–11. https://doi.org/10.1186/s13643-016-0337-y
- [2] Luis A Aguilar. 2015. The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses. https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html
- [3] F Ahmed, A Burney, and A Malik. 2020. Security Aspects of Virtualization and Its Impact on Business Information Security. https://doi.org/10.1109/ICISCT49550.2020.9080029
- [4] N N Ahmed and K Nanath. 2021. Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System. Journal of Cyber Security and Mobility 10, 3 (2021), 511–536. https://doi.org/10.13052/jcsm2245-1439.1032
- [5] Abdulmajeed Alahmari and Bob Duncan. 2020. 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, Cyber SA 2020. Institute of Electrical and Electronics Engineers Inc., 1–5. https://doi.org/10.1109/CYBERSA49311.2020.9139638
- [6] Abdulmajeed Abdullah Alahmari and Robert Anderson Duncan. 2021. Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2021 13 (7 2021), 1–6. https://doi.org/10.1109/ECAI52376.2021.9515166
- [7] Fatimah Alghamdi, Nermin Hamza, and Moutasm Tamimi. 2019. Factors that Influence the Adoption of Information Security on Requirement Phase for Custom-Made Software at SMEs. 2nd International Conference on Computer Applications and Information Security, ICCAIS 2019 2 (5 2019), 1-5. https://doi.org/10.1109/CAIS.2019.8769519
- [8] F Alharbi, M Alsulami, A Al-Solami, Y Al-Otaibi, M Al-Osimi, F Al-Qanor, and K Al-Otaibi. 2021. The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. https://doi.org/10.3390/s21206901
- [9] Dhoha Almubayedh, Mashael Al Khalis, Ghadeer Alazman, Manal Alabdali, Rouqaiah Al-Refai, and Naya Nagy. 2018. Security Related Issues in Saudi Arabia Small Organizations: A Saudi Case Study. 21st Saudi Computer Society National Computer Conference, NCC 2018 21 (12 2018), 1-6. https://doi.org/10.1109/NCG.2018.8593058
- [10] Maria Bada and Jason R C Nurse. 2019. Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). https://doi.org/10.1108/ICS-07-2018-0080
- [11] Tony Bailetti and Daniel Craigen. 2020. Examining the relationship between cybersecurity and scaling value for new companies. https://doi.org/10.22215/timreview/1329
- [12] Yves Barlette, Katherine Gundolf, and Annabelle Jaouen. 2017. CEOs' information security behavior in SMEs: Does ownership matter? https://doi.org/10.3917/sim.173.0007
- [13] Y Barlette and A Jaouen. 2019. Information security in SMEs: Determinants of CEOs' protective and supportive behaviors. https://doi.org/10.3917/sim.193.0007
- [14] Wolfgang Bergthaler, Kenneth Kang, Yan Liu, and Dermot Monaghan. 2015. Tackling Small and Medium Sized Enterprise Problem Loans in Europe; by Wolfgang Bergthaler, Kenneth Kang, Yan Liu, and Dermot Monaghan; IMF Staff Discussion Notes SDN/15/04; March, 2015. Technical Report. INTERNATIONAL MONETARYFUND. https://doi.org/10.5089/9781498384834.006
- [15] John M. Blythe and Shane D. Johnson. 2021. A systematic review of crime facilitated by the consumer Internet of Things. Security Journal 34, 1 (3 2021), 97–125. https://doi.org/10.1057/s41284-019-00211-8
- [16] Virginia Braun and Victoria Clarke. 2008. Using thematic analysis in psychology. Qualitative Research in Psychology 3, 2 (1 2008), 77–101. https://doi.org/10.1191/1478088706qp063oa
- [17] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? Qualitative Research in Psychology 18, 3 (7 2021), 328–352. https://doi.org/10.1080/14780887.2020.1769238
- [18] Michael Brunner, Andrea Mussmann, and Ruth Breu. 2018. Introduction of a Tool-Based Continuous Information Security Management System: An Exploratory Case Study. https://doi.org/10.1109/QRS-C.2018.00088
- [19] Ted Byrt, Janet Bishop, and John B. Carlin. 1993. Bias, prevalence and kappa. Journal of Clinical Epidemiology 46, 5 (5 1993), 423–429. https://doi.org/10.1016/0895-4356(93)90018-V
- [20] J F Carias, S Arrizabalaga, L Labaka, and J Hernantes. 2021. Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs. IEEE Access 9 (2021), 80741–80762. https://doi.org/10.1109/ACCESS.2021.3085530
- [21] J F Carías, M R S Borges, L Labaka, S Arrizabalaga, and J Hernantes. 2020. Systematic Approach to Cyber Resilience Operationalization in SMEs. https://doi.org/10.1109/ACCESS.2020.3026063
- [22] Carlos R. 2022. jrrombaldo/literature_review: scripts to support literature review. https://github.com/jrrombaldo/literature_review
- [23] U K National Cyber Security Centre. 2017. Cyber Security Small Business Guide. https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know
- [24] N A Chandra and M Sadikin. 2020. ISM application tool, a contribution to address the barrier of information security management system implementation. *Journal of Information and Communication Convergence Engineering* 18, 1 (2020), 39–48. https://doi.org/10.6109/jicce.2020.18.1.

39

- [25] CISA. 2022. Cyber Guidance for Small Businesses. https://www.cisa.gov/small-business
- [26] Jeffrey Cleveland and Abigail Scheg. 2018. Small-Medium Business Information Security Intention Related to Cyberthreat Awareness: A Quantitative Experiment. Ph. D. Dissertation. Northcentral University, Ann Arbor. https://www.proquest.com/dissertations-theses/small-medium-business-information-security/docview/2050026809/se-2?accountid=14511
- [27] European Commission. 2020. The EU Cybersecurity Act_Shaping Europe's digital future. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
- [28] Matt Dickson. 2019. Small firms suffer close to 10,000 cyber-attacks daily | FSB, The Federation of Small Businesses. https://www.fsb.org.uk/resources-page/small-firms-suffer-close-to-10-000-cyber-attacks-daily.html
- [29] Willian Dimitrov, Katia Rasheva-Yordanova, Oleg Konstantinov, Kristina Bosakova, and Viktoriya Angelova. 2019. TOWARD OVER-COMING THE DISPROPORTION BETWEEN THE DEMAND FOR PROFESSIONALS AND THE PROVISION OF TRAINING IN CYBERSECURITY. EDULEARN19 Proceedings 1 (7 2019), 1656–1664. https://doi.org/10.21125/EDULEARN.2019.0485
- [30] P Douchek, L Nedomova, L Luc, and L Novak. 2020. Information security: The glory and penury of SMEs in the Czech and Slovak Republics. In Int. Conf. Eng. Manag. Commun. Technol., EMCTECH - Proc. Institute of Electrical and Electronics Engineers Inc., 1–7. https://doi.org/10.1109/EMCTECH49634.2020.9261506
- [31] Olatunde Durowoju, Hing Kai Chan, and Xiaojun Wang. 2020. Investigation of the Effect of e-Platform Information Security Breaches: A Small and Medium Enterprise Supply Chain Perspective. https://doi.org/10.1109/TEM.2020.3008827
- [32] Josiah Dykstra, Rohan Mathur, and Alicia Spoor. 2020. Cybersecurity in Medical Private Practice: Results of a Survey in Audiology. Proceedings - 2020 IEEE 6th International Conference on Collaboration and Internet Computing, CIC 2020 6 (12 2020), 169–176. https://doi.org/10. 1109/CIC50333.2020.00029
- [33] Darrell Eilts. 2020. An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses. ProQuest Dissertations and Theses 11, 15 (2020), 309. https://www.proquest.com/dissertations-theses/empirical-assessment-cybersecurity-readiness/docview/2392421605/se-2?accountid=135034
- [34] Sandra M. Eldridge, Claire L. Chan, Michael J. Campbell, Christine M. Bond, Sally Hopewell, Lehana Thabane, Gillian A. Lancaster, Alicia O'Cathain, Doug Altman, Frank Bretz, Marion Campbell, Erik Cobo, Peter Craig, Peter Davidson, Trish Groves, Freedom Gumedze, Jenny Hewison, Allison Hirst, Pat Hoddinott, Sarah E. Lamb, Tom Lang, Elaine McColl, Daniel R. Shanahan, Chris Sutton, and Peter Tugwell. 2016. CONSORT 2010 statement: Extension to randomised pilot and feasibility trials. Pilot and Feasibility Studies 2, 1 (2016), 64. https://doi.org/10.1186/s40814-016-0105-8
- [35] O Elezaj, S Y Yayilgan, M Abomhara, P Yeng, and J Ahmed. 2019. Data-Driven Intrusion Detection System for Small and Medium Enterprises. https://doi.org/10.1109/CAMAD.2019.8858166
- [36] European Commission. 2021. Bridging the security, privacy and data protection gap for smaller enterprises in Europe | SENTINEL Project | Fact Sheet | H2020 | CORDIS | European Commission. https://cordis.europa.eu/project/id/101021659
- [37] European Commission. 2022. High-Level Guidelines on Cybersecurity for SMEs | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/library/high-level-guidelines-cybersecurity-smes
- [38] European Digital SME Alliance. 2017. Europe needs a cybersecurity strategy to foster its SME ecosystem European DIGITAL SME Alliance. https://www.digitalsme.eu/europe-needs-cybersecurity-strategy-foster-sme-ecosystem/
- [39] EUROSTAT. 2022. Small and medium-sized enterprises (SMEs) Structural business statistics Eurostat. https://ec.europa.eu/eurostat/web/structural-business-statistics/small-and-medium-sized-enterprises
- [40] FCC. 2016. Cybersecurity for Small Business | Federal Communications Commission. https://www.fcc.gov/general/cybersecurity-small-business
- [41] Dávid János Fehér. 2020. Cybersecurity threats of cloud and third-party services in small and medium-sized enterprise environment. Management, Enterprise and Benchmarking in the 21st Century (2020), 36–41. https://www.proquest.com/scholarly-journals/cybersecurity-threats-cloud-third-party-services/docview/2474920793/se-2?accountid=14511
- [42] James H Felton Jr. and Oludotun Oni. 2021. Cyber Resilience of Small Business Owners., 121 pages. https://www.proquest.com/dissertations-theses/cyber-resilience-small-business-owners/docview/2504819573/se-2?accountid=14511
- [43] Key Findings. 2016. How Gartner Defines Threat Intelligence. https://www.gartner.com/en/documents/3222217
- [44] Ruti Gafni and Tal Pavel. 2019. The invisible hole of information on SMB's cybersecurity. Online Journal of Applied Knowledge Management 7, 1 (2019), 14–26. https://doi.org/10.36965/ojakm.2019.7(1)14-26
- [45] Geiger. 2021. GEIGER Cybersecurity for SMEs. https://project.cyber-geiger.eu/
- [46] Charlotte E. Gill. 2011. Missing links: How descriptive validity impacts the policy relevance of randomized controlled trials in criminology. Journal of Experimental Criminology 7, 3 (9 2011), 201–224. https://doi.org/10.1007/s11292-011-9122-z
- [47] Global Cyber Alliance. 2022. GCA Cybersecurity Toolkit for Small Business Handbook. https://gcatoolkit.org/wp-content/uploads/2021/06/GCA-Toolkit-Handbook.pdf
- [48] K Grondys, O Ślusarczyk, H I Hussain, and A Androniceanu. 2021. Risk assessment of the sme sector operations during the covid-19 pandemic. https://doi.org/10.3390/ijerph18084183

- [49] Thomas Groß. 2021. Fidelity of Statistical Reporting in 10 Years of Cyber Security User Studies. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 11739 LNCS (2021), 3–26. https://doi.org/10.1007/978-3-030-55958-8[_]1
- [50] Guidance Small to medium sized enterprise (SME) action plan. 2022. Small to medium sized enterprise (SME) action plan GOV.UK., 2 pages. https://www.gov.uk/government/publications/fcdo-small-to-medium-sized-enterprise-sme-action-plan/small-to-medium-sized-enterprise-sme-action-plan
- [51] Michael Heidenreich. 2019. Conceptualization of a measurement method proposal for the assessment of IT security in the status quo of micro-enterprises. In Proceedings - 2019 International Conference on Computing, Electronics and Communications Engineering, iCCECE 2019. IEEE, 187–192. https://doi.org/10.1109/iCCECE46942.2019.8941688
- [52] Margareta Heidt, Jin P. Gerlach, and Peter Buxmann. 2019. Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. Information Systems Frontiers 21, 6 (12 2019), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1
- [53] Julian P.T. Higgins, James Thomas, Jacqueline Chandler, Miranda Cumpston, Tianjing Li, Matthew J. Page, and Vivian A. Welch. 2019. Cochrane handbook for systematic reviews of interventions. Wiley. 1–694 pages. https://doi.org/10.1002/9781119536604
- [54] Thomas J. Holt. 2016. The evolution of cybercrime, 2006–2016. In Cybercrime Through an Interdisciplinary Lens. Vol. 1. Routledge, 29–50. https://doi.org/10.4324/9781315618456-9
- [55] N Huaman, B von Skarczinski, C Stransky, D Wermke, Y Acar, A Dreißigacker, S Fahl, and Baidu; et al.; Facebook; Google; Salesforce; USENIX. 2021. A large-scale interview study on information security in and attacks against small and medium-sized enterprises. In 30th USENIX Security Symposium, USENIX Security 2021. USENIX Association, 1235–1252. https://www.usenix.org/conference/usenixsecurity21/presentation/huaman
- [56] F E Ikuero and W Zeng. 2022. Improving Cybersecurity Incidents Reporting in Nigeria: Micro and Small Enterprises Perspectives. https://doi.org/10.4314/nit.v41i3.10
- [57] Eric Imsand, Brian Tucker, Joe Paxton, and Sara Graves. 2020. A survey of cyber security practices in small businesses. In Advances in Intelligent Systems and Computing, Vol. 1055. Springer, 44–50. https://doi.org/10.1007/978-3-030-31239-8[_]4
- [58] Marko Jantti. 2020. Studying Data Privacy Management in Small and Medium-Sized IT Companies. Proceedings of the 2020 14th International Conference on Innovations in Information Technology, IIT 2020 14 (2020), 57–62. https://doi.org/10.1109/IIT50501.2020.9299050
- [59] Andreas Johannsen, Daniel Kant, and Reiner Creutzburg. 2020. Measuring IT security, compliance and data governance within small and medium-sized IT enterprises. Electronic Imaging 32, 3 (1 2020), 1–11. https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-252
- [60] S Kabanda, M Tanner, and C Kent. 2018. Exploring SME cybersecurity practices in developing countries. https://doi.org/10.1080/10919392. 2018.1484598
- [61] Basel Katt and Nishu Prasher. 2018. Quantitative security assurance metrics: REST API case studies. https://doi.org/10.1145/3241403.3241464
- [62] A Ključnikov, L Mura, and D Sklenár. 2019. Information security management in smes: Factors of success. Entrepreneurship and Sustainability Issues 6, 4 (2019), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)
- [63] Tebogo Kesetse Lejaka, Adele Da Veiga, and Marianne Loock. 2019. Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa. 2019 Conference on Information Communications Technology and Society, ICTAS 2019 (4 2019), 1–6. https://doi.org/10.1109/ICTAS.2019.8703609
- [64] Emanuel Löffler, Bettina Schneider, Trupti Zanwar, and Petra Maria Asprion. 2021. CySecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness. International Journal of Serious Games 8, 1 (1 2021), 59–70. https://doi.org/10.17083/ijsg.v8i1.413
- [65] Ivorine M Lynch, Henry A Williams, and Sherree R B Davis. 2020. Department of Defense Controlled Unclassified Information Compliance: The Impact on Small Business Contractors. https://www.proquest.com/dissertations-theses/department-defense-controlled-unclassified/docview/2419860985/se-2?accountid=14511
- [66] Amy Mahn, Jeffrey Marron, Stephen Quinn, and Daniel Topper. 2021. Small Business Cybersecurity Corner | NIST. https://doi.org/10.6028/ NIST.SP.1271
- [67] Steve Mansfield-Devine. 2022. Cyber Security Breaches Survey 2022. Technical Report 4. UK Government Official Statistics. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
- [68] Steve Mansfield-Devine. 2023. Cyber Security Breaches Survey 2023. Technical Report 4. UK Government Official Statistics. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
- [69] P Mayer, N Gerber, R McDermott, M Volkamer, and J Vogt. 2017. Productivity vs security: Mitigating conflicting goals in organizations. Information and Computer Security 25, 2 (2017), 137–151. https://doi.org/10.1108/ICS-03-2017-0014
- [70] Landon McLilly and Yanzhen Qu. 2020. Quantitatively Examining Service Requests of a Cloud-Based On-Demand Cybersecurity Service Solution for Small Businesses. Proceedings - 2020 International Conference on Computational Science and Computational Intelligence, CSCI 2020 (2020), 116–121. https://doi.org/10.1109/CSCI51800.2020.00027
- [71] Stan Mierzwa and James Scott. 2017. Cybersecurity in non-profit and non-governmental organizations. https://www.researchgate.net/publication/314096686_Cybersecurity_in_Non-Profit_and_Non-Governmental_Organizations
- [72] Frederik Mijnhardt, Thijs Baars, and Marco Spruit. 2016. Organizational characteristics influencing sme information security maturity. Journal of Computer Information Systems 56, 2 (2016), 106–115. https://doi.org/10.1080/08874417.2016.1117369

- [73] Andrei-Laurențiu Mitrofan, Elena-Veronica CRUCERU, and Andreea BARBU. 2020. Determining the Main Causes That Lead To Cybersecurity Risks in Smes. Business Excellence and Management 10, 4 (2020), 38-48. https://doi.org/10.24818/beman/2020.10.4-03
- [74] David Moher, Larissa Shamseer, Mike Clarke, Davina Ghersi, Alessandro Liberati, Mark Petticrew, Paul Shekelle, Lesley A. Stewart, Mireia Estarli, Eliud S.Aguilar Barrera, Rodrigo Martínez-Rodríguez, Eduard Baladia, Samuel Duran Agüero, Saby Camacho, Kristian Buhring, Aitor Herrero-López, Diana Maria Gil-González, Douglas G. Altman, Alison Booth, An Wen Chan, Stephanie Chang, Tammy Clifford, Kay Dickersin, Matthias Egger, Peter C. Gøtzsche, Jeremy M. Grimshaw, Trish Groves, Mark Helfand, Julian Higgins, Toby Lasserson, Joseph Lau, Kathleen Lohr, Jessie McGowan, Cynthia Mulrow, Melissa Norton, Matthew Page, Margaret Sampson, Holger Schünemann, Iveta Simera, William Summerskill, Jennifer Tetzlaff, Thomas A. Trikalinos, David Tovey, Lucy Turner, and Evelyn Whitlock. 2016. Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. Revista Espanola de Nutricion Humana y Dietetica 20, 2 (12 2016), 148–160. https://doi.org/10.1186/2046-4053-4-1
- [75] Moraba Mokwetli and Tranos Zuva. 2018. Adoption of the ICT Security Culture in SMME's in the Gauteng Province, South Africa. 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, icABCD 2018 (2018), 1–7. https://doi.org/10. 1109/ICABCD.2018.8465139
- [76] Sadiq Nasir and Narasimha Rao Vajjhala. 2020. Evaluating information security awareness and compliance in sub-Saharan Africa: An interpretivist perspective. Proceedings of the 13th IADIS International Conference Information Systems 2020, IS 2020 13 (2020), 187–190. https://doi.org/10.33965/is2020{_j202006r025
- [77] Tabisa Ncubukezi, Laban Mwansa, and Francois Rocaries. 2020. A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. In 2020 15th International Conference for Internet Technology and Secured Transactions, ICITST 2020. IEEE, 1–6. https://doi.org/10. 23919/ICITST51030.2020.9351339
- [78] OECD. 2011. OECD Studies on SMEs and Entrepreneurship SMEs, Entrepreneurship and Innovation., 126–127 pages. https://doi.org/10.1787/bdb9256a-en
- [79] E Osborn and A Simpson. 2018. Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study. https://doi.org/10.1093/cominl/bxx093
- [80] Mourad Ouzzani, Hossam Hammady, Zbys Fedorowicz, and Ahmed Elmagarmid. 2016. Rayyan—a web and mobile app for systematic reviews. Systematic Reviews 5, 1 (2016), 210. https://doi.org/10.1186/s13643-016-0384-4
- [81] B Y Ozkan and M Spruit. 2019. Cybersecurity standardisation for SMEs: The stakeholders' perspectives and a research agenda. https://doi.org/10.4018/IJSR.20190701.oa1
- [82] Bilge Yigit Ozkan, Marco Spruit, Roland Wondolleck, and Verónica Burriel Coll. 2020. Modelling adaptive information security for SMEs in a cluster. https://doi.org/10.1108/JIC-05-2019-0128
- [83] H. Park, Y. Yoo, and H. Lee. 2021. 7s model for technology protection of organizations. Sustainability (Switzerland) 13, 13 (2021), 7020. https://doi.org/10.3390/su13137020
- [84] D Pérez-González, S T Preciado, and P Solana-Gonzalez. 2019. Organizational practices as antecedents of the information security management performance: An empirical investigation. https://doi.org/10.1108/ITP-06-2018-0261
- [85] Brian Pickering, Costas Boletsis, Ragnhild Halvorsrud, Stephen Phillips, Pickering Surridge Brian, Costas Boletsis, Ragnhild Halvorsrud, Stephen Phillips, and Mike Surridge. 2021. It's Not My Problem: How Healthcare Models Relate to SME Cybersecurity Awareness. https://doi.org/10.1007/978-3-030-77392-2{_}22
- [86] Andrew Rae and Asma Patel. 2020. Developing a security behavioural assessment approach for cyber rating UK MSBs. https://doi.org/10. 1109/CyberSecurity49315.2020.9138893
- [87] A Rae, A Patel, Heng S.-H., and Lopez J. 2019. Defining a New Composite Cybersecurity Rating Scheme for SMEs in the U.K. https://doi.org/10.1007/978-3-030-34339-2[_]20
- [88] Ellen M Raineri and Jessica Resig. 2020. Evaluating Self-Efficacy Pertaining to Cybersecurity for Small Businesses. The Journal of Applied Business and Economics 22, 12 (2020), 13–23. https://doi.org/10.33423/jabe.v22i12.3876
- [89] Elicia Ratajczyk, Ute Brady, Jacopo A. Baggio, Allain J. Barnett, Irene Perez-Ibara, Nathan Rollins, Cathy Rubiños, Hoon C. Shin, David J. Yu, Rimjhim Aggarwal, John M. Anderies, and Marco A. Janssen. 2016. Challenges and opportunities in coding the commons: Problems, procedures, and potential solutions in large-N comparative case studies. *International Journal of the Commons* 10, 2 (9 2016), 440–466. https://doi.org/10.18352/ijc.652
- [90] Nisha Rawindaran, Ambikesh Jayal, Edmond Prakash, and Chaminda Hewage. 2021. Cost Benefits of Using Machine Learning Features in NIDS for Cyber Security in UK Small Medium Enterprises (SME). Future Internet 13, 8 (1 2021), 186. https://doi.org/10.3390/fi13080186
- [91] Chris Rhodes. 2018. House of Commons Library Business Statistics. House of Commons 12, 1 (2018), 16. https://commonslibrary.parliament.uk/research-briefings/sn06152/
- [92] W. S. Richardson, M. C. Wilson, J. Nishikawa, and R. S. Hayward. 1995. The well-built clinical question: a key to evidence-based decisions. ACP journal club 123, 3 (11 1995), A12–A13. https://doi.org/10.7326/acpjc-1995-123-3-a12
- [93] Pablo Saa, Oswaldo Moscoso-Zea, Andres Cueva Costales, and Sergio Lujan-Mora. 2017. Data security issues in cloud-based Software-as-a-Service ERP. Iberian Conference on Information Systems and Technologies, CISTI 12 (7 2017), 1-7. https://doi.org/10.23919/CISTI.2017.7975779
- [94] K A Saban, S Rau, and C A Wood. 2021. "SME executives' perceptions and the information security preparedness model". Information and Computer Security 29, 2 (2021), 263–282. https://doi.org/10.1108/ICS-01-2020-0014

- [95] SMESEC. 2022. SMESEC Cybersecurity for SMEs. https://www.smesec.eu/
- [96] Statista Inc. 2019. Cloud IT infrastructure spending worldwide 2013-2026 | Statista. https://www.statista.com/statistics/503686/worldwide-cloud-it-infrastructure-market-spending/
- [97] Statista Inc. 2023. Enterprise public cloud service usage worldwide 2022 | Statista. https://www.statista.com/statistics/511508/worldwide-survey-public-coud-services-running-applications-enterprises/
- [98] T Tam, A Rao, and J Hall. 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. https://doi.org/10.1016/j.cose.2021.102385
- [99] Haydar Teymourlouei and Vareva Harris. 2019. Effective methods to monitor IT infrastructure security for small business. Proceedings 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019 10 (12 2019), 7–13. https://doi.org/10.1109/CSC149370. 2019.00009
- [100] The World Bank. 2022. World Bank SME Finance: Development news, research, data | World Bank. , 4 pages. https://www.worldbank.org/en/topic/smefinance
- [101] David Tranfield, David Denyer, and Palminder Smart. 2003. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. , 207–222 pages. https://doi.org/10.1111/1467-8551.00375
- [102] P Ulrich, V Frank, A Timmermann, Cristani M., Toro C., Zanni-Merk C., Howlett R.J., Jain L.C., and Jain L.C. 2020. The dark side of data science An empirical study of cyber risks in German SMEs. 24th KES International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, KES 2020 176 (2020), 2615–2624. https://doi.org/10.1016/j.procs.2020.09.307
- [103] United Nations. 2017. definition-statistics-SMEs. https://tfig.unece.org/contents/definition-statistics-SMEs.html
- [104] United States International Trade Co. 1983. (United States International Trade Commission reports). Technical Report. United States International Trade Commission. www.usitc.gov
- [105] Mojtaba Vaismoradi and Sherrill Snelgrove. 2019. Theme in qualitative content analysis and thematic analysis. Forum Qualitative Sozialforschung 20, 3 (9 2019), 23. https://doi.org/10.17169/fqs-20.3.3376
- [106] Max van Haastrecht, Guy Golpur, Gilad Tzismadia, Rolan Kab, Cristian Priboi, Dumitru David, Adrian Răcătăian, Matthieu Brinkhuis, and Marco Spruit. 2021. A shared cyber threat intelligence solution for smes. Electronics (Switzerland) 10, 23 (11 2021), 2913. https://doi.org/10.3390/electronics10232913
- [107] Max Van Haastrecht, Bilge Yigit Ozkan, Matthieu Brinkhuis, and Marco Spruit. 2021. Respite for smes: A systematic review of sociotechnical cybersecurity metrics. Applied Sciences (Switzerland) 11, 15 (8 2021), 6909. https://doi.org/10.3390/app11156909
- [108] Verizon Communications Inc. 2022. 2022 Data Breach Investigations Report (DBIR). , 5–108 pages. https://www.verizon.com/business/resources/reports/dbir/
- [109] Verizon Communications Inc. 2022. Small Business Cyber Security and Data Breaches | Verizon. https://www.verizon.com/business/resources/articles/small-business-cyber-security-and-data-breaches/
- [110] David Weisburd, David P. Farrington, Charlotte Gill, Mimi Ajzenstadt, Trevor Bennett, Kate Bowers, Michael S. Caudy, Katy Holloway, Shane Johnson, Friedrich Lösel, Jacqueline Mallender, Amanda Perry, Liansheng Larry Tang, Faye Taxman, Cody Telep, Rory Tierney, Maria M. Ttofi, Carolyn Watson, David B. Wilson, and Alese Wooditch. 2017. What Works in Crime Prevention and Rehabilitation: An Assessment of Systematic Reviews. Criminology and Public Policy 16, 2 (2017), 415–449. https://doi.org/10.1111/1745-9133.12298
- [111] Gareth R T White, Robert A Allen, Anthony Samuel, Ahmed Abdullah, and Robert J Thomas. 2020. Antecedents of Cybersecurity Implementation: A Study of the Cyber-Preparedness of U.K. Social Enterprises. https://doi.org/10.1109/TEM.2020.2994981
- [112] J A Young. 2020. The development of a red teaming service-learning course. https://aisel.aisnet.org/jise/vol31/iss3/1
- [113] Ratna Yudhiyati, Afrida Putritama, and Diana Rahmawati. 2021. What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society* 19, 4 (1 2021), 446–462. https://doi.org/10.1108/JICES-03-2021-0035
- [114] Zotero. 2022. Zotero | Your personal research assistant. https://www.zotero.org/

Received 26 September 2023