Mujtaba, Awan ORCID logoORCID: https://orcid.org/0000-0001-9055-2869, Alam, Abu ORCID logoORCID: https://orcid.org/0000-0002-5958-7905 and Kamran, Muhammad (2025) Cybersecurity Challenges in Small and Medium Enterprises: A Scoping Review. Journal of Cyber Security and Risk, 2025 (3). pp. 89-102. doi:10.63180/jcsra.thestap.2025.3.7

Official URL: https://doi.org/10.63180/jcsra.thestap.2025.3.7
DOI: 10.63180/jcsra.thestap.2025.3.7
EPrint URI: https://eprints.glos.ac.uk/id/eprint/15581

Disclaimer

The University of Gloucestershire has obtained warranties from all depositors as to their title in the material deposited and as to their right to deposit such material.

The University of Gloucestershire makes no representation or warranties of commercial utility, title, or fitness for a particular purpose or any other warranty, express or implied in respect of any material deposited.

The University of Gloucestershire makes no representation that the use of the materials will not infringe any patent, copyright, trademark or other property or proprietary rights.

The University of Gloucestershire accepts no liability for any infringement of intellectual property rights in any material deposited but will remove such material from public view pending investigation in the event of an allegation of any such infringement.

Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Cybersecurity Challenges in Small and Medium Enterprises: A Scoping Review

Mujtaba Awan[1], Abu Alam[1], Muhammad Kamran[2]

[1] *University of Gloucestershire School of Computing and Engineering CHELTENHAM, United Kingdom*
[2] *Department of Computer Science, Air University Islamabad, Aerospace and Aviation Campus Kamra, Pakistan*

ARTICLE INFO

Article History

Received: 25-04-2025
Revised: 04-07-2025
Accepted: 09-07-2025
Published: 10-07-2025

Academic Editor:

Prof. Youakim Badr

Vol.2025, No.3

DOI:
https://doi.org/10.63180/jcsra.thestap.2025.3.7

ABSTRACT

Small and medium-sized enterprises (SMEs) are one of the most important engines to add to the global economy by providing financial benefits to the human population, in the form of businesses (90%) and employment ships (60%). With the increase in the ratio of cybercrimes, SMEs have been overlooked in terms of cybersecurity measures, leaving them unprepared to deal with the increasing frequency, sophistication, and destructiveness of cyber challenges. This scoping review is designed to address the various cybersecurity threats to SMEs and their possible overcome. In this review, various databases such as Google Scholar, IEEE, Elsevier, Science Direct, and Taylor & Francis online were utilized in exploring the reported literature, and searched under various terminologies, in combinations and separately. Overall, 30 research articles were found to be most relevant to the respective topic, from which 20 unique themes were identified and categorized in novel findings. A framework was proposed for this scoping review by performing data analysis, which led us to find 20 different types of cyber challenges in SMEs. These challenges were further standardized into four classes. In this review, the main challenges to attaining cybersecurity resilience in SMEs are found to be a lack of awareness, unsuitable guidelines for SMEs, limited cybersecurity Knowledge, and constrained financial resources.

Keywords: *Cybersecurity, Cybersecurity Threat, Small and medium enterprises, Challenges, Barriers.*

How to cite the article
Awan, M., Alam, A., & Kamran, M. (2025). Cybersecurity Challenges in Small and Medium Enterprises: A Scoping Review. Journal of Cyber Security and Risk Auditing, 2025(3), 89–102. https://doi.org/10.63180/jcsra.thestap.2025.3.7

*Corresponding author. Email: Mujtabaawan99@gmail.com

1. Introduction

SMEs account for more than 90% of the global business economy. In Europe, 99% of businesses are classified as small and medium-sized enterprises (SMEs) according to the definition outlined in EU law 2003/361[1], [2]. However, in the UK, SMEs make up 99.9% of all businesses. Since there are many variations in the definition of SMEs, we use the European Union definition of SMEs as an organization employing between 10 and 250 people [3].

Based on the significant contributions by SMEs to the overall country's economy, they are expected to adopt and implement cybersecurity strategies appropriately. However, this is not the case as presented by Renaud and Weir in 2016 [4], indicating that the main cause is the financial conflict and online confusion between industry and company authorities. This makes them more vulnerable to various financial, productive, and legal expenses, which may ultimately result in bankruptcy. SMEs are easy targets for cyber attackers on which they are focusing now, due to a lack of awareness [5] or vulnerabilities and low-risk management [6]. SMEs remain victims of cyber attackers, although they are well prepared and take suitable measures to protect their businesses [7].

According to the statistics, 62% of SMEs in Australia said they had experienced cyberattacks. This data closely aligned with the global number from 2017, according to which cybercriminals have attacked 66% of SMEs in the last 12 months. These numbers are not only a great concern for SMEs themselves but for the suppliers and clients as well. A recent study highlighted a concerning trend of successful cyber-attacks against SMEs [8][9] according to sources such as the Verizon report, 58% of attacks registered in 2019 targeted SMEs.

Another study described in Verizon Communications indicated various data breaches, of which 43% of breaches involved SMEs as the victims [10][11]. In the UK Federation of Small Business, SMEs are becoming increasingly targeted, and a daily rate of 10,000 attacks against UK-based SMEs [12]. These attacks can result in significant financial losses and breaches. Despite these worrying statistics, many SMEs still need to prepare for cyberattacks, with recent surveys showing that only 17% of UK businesses have undertaken vulnerability audits [13]. Research suggests that this is due to a need for more awareness of the threats faced as well as a low-risk perception and prioritization. Other contributing factors include insufficient investments in cybersecurity and poor cybersecurity literacy to establish defensive programs [14], [15].

Cyber security is the art of protecting networks, devices, and data against unauthorized access or illegal usage. It also deals with the practice of assuring information confidentiality, integrity, and unavailability to the public. Cybersecurity is one of the growing areas of research with numerous topics for groups of scientists. This technology is of one the recently emerging critical technologies, and the research on cybersecurity in SMEs specifically still needs to be improved, as shown in the literature [16], [17]. As cyber-attacks increase on a large scale, attackers have shifted their attention from large organizations to small and medium enterprises with less resilience. Our study was mandatory to realize that very little literature was available regarding the global cybersecurity challenges concerning small and medium enterprises. To the best of our knowledge and based on the reported literature, only one survey of a similar nature has been done [18].

The overall situation regarding the cybersecurity challenges and their classification in SMEs needs more clarification and must be worked out in quite detail to address researchers and practitioners. The current scoping review aims to provide a deeper understanding of the issue and make practitioners able to prioritize the critical cybersecurity challenges that can be fatal to SMEs. Here we attempted to consolidate most of the previously reported information and tried to find a gap in important cybersecurity challenges, highlighted in SME literature, offering more useful prospects for researchers in this field. This review paper includes the first section of the scoping review methodology, used to ensure the precision and reliability of the current study. The next section presents our findings and analysis. In the last section, results and findings are elaborated and explained in detail identifying gaps, and future implications are considered and discussed.

2. Methodology

The methodology utilized in this scoping review was initially demonstrated by Arksey and O'Malley [19] and Levac *et al*. [20]. The Arksey and O'Malley framework is implemented to ensure that the study complies with rigorous standards of precision, consistency, and reliability [21].

The reason for conducting the scoping review is to focus precisely on an emerging theme to explore the literature size, identify gaps, and propose research schemas according to the most recent implications in the field. Traditional systematic literature review focuses on the findings of previously conducted empirical studies on a more established topic, involving searches for a more general problem to solve. A general question identified is almost likely as "What is best for this research area? [21]. Literature studies showed that "cybersecurity challenges in SMEs" is one of the new areas of research in this field [18][22]. Therefore, we choose a scoping review methodology instead of the SLR methodology. A pictorial representation of various stages worked in the current scoping review is given in Figure 1.

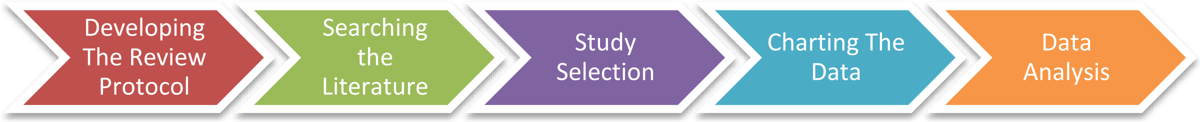


Figure 1. Stages of Scoping Review Methodology

2.1. Developing the review Protocol

During the first phase, a comprehensive review process is developed and trailed throughout the various phases of this review. This protocol is quite flexible and can be modified by the study fit, acting more likely as a set procedure rather than a guiding tool. Developing the protocol involves the identification of the research problem, study scope, setting of search criteria *i.e.* inclusion and exclusion criteria, background concepts, data extraction, roles and duties of each team member, data analysis procedures, and work designs. The concept of current research and the actual problem statement are discussed as under.

(1) What are the main cybersecurity challenges, faced by SMEs?
(2) What are the significant gaps, which are identified from the literature during this study? And
(3) What are the possible solutions and recommendations for SMEs, to meet with identified cybersecurity challenges?

The overall objectives of this review article are categorized into three main areas. Firstly, it aims to present a comprehensive evaluation of the current literature, thereby contributing to the establishment of a standardized knowledge base. Secondly, it intends to identify any gaps in the existing research based on the findings from previous studies. Lastly, it aims to highlight potential areas for future research, specifically targeting scholars in the field. Moreover, this paper is significant from a practitioner's viewpoint and more valuable for companies, like SMEs who face cybersecurity threats in their organizations. It is also beneficial for information systems practitioners, trying to find the major cybersecurity challenges that greatly affect small and medium enterprises.

2.2. Searching the literature

A comprehensive search and examination of major databases were conducted to get a comprehensive collection of relevant literature for this investigation. The databases that were encompassed in the study consisted of Taylor & Francis Online, IEEE, Science Direct, and Google Scholar.

The citations and articles obtained from these databases were organized based on the time frame of 2018-2024 to locate the most up-to-date material for inclusion. The final keywords were selected for evaluation after each team member individually conducted a model test utilizing the designated databases. The keywords, frequently utilized were identified by various discussions and tests among participating members which include “cybersecurity,” “Challenges,” “cyber-security,” “Problems,” “SME,” “small and medium enterprises,” and “SMB.” The timeframe is chosen for the studies to be conducted with more specified keywords. It may also be the case that there is no time restriction set for searching keywords to investigate more literature, but only to select accurate and more general keywords.

In this study, after searching the literature using the above-mentioned keywords and by utilizing Boolean operators, 28 articles were selected from Taylor & Francis Online, 40 from IEEE, 19 from Google Scholar, and 15 from Science Direct. Table 1 shows the results of applying Boolean operators AND & OR. 102 articles were considered in total, initially for further evaluation.

Table 1: Search Strings

Scope	Search Strings
Cyber Security	“Cyber Security” Or “Cybersecurity” Or “Cyber-Security” Or “Cyber-Threats”
Challenges	“Challenges” Or “Challenge” Or “Barriers” Or “Issues”
SME	“Small & Medium Enterprises” Or “SME” Or “SMB” Or “Businesses”

2.3. Study Selection

Scoping research can be time-consuming, but Arksey and O'Malley [19] provided very helpful guidelines about the selection criteria for the most relevant research article to include in a scoping review. In our experience, this phase involved more iteration and more processes than were originally anticipated by the framework. We considered here a team approach, not specifically recommended by Arksey and O'Malley [19] in agreement with some other scholars that the scoping studies involve multidisciplinary teams, employing a transparent and verifiable method [20][23]. Identifying articles for this review initially, all the team members scheduled a meeting and identified 5 research papers out of 102 selected articles for training purposes, utilizing inclusion and exclusion criteria. Keeping in view that all the team members are proficient having sound knowledge to implement the inclusion and exclusion criteria, these five papers were picked randomly by the members. In this phase, additional analysis was carried out, so that each member makes sure that the selected paper should answer one of the research questions mentioned in phase one. Two members of the team scrutinized all 102 research articles independently so that all the results could be filtered compared and verified. The final decision is made by a third team member, cross-checking the reviewed articles.

The practice enhances the integrity and reliability of the review process. Throughout the process of screening and cross-checking articles, the entire team met together, discussed, and iteratively improved the search criteria on many occasions. After the screening process, the authors also carried out an in-depth analysis of the data independently and working in teams.

This aided in selecting the conclusive studies to be included in the research study. During the screening studies, we discovered several duplicate research papers, publications that required to be translated into English, and articles unrelated to the issue, which were excluded, as shown in Figure 2. Finally, following the selection procedure, 30 research papers were led to be investigated further.

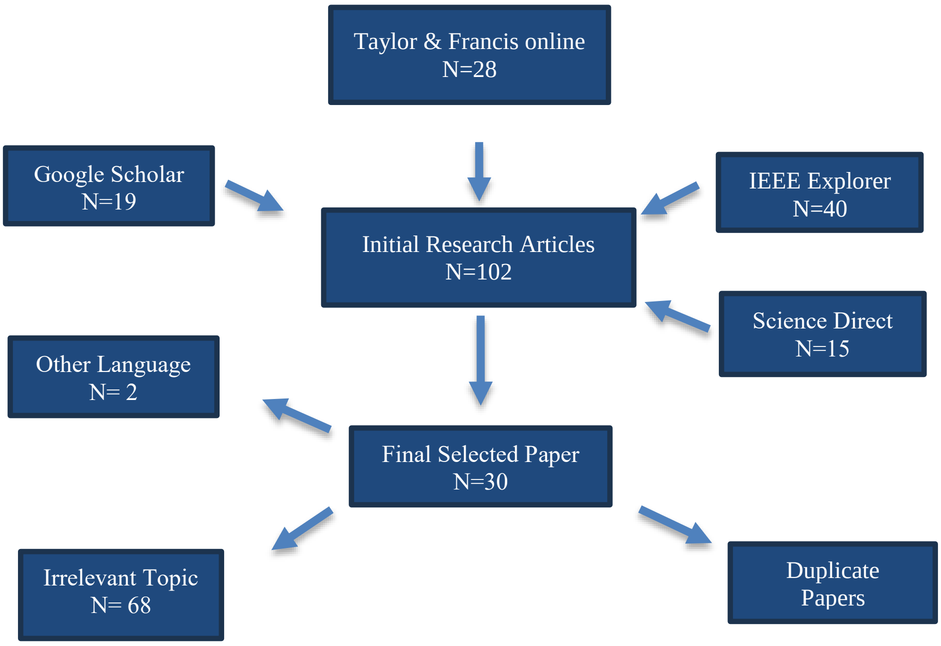


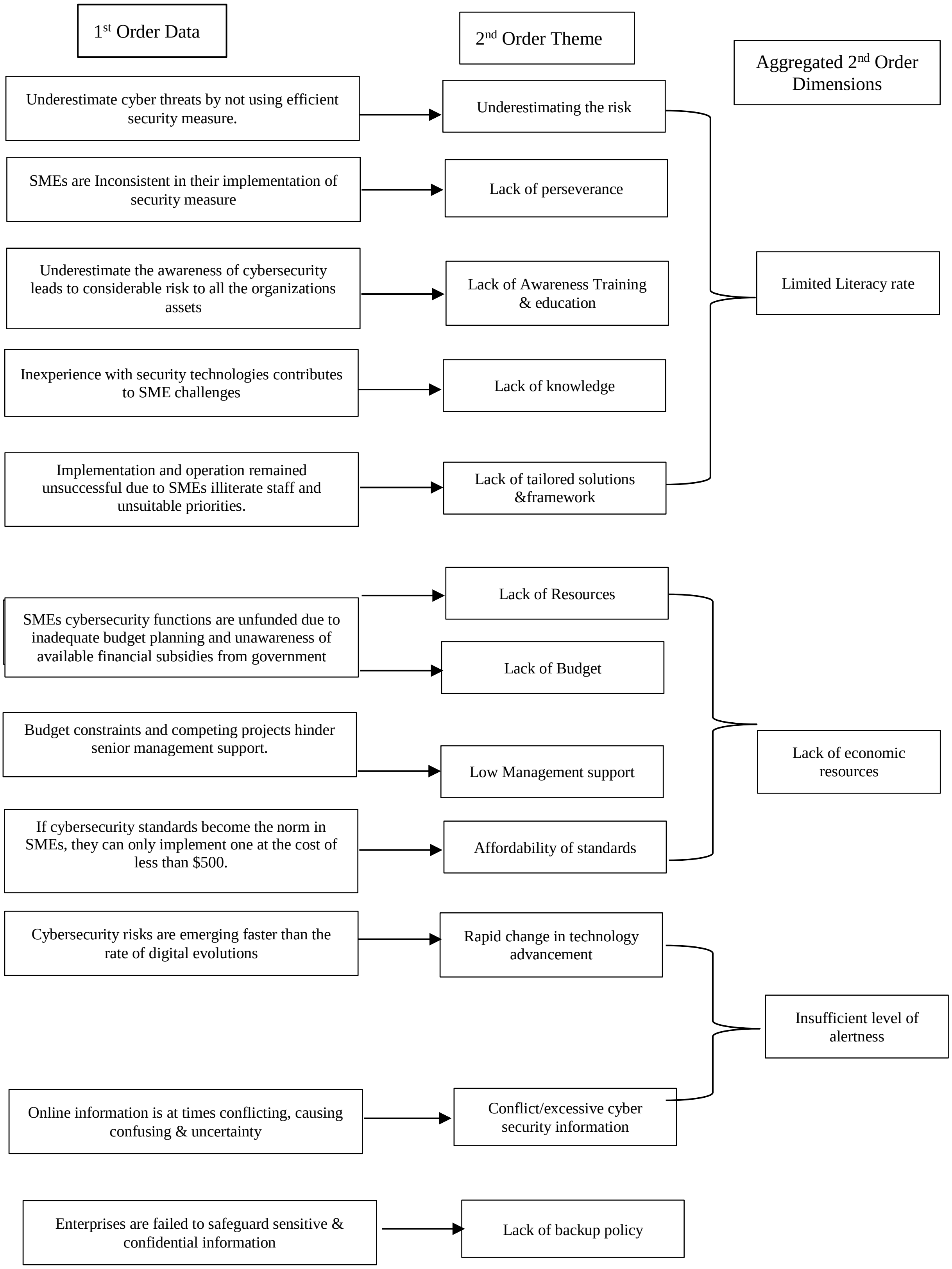
Figure 1. Paper Selection Process Flowchart

2.4. Charting the Data

During this phase of the process, a coding worksheet in MS Excel was created to extract pertinent information from each of the articles selected. The worksheet presents the primary information about each paper included in the study. This information sheet is initiated with the publisher's name, followed by the paper title, the author's name, the paper type, the origin of publication (country), and finally the publication year. The research team created another fundamental data sheet that includes the research questions, titles, and brief explanations for each cybersecurity challenge mentioned in the literature. Following that, they highlighted similar cybersecurity threats described in all 30 selected articles by using a single colour to make it convenient to code and create themes, for all the team members. Overall, 20 cyber challenges were identified by the team which are faced by SMEs.

The major objective of the current study is to investigate the cybersecurity challenges for SMEs and all the related companies. These challenges were identified by implementing the study's basic selection criteria. During the scoping review process, all the selected papers were discussed and elaborated by a group of team members. They developed and implemented the coding, and theme analysis to make coherent interpretations of the results and try to eliminate the possible bias and errors. This collaborative approach sought to improve the reliability and integrity of the review process. A framework designed by Salvato and Corbetta [24] was adopted to organize the data by developing various themes and categories.

The framework and main headings adopted from Salvato and Corbetta' work were, (1) First-order data; involving the detailed description of the cyber security threats faced by SMEs, collectively identified and organized by all team members in core data sheet from the selected research articles, (2) second-order theme; involves identified cyber security challenges in the SMEs, from first-order data, and finally (3) the consolidated second-order data dimensions; which include overall 20 such challenges, themes identified in SMEs from second-order data. These identified cyber security threats are standardized for further classification, depicted in Figure 3.


1st Order Data
2nd Order Theme
Aggregated 2nd Order Dimensions
Underestimate cyber threats by not using efficient security measure.
Underestimating the risk
SMEs are Inconsistent in their implementation of security measure
Lack of perseverance
Underestimate the awareness of cybersecurity leads to considerable risk to all the organizations assets
Lack of Awareness Training & education
Limited Literacy rate
Inexperience with security technologies contributes to SME challenges
Lack of knowledge
Implementation and operation remained unsuccessful due to SMEs illiterate staff and unsuitable priorities.
Lack of tailored solutions &framework
Lack of Resources
SMEs cybersecurity functions are unfunded due to inadequate budget planning and unawareness of available financial subsidies from government
Lack of Budget
Budget constraints and competing projects hinder senior management support.
Lack of economic resources
Low Management support
If cybersecurity standards become the norm in SMEs, they can only implement one at the cost of less than $500.
Affordability of standards
Cybersecurity risks are emerging faster than the rate of digital evolutions
Rapid change in technology advancement
Insufficient level of alertness
Online information is at times conflicting, causing confusing & uncertainty
Conflict/excessive cyber security information
Enterprises are failed to safeguard sensitive & confidential information
Lack of backup policy

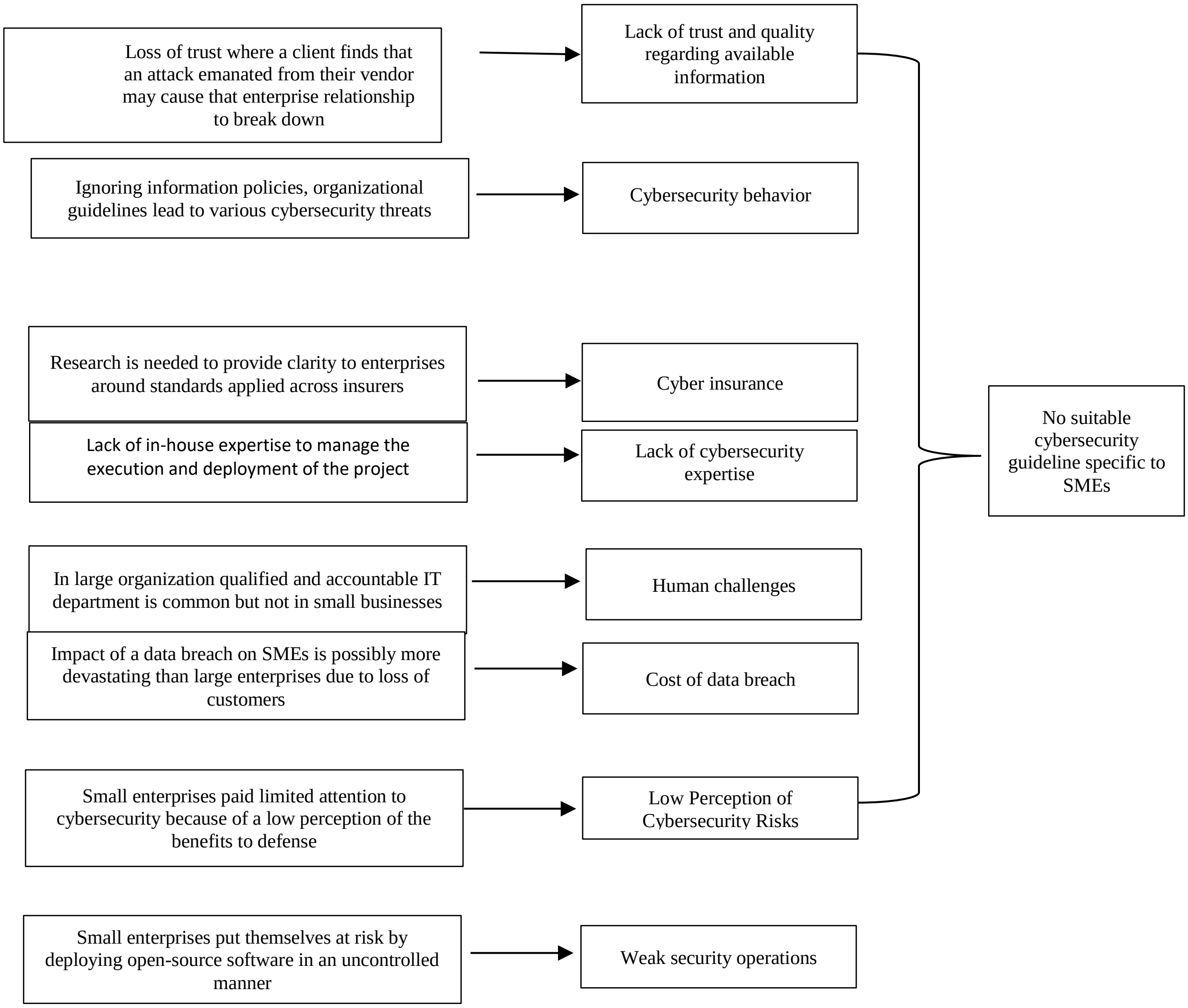

Loss of trust where a client finds that an attack emanated from their vendor may cause that enterprise relationship to break down
Lack of trust and quality regarding available information
Ignoring information policies, organizational guidelines lead to various cybersecurity threats
Cybersecurity behavior
Research is needed to provide clarity to enterprises around standards applied across insurers
Cyber insurance
Lack of in-house expertise to manage the execution and deployment of the project
Lack of cybersecurity expertise
No suitable cybersecurity guideline specific to SMEs
In large organization qualified and accountable IT department is common but not in small businesses
Human challenges
Impact of a data breach on SMEs is possibly more devastating than large enterprises due to loss of customers
Cost of data breach
Small enterprises paid limited attention to cybersecurity because of a low perception of the benefits to defense
Low Perception of Cybersecurity Risks
Small enterprises put themselves at risk by deploying open-source software in an uncontrolled manner
Weak security operations

Figure 3: Thematic Analysis for Cybersecurity Challenges in SMEs

2.5. Data Analysis

In this Phase, all the members worked together and collectively created coding sheets to perform thematic analysis of the data obtained. Descriptive categorization, like most other scoping reviews, was conducted for cybersecurity challenges of a similar nature under one theme. This practice describes the scope and utility of the current research. A detailed scoping review was carried out by implementing the guidelines and recommendations suggested by Liu *et al.* [21]. All the significant results obtained, are given in the upcoming section.

3. Research Findings

3.1. Publication Year

In this scoping review, the most recent literature is included so that the articles published in the years 2018 to 2023 were taken into subject. It is obvious from the literature that the adoption and execution of cyber-security in SMEs is a relatively new field, attracting recent attention. The exact percentages established from the current literature review are as under; 20% and 13% of the total paper count were published in 2018 and 2019 respectively. In 2020, 18% of articles were published, while in 2021 only 10% of related articles were published. In 2022 13% of articles were published. Whereas in

2023 & 2024, the total paper count published was 15% and 11% respectively. The visual representation of primary studies identified for each year, obtained from the current research is depicted in Figure 4.

3.2. *Publication Type*

The data obtained and presented in Figure 5, revealed that most of the research articles selected for this review, specifically 90% of the sample, were sourced from peer-reviewed journals. 10% of the sample consisted of papers sourced from conference proceedings and reports. Analyzing the data from publication year and publishing type, a progressive increase was found in the number of journal papers about the current subject mainly after 2018. From this fact, it can deduce that the topic could gain much of the core interest of practitioners as well as researchers, who aim to work in this research area in the future.

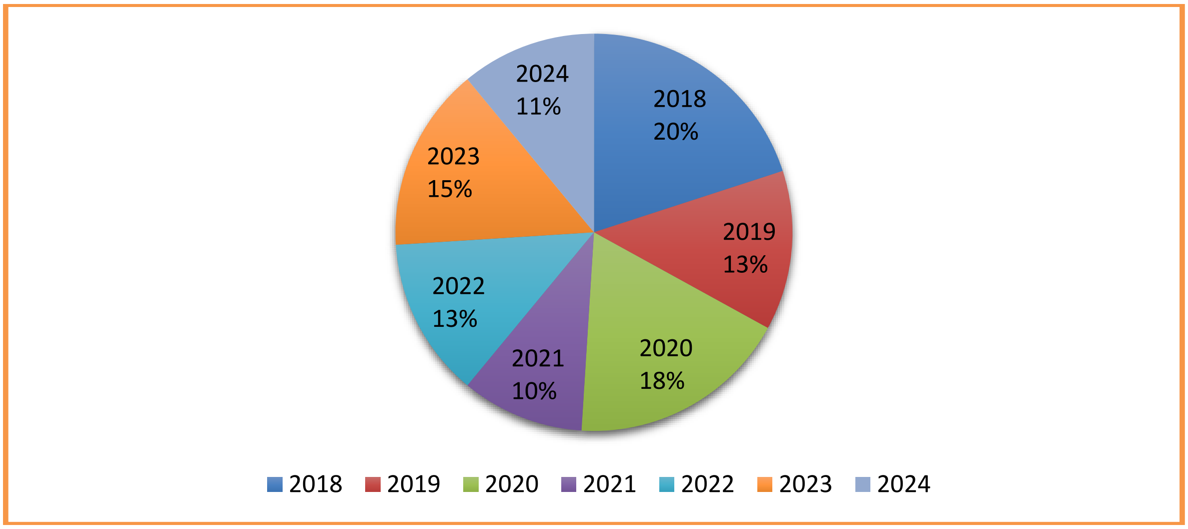


Figure 4. Research Article Sample from Each Year

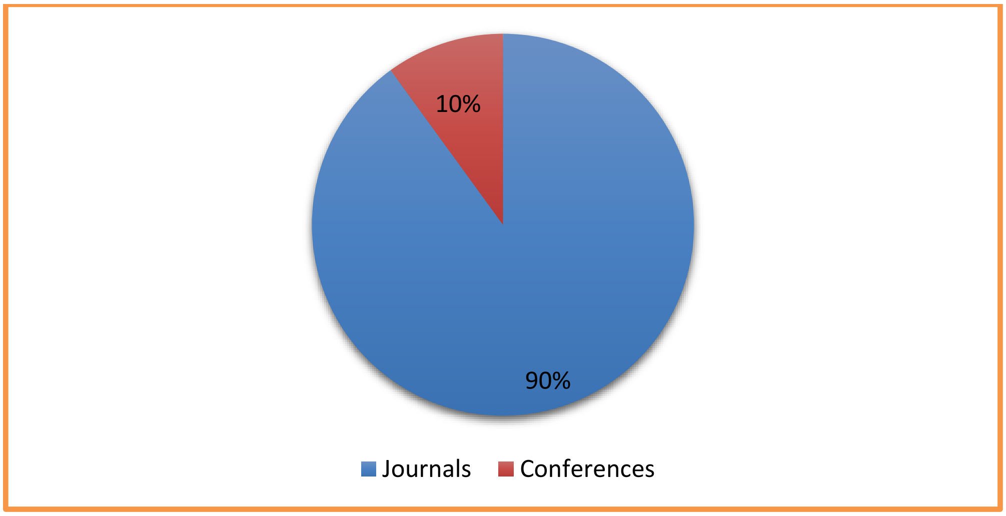


Figure 5: Type of Publication

3.3. Cybersecurity Challenges in Small & Medium Enterprises

A framework adapted from Salvato and Codetta [24] was utilized to conduct a thematic analysis. The first-order data include a detailed summary of the cybersecurity challenges in small & medium enterprises while the theme for each of these challenges is described in second-order themes. To ensure the validity and rigor of the review, independent analyses were accomplished by each team member independently, discussed in the methodology. After careful consideration, results were revealed, in which a total of four standardized cybersecurity challenges were reported. These were considered the most common and fatal challenges to SMEs, depicted in aggregated 2nd-order dimensions. The thematic analysis of cybersecurity challenges in SMEs is described in quite detail in Figure 3. An overview of these thematic findings, demonstrating how the literature references connected in each cyber threat category, is depicted in Table 2. Four standardized types of cybersecurity challenges in SMEs are shown in the first left column of the table. All the themes developed about these challenges using literature description are depicted in the middle column while the literature references for each of the themes and classes are given in the extreme right column, as shown in Table 2.

Table 2: Categorization of Cybersecurity Challenges in SMEs

Categorization of Cyber security challenges in SMEs	Themes Identified	Literature reference from sample studies
	Underestimating the risk	
	Lack of perseverance	
Limited Literacy rate	Lack of Awareness Training & education	[6][9][12][22]
	Lack of knowledge	[11][27][4]
	Lack of tailored solutions &framework	
	Lack of Resources	
Lack of economic resources	Lack of Budget	[15][16][22][5][12][4]
	Low Management support	
	Affordability of standards	
	Rapid change in technology advancement	
Insufficient level of alertness	Conflict/excessive cyber security information	[15][17][22]
	Lack of backup policy	
	lack of trust and quality regarding available information	
	Cybersecurity behaviour	
	Cyber insurance	
Not suitable cybersecurity guideline specific to SMEs	lack of cybersecurity expertise	[11][12][20][18][25][19][20][38]
	Human challenges	
	Cost of data breach	
	Low Perception of Cybersecurity Risks	
	Weak security operations	

3.4. Nature of Cyber Security Challenges

This research study revealed that the major issue for SMEs is the unavailability of suitable cybersecurity guidelines, which is up to 50% of the total research studies. Limited literacy rate and budgetary issues are investigated to be the second major cybersecurity challenges in SMEs which is about 45% for each. Insufficient level of alertness is the other notable cybersecurity challenge that was documented in small enterprises in our sample research articles. A visual representation of sample studies is given in Figure 6, demonstrating the overall challenges in SMEs for each of the themes

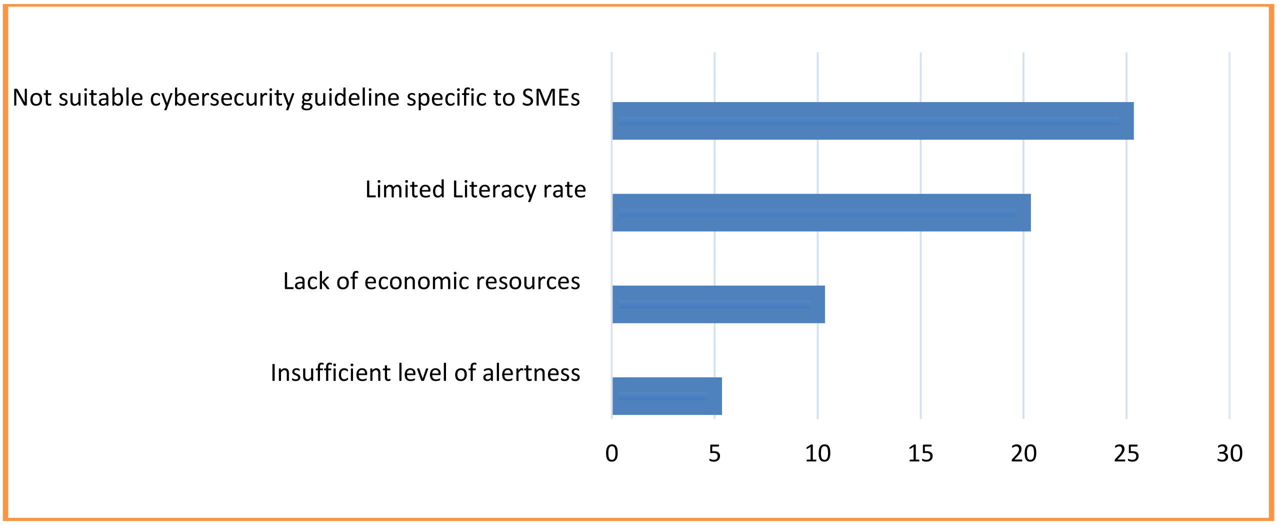


Figure 6. Cybersecurity Challenges in SMEs Reported by Sample Studies

3.5. Solutions for Cybersecurity Challenges

In our current scoping review, it is analyzed that there are only a few articles available in the literature that mainly work on the solution to various cybersecurity challenges. There is much less data reported about the solution to these challenges specifically in SMEs.

The possible solutions which are given by most of the research studies in context to SMEs are Lack of awareness, cybersecurity knowledge, and lack of concern training as well trainers. In Table 3, we tried to summarize all the possible solutions to these challenges in SMEs. There is still room to investigate more practical solutions to solve these crucial challenges. Further research investigations are needed to solve these vast ranges of cybersecurity concerns mentioned in several research articles about SMEs.

4. Discussion and Recommendation

The results and findings of the scoping review demonstrate the current research on cybersecurity challenges in SMEs. This review study highlighted the most documented cybersecurity challenges faced by small and medium business corporations. The study findings indicate the necessity for further research in this area of domain. It is investigated that most of the research studies reporting the cybersecurity challenges in SMEs are based on review studies. The studies demonstrated by Liu, Xiang, *et al.* [25], Sukumar, Arun, *et al.* [26], S Kabanda *et al.* [10], and Falch, M., *et al.* [22] showed that most of the studies are based on reviews instead of empirical considerations. Furthermore, significant research gaps were identified by our current analysis, in the literature on cybersecurity challenges in small and medium enterprises. Here we recognised a few notable gaps found in our current sample results. Our analysis of the sample studies revealed that; firstly, “No suitable guidelines for SMEs” is one of the most significant challenges that small enterprises face, which is highlighted here. This challenge can be so harmful that can cause a closure of the business identified by Ahmed *et al.* in 2021. Galvin [27] and Chidukwani [18] reported that around 1 billion dollars are annually spent by the Australian Criminal Intelligence Commission (ACIC) to prevent cybercrime.

This challenge can have an extensive impact, leading to the loss of business and damage to personal identity. It also revealed that about 60% of SMEs are so badly victimized by cyber attackers, which most of the business vanished within six months. This issue being very crucial needs guidelines and empirical studies to resolve. Therefore, it is strongly recommended that researchers should investigate the issue in more detail and design powerful strategies to minimize this challenge as much as possible. The second fact analyzed here is that the studies emphasizing the industry, especially those that look at cybersecurity issues in SMEs are rare. According to our analysis, 50% of the current literature discusses the cyber-security issues in SMEs without mentioning any industry. "Knowledge of cybersecurity issues" in SMEs specifying the nature of certain industries is lacking. Other results revealed that only a few studies focused on the education, banking, and IT sectors. Therefore, in the future, such research should be designed which investigate the cybersecurity challenges in SMEs with specific industry sectors.

Addressing this research gap, the current literature is enhanced which intern very beneficial for the practitioners facing cybersecurity challenges in the relevant industry. Most of the authors have explored the difficulties, but more research studies should be conducted to address the identified cybersecurity challenges. From the above analysis, it's been clear that the solutions to most of the identified cybersecurity concerns have not been thoroughly investigated. Therefore, more empirical research studies on cybersecurity challenges in SMEs are needed.

At this stage of knowledge, scientific research intending to provide solutions to cybersecurity concerns in SMEs is an intriguing research opportunity, substantial and most applicable field to SMEs [28]. Novel research studies may assist researchers in developing better solutions to the previously stated cybersecurity challenges. We carefully examined and evaluated the scoping review; however, certain limitations are there in this study as well. Firstly, the current research study is mainly restricted to the articles published in English only

This information is deduced from the independent search performed by each team member individually, using our selected databases and keyword search. There are only two papers were found published in other languages. Secondly, the selection bias may present one of the restrictions for the current scoping review. We tried to search the maximum possible number of articles, based on the keyword search in different databases, used regularly by the researchers. However, there can be a possibility to overlook the research papers published on this issue in other databases. During this review, we found a good agreement between the study concepts of various research groups about good cybersecurity practices. Bryan's [29] investigations revealed that an affordable and reliable starting point to practice good cybersecurity in SMEs is to design a comprehensive information security system. The main objective of the information system is to educate the employees, their cybersecurity training, and computer use policy [4]. According to Kaila and Urpo [30], the foremost beneficial step for SMEs is the identification of risks and protection themes for systems and data. Other researchers suggested that small enterprises should emphasize more on such measures that can help to reduce the impact of cyber-attacks. The important practices include an increased investment in cybersecurity expertise and inspection teams. It is not solely upon the SMEs but also the responsibility of technology vendors as well, who have been challenged to incorporate security into computing systems, providing an assist to SMEs with limited access to expertise [29], [31], [32]**.** Table 3 summarizes the recommended practices by different researchers [18][33][34] [35][36]. In SMEs, the practical implementation of these practices is slightly difficult. Therefore, various authors *e.g.* Carias and Borges offered a framework for the implementation order of these practices [37], [38].

Table 3. Good Cyber Security Practices

1	Make budget for cybersecurity	10	Ensure backup policies
2	Use multifactor authentication	11	Develop a strategy to train staff
3	Create password policies	12	Have regular training awareness
4	Install malware and antivirus	13	Grow cyber security as the business grow
5	Perform a risk management assessment	14	Make sure employee are familiar with security policies
6	Hire trustworthy employees	15	Perform automatic backups of all data
7	Implement multifactor authentication	16	Employ dedicated cyber staff
8	Up-to-date incident response plan	17	Consider investing in cyber insurance
9	Secure remote access	18	Review contract and policies with vendor

5. Conclusion

The identification of cybersecurity challenges and the creation of their solutions is one of the emerging and most important areas of research. Continuous research is necessary to aid in the creation of cybersecurity solutions for small and medium-sized businesses (SMBs). Cybersecurity research makes up a significant section of the corporate sector but most often neglects small and medium-sized businesses (SMBs). SMEs play a significant role in the global economy, and in the UK, they make up 99% of all businesses. Despite their large proportion and importance, the current study reveals that cybersecurity research in SMEs needs to be expanded and more focused. The focus of this scoping review is to investigate the scope of cybersecurity concerns, its size, and research gaps found in the reported literature on these challenges. It is shown here that most of the sample research studies are based on cyber-security challenges in SMEs, without focusing on a specific industry sector. Also, the ratio of the empirical studies is quite low as compared to the conceptual-based review studies. It is evaluated that more empirical research is required on this issue and can be an important topic for researchers. It is also reduced here from the current studies that there are only a few strategies are investigated to cope with cybersecurity issues and much fewer solutions are proposed for these challenges in SMEs. The most common challenges that SMEs face, pointed out here are unsuitable guidelines, low literacy rate, lack of resources, and insufficient level of alertness. It is also indicated here that there is much shortage of literature that can provide various types of strategies needed to implement to minimize the cyber threats to organizations. The governments and academic institutions are required to invest in the said research area and incentivize the researchers to conduct more investigational studies regarding SME cyber-security. The findings of current research studies can be utilized as guidelines for future researchers, academic and research institutions, governments, and policymakers when comes to selecting the focus of cyber security research in SMEs.

Corresponding author

Mujtaba Awan

Mujtabaawan99@gmail.com

Acknowledgment

NA

Funding

This research received no external funding.

Contributions

M.A; A.A; M.K; Conceptualization, M.A; A.A; M.K; Investigation, M.A; A.A; M.K; Writing (Original Draft), M.A; A.A; M.K; Writing (Review and Editing) Supervision, M.A; A.A; M.K; Project Administration.

Ethics declarations

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication

Not applicable.

Conflicts Of Interest

The authors declare no conflicts of interest.

6. References

[1] Vives, A. (2014). Social and environmental responsibility in small and medium enterprises in Latin America. *Journal of Corporate Citizenship*, 2006(21), 39–50. https://doi.org/10.9774/gleaf.4700.2006.sp.00006

[2] European Commission. (n.d.). *What is an SME?* Retrieved from http://ec.europa.eu/enterprise/policies/sme/factsfigures.analysis/sme-definition/index_en.htm

[3] European Union. (2003). *Recommendation 361 concerning the definition of micro, small and medium-sized enterprises*. Poslední aktualizace 6.5.

[4] Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the unbearability of uncertainty. In *Proceedings of the 2016 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 137–143). IEEE. https://doi.org/10.1109/CCC.2016.29

[5] IEEE Industrial Electronics Society & IEEE. (2016). *2016 International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS)*, 21–24 June 2016.

[6] Onwubiko, C., & Lenaghan, A. P. (n.d.). Managing security threats and vulnerabilities for small to medium enterprises.

[7] Ponemon, L. (2019). What's new in the 2019 cost of a data breach report. *Security Intelligence*.

[8] Ahmed, N. N., & Nanath, K. (2021). Exploring cybersecurity ecosystem in the Middle East: Towards an SME recommender system. *Journal of Cyber Security and Mobility*, 10(3), 511–536. https://doi.org/10.13052/jcsm2245-1439.1032

[9] Alahmari, A., & Duncan, B. (n.d.). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence.

[10] Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

[11] Verizon Communications Inc. (2022). *Small business cyber security and data breaches*. https://www.verizon.com/business/en-gb/resources/reports/dbir/

[12] Dickson, M. (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

[13] Mansfield-Devine, S. (2022). *Cyber Security Breaches Survey 2022*.

[14] Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: Factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081–2094. https://doi.org/10.9770/jesi.2019.6.4(37)

[15] Raineri, E. M., & Resig, J. (2020). Evaluating self-efficacy pertaining to cybersecurity for small businesses. *Journal of Applied Business & Economics, 22*(12).

[16] Suryotrisongko, H., & Musashi, Y. (2019). Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective. In *Proceedings of the 2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA)* (pp. 162–167). IEEE. https://doi.org/10.1109/SOCA.2019.00031

[17] Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A narrative review of cybersecurity implications for Australian small businesses. *Computers & Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

[18] Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cybersecurity of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, *10*, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

[19] Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International Journal of Social Research Methodology*, *8*(1), 19–32. https://doi.org/10.1080/1364557032000119616

[20] Levac, D., Colquhoun, H., & O'Brien, K. K. (2010). Scoping studies: Advancing the methodology. *Implementation Science, 5*(1), 69. https://doi.org/10.1186/1748-5908-5-69

[21] Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management, 52*(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008

[22] Falch, M., Olesen, H., Skouby, K. E., Tadayoni, R., & Williams, I. (2023). Cybersecurity strategies for SMEs in the Nordic Baltic region. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.1161

[23] Anderson, S., Allen, P., Peckham, S., & Goodwin, N. (2008). Asking the right questions: Scoping studies in the commissioning of research on the organisation and delivery of health services. *Health Research Policy and Systems, 6*(1), 7. https://doi.org/10.1186/1478-4505-6-7

[24] Salvato, C., & Corbetta, G. (2013). Transitional leadership of advisors as a facilitator of successors' leadership construction. *Family Business Review, 26*(3), 235–255. https://doi.org/10.1177/0894486513490796

[25] Liu, X., et al. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology, 13*. https://doi.org/10.3389/fpsyg.2022.927398

[26] Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis, 43*(10), 2082–2098. https://doi.org/10.1111/risa.14092

[27] Galvin, J. (2021). Percent of small businesses fold within 6 months of a cyber-attack. Here's how to protect yourself. *Inc.com*.

[28] Williams, P. A. H., Manheke, R. J., & Manhcke, R. J. (n.d.). Small business – A cyber resilience vulnerability. Retrieved from http://ro.ecu.edu.au/icr/14

[29] Bryan, L. L. (2020). Effective information security strategies for small business. *International Journal of Cyber Criminology*, *14*(1), 341–360. https://doi.org/10.5281/zenodo.3760328

[30] Kaila, U., & Nyman, L. (2018). Information security best practices: First steps for startups and SMEs.

[31] Polkowski, Z., & Dysarz, J. (2018). *IT security management in small and medium enterprises*. Retrieved from https://www.researchgate.net/publication/324966050

[32] Sangani, N. K., & Vijayakumar, B. (n.d.). *Cyber security scenarios and control for small and medium enterprises*.

[33] Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers, 21*(6), 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

[34] McLilly, L., & Qu, Y. (2020). Quantitatively examining service requests of a cloud-based on-demand cybersecurity service solution for small businesses. In *2020 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 116–121). IEEE. https://doi.org/10.1109/CSCI51800.2020.00027

[35] Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

[36] McLaurin, T., Olson, P., & Aberman, J. (2021). *Efficacy of small business cybersecurity: A study on the efficacy of small business cybersecurity controls*.
[37] Carias, J. F., Borges, M. R. S., Labaka, L., Arrizabalaga, S., & Hernantes, J. (2020). Systematic approach to cyber resilience operationalization in SMEs. *IEEE Access*, *8*, 174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063
[38] Junior, C. R., Becker, I., & Johnson, S. (2023). *Unaware, unfunded and uneducated: A systematic review of SME cybersecurity*. Retrieved from http://arxiv.org/abs/2309.17186

Biographies

Mujtaba Awan is doing a Ph.D. degree in Cyber & technical computing from the University of Gloucestershire, UK. He is also a graduate of a Master of Philosophy in (Software Engineering) and a Bachelor of Computer Science. He has been with the RIPHAH International University Malakand Campus, Khyber Pakhtunkhwa, Pakistan, since 2019. His current research interests include Cyber security, Software Engineering, Empirical Software Engineering, Artificial Intelligence, Global Software Development. Mujtabaawan99@gmail.com

Dr Abu Alam received a PhD Degree in Computer Science from University of Gloucestershire UK. He is currently a Senior Lecturer in the School of Computing and Engineering, University of Gloucestershire, Cheltenham, UK. His current research interests include cyber security, Database Systems, Mobile Application Development, Advanced Programming and Web design. aalam@glos.ac.uk

Dr. Muhammad Kamran received a PhD Degree in Computer Science from Comsats University Pakistan. He is currently a Senior Lecturer in the Air University Kamra, Pakistan. His current research interests include cyber security, blockchains, Mobile Application Development. kamran.uow@gmail.com