Enhancing Cybersecurity Programs in Small and Medium Enterprises (SMEs): A Systematic Literature Review

Eliana Ludin[1], Masnizah Mohd[2], Fariza Fauzi[3]
Center for Cyber Security-Faculty of Information Science & Technology,
Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia[1, 2, 3]
College of Computing and Informatics, Universiti Tenaga Nasional, Putrajaya Campus, Selangor, Malaysia[1]

***Abstract*—Small and Medium Enterprises (SMEs) in Malaysia face increasing cybersecurity risks, yet their adoption of Security Education, Training, and Awareness (SETA) programs remains limited. Unlike prior reviews that focus broadly on SMEs, this study contributes novelty by systematically synthesizing empirical evidence within the Malaysian context. Guided by the PRISMA framework and supported by NVivo analysis, 57 studies published between 2019 and 2025 were examined to classify both the importance of SETA and the barriers to its implementation. The thematic analysis revealed six recurring domains of challenges: financial constraints, human resource limitations, management support, cultural resistance, technical infrastructure, and legal/data protection. Beyond consolidating fragmented insights, the study provides a taxonomy of challenges and practical recommendations such as modular training, role-specific awareness, and leveraging national initiatives. While this review offers structured guidance for policymakers and practitioners, its descriptive nature without empirical SME validation is a limitation, highlighting the need for future applied studies.**

***Keywords*—Cybersecurity program; Security Education, Training, Awareness (SETA); systematic evaluation; Malaysian SMEs; NVivo; PRISMA**

I. Introduction

In the wake of rapid digital transformation, Small and Medium Enterprises (SMEs) in Malaysia face an increasing risk of cyberattacks, exacerbated by limited cybersecurity awareness and preparedness. Despite growing reliance on digital platforms, many SMEs significantly underestimate their vulnerability, with studies revealing a persistent gap between perceived and actual cyber risk exposure [1], [12]. For instance, although 67% of Malaysian SMEs believed they were less likely to be targeted than large firms, 84% had already experienced attacks.

This disconnect underscores a critical challenge: the lack of effective Security Education, Training, and Awareness (SETA) programs tailored to the SME context. While national strategies, such as the Malaysia Cyber Security Strategy (MCSS) 2020–2024, provide broad frameworks, SMEs often lack the capacity and guidance to translate these strategies into actionable practices. The consequences include increased susceptibility to phishing, social engineering, and insider threat risks that are intensified by low budgets, minimal technical staff, and inconsistent policy adherence [2], [11].

To address this gap, this study conducts a Systematic Literature Review (SLR) of cybersecurity-related SETA programs in SMEs, focusing on both their importance and the implementation challenges, particularly within the Malaysian context. This review aims to provide structured insights for policymakers, practitioners, and researchers seeking to enhance cybersecurity resilience in small businesses.

The structure of the paper is organized as follows. Section II presents the background and related works, offering a detailed overview of Security Education, Training, and Awareness (SETA) concepts, along with the current cybersecurity landscape affecting SMEs in Malaysia. Section III describes methodology, outlining the systematic literature review (SLR) process guided by PRISMA, including article selection criteria and the use of NVivo software for thematic analysis. Section IV discusses the results, which are categorized into two primary themes: the importance of SETA programs and the challenges SMEs face in implementing them. Section V provides a critical discussion of the implications of these findings, offering practical insights for SME stakeholders and policymakers. Section VI delivers the conclusion, summarizing the key outcomes of the review. Finally, Section VII suggests directions for future research in the field of SME cybersecurity and SETA development.

II. Background and Related Work

Numerous studies have examined the cybersecurity vulnerabilities of Small and Medium Enterprises (SMEs), with a particular focus on the human factors addressed through Security Education, Training, and Awareness (SETA) programs. SETA initiatives are widely recognized as a vital tool for reducing cybersecurity risks stemming from human error, yet their implementation in SMEs remains inconsistent and under-researched. For instance, [3], [23] proposed a lifecycle model for SETA programs, emphasizing their success factors but primarily within larger organizational contexts. Similarly, [4], [13] highlighted the significance of security culture, but did not address how SETA can be operationalized specifically in SMEs Several national programs in Malaysia, such as CyberSAFE and the Cyber Security Health Check initiative, have offered general cybersecurity training to SMEs. However, these programs often lack customization for specific organizational needs and are not always accompanied by long-term impact evaluations [11]. Moreover, existing literature often emphasizes technological

solutions without adequately addressing behavioral change and policy adherence in small business environments [5], [58].

In parallel with SETA, emerging research in lightweight cryptography and side-channel attack (SCA) countermeasures has provided essential solutions to secure low-resource environments like SMEs. Side-channel attacks exploit hardware-level leaks such as power consumption or electromagnetic emissions to extract cryptographic keys. While widely studied in embedded systems and IoT, SCAs are becoming increasingly relevant for SMEs deploying smart devices or industrial control systems. For example, Charalambous and Stavrou (2024) highlighted the role of talent specialization in SETA programs to combat hardware-based threats, including SCAs [7], [57]. Similarly, new work in lightweight cryptographic protocols aims to secure constrained environments, with recent advancements improving resistance against SCAs and improving adoption in SME settings [8], [60].

Despite these advances, a major research gap remains in synthesizing existing SETA literature specifically for SMEs using a systematic approach, particularly within the Malaysian context. No prior study has applied a comprehensive SLR methodology combined with qualitative NVivo analysis to classify both the importance and challenges of SETA implementation. This study addresses that gap by offering a focused and empirical synthesis of SETA-related cybersecurity strategies tailored to the Malaysian SME environment, highlighting areas that require further investigation and practical improvement.

III. Methodology

The present study employed the established systematic review methodologies delineated by [9], [19]. The procedures can be classified into three discrete phases: The initial planning of the review, which consists of defining its necessity, providing a clear explanation, and designing the review procedure, comprises Stage 1. Reviewing the primary study field, locating pertinent studies, assessing these studies, extracting the data, and analyzing the extracted data are included in the second stage. The third stage consists of reporting and distributing the review's findings. This entails disseminating the recommendations and guaranteeing that the pertinent stakeholders in the field of study are informed [18], [19]. The preliminary stage, known as "review planning," has been predominantly shaped by the thorough elucidation and presentation of previous inquiries. In the subsequent phase, a comprehensive analysis was conducted by employing a precise set of keywords to identify scholarly articles that explored the subject of cybersecurity about SETA programs in SMEs from multiple perspectives.

The review process involved assessing each selected study's methodologies and key findings to synthesize the most relevant and impactful information. This analysis identified common themes and gaps in the existing literature, leading to the development of key recommendations for improving cybersecurity practices in SMEs through SETA programs. These recommendations will be shared with policymakers, industry leaders, and academics to promote a collaborative approach to addressing cybersecurity challenges in small and medium enterprises. By disseminating these findings effectively, the review aims to drive positive change and foster a more secure digital landscape for SMEs.

A. Research Questions

Review studies are conducted to broaden and improve our comprehension of the limits of current knowledge. Following a more thorough elucidation of the data analysis methods and the principal findings obtained during this inquiry, the subsequent section concludes with a discussion of the study's limitations. The following questions were formulated to expand the investigation.

RQ1: Is the SETA program important in SME companies?

RQ2: What are the challenges in SME companies?

These questions aim to address any research gaps and suggest avenues for further exploration. Additionally, the review study seeks to contribute valuable insights to the existing literature and offer recommendations for future research directions. By critically examining the data and findings, researchers can enhance the validity and reliability of their study, ultimately advancing our understanding of the subject matter.

B. Record Screening Process

Prominent academic databases, including Emerald, Scopus, Science Direct, SpringerLink, IEEE, and Taylor, were queried using specified keywords. To be evaluated for inclusion in this paper's review, the articles must have a combination of two specific keywords in their titles, keywords, or abstracts. The initial set of keywords is most frequently used and pertains to SMEs. Based on the given phrases, the initial group has been identified: "small and medium-sized enterprises in Malaysia,"; "SMEs" or "SME in Malaysia"; "small business in Malaysia"; "small firm in Malaysia"; "small enterprise in Malaysia"; "small company in Malaysia"; "medium-sized firm in Malaysia"; "medium-sized business in Malaysia"; "medium-sized enterprise in Malaysia"; or "medium-sized company in Malaysia" The subsequent collection of keywords is concerned with security, specifically cybersecurity. ("cybersecurity*" OR "cyber*" OR "cybercrime*" OR "cyberattack*" OR "cyber threat*") were identified as these keywords. The efficacy of keywords such as "Security Education, Training, and Awareness Programmes" and "SETA Programme" has been assessed. The results, however, needed to be more general and resolve the Stage 2 criteria. Moreover, this inquiry focuses on recently published studies, including every article published between 2019 and 2025.

In addition, the selection process for each article was guided by two distinct criteria. The cybersecurity of SMEs must be the subject of each essay. In addition, every paper must incorporate an empirical inquiry. Articles of a theoretical nature that needed more empirical investigation were excluded from consideration. As a result, approximately fifty out of one hundred articles that qualified for inclusion in this paper met each of the criteria above. Nevertheless, more papers were excluded from the subsequent analysis phase due to the following justifications: In the methodology sections of several articles, an empirical approach or a comprehensive explanation is required. Although certain sections of these publications, such as the abstracts and titles, did include relevant keywords, their primary emphasis

was on significant corporations. The document should have mentioned small-and medium-sized businesses (SMEs). Subsequently, the remaining papers were employed to progress to the second and third phases of the systematic review methodology, as suggested by [10], [19].

C. Assessment Criteria

The screening methods and eligibility criteria utilized in this inquiry are delineated in this section. In the beginning, duplicate entries were removed by considering each record's digital object identifier (DOI). The removal was performed without any other specialized instrument, utilizing a spreadsheet. Suppose a database record lacked a DOI; a manual search and eradication process employed the title, author, year, or other distinguishing characteristics linked to the entry. Moreover, we used precise criteria to ascertain participants' inclusion and exclusion. The study establishes the requirements as follows:

1) Studies derived from organization reports, guidelines, and technical opinion reports are excluded from consideration. In addition, testimonials, reviews, and editorials should be excluded from the research design, as they are derived from secondary sources and would render this review tertiary. Additionally, non-research literature ought to be omitted.

2) The study's inclusion criteria are as follows: articles must be composed in English, published from 2019 to 2025, and grounded in original research that utilizes empirical or theoretical data. Furthermore, publication in academic journals, conference proceedings, or book/book sections is required for the studies.

D. Analysis Include Article

The results presented in this literature review have been obtained by extracting pertinent data from the articles. The results synthesized are based on the knowledge of the reviewers as well as the quality and substance of the available literature [20]. All results, excluding those presented in Section 3.3, were obtained through data abstraction. The NVIVO software was utilized in Section 3.3 to determine the most frequently occurring terms from a compiled text that included all analytical sections of each article in the review.

This study conducts a literature review using the SETA Systematic Evaluation of Technical Articles for SMEs organizations, utilizing the NVivo software query tool. NVivo is a software application designed specifically for executing qualitative and mixed-methods research. It is used extensively in the analysis of disorganized data. Formulate a Text Search Query to identify specific words or phrases. This software empowers users to conduct word usage, context, and meaning analyses, identify prevalent concepts or subjects within documents, and classify words or phrases automatically. The system can employ well-established synonyms to detect exact parallels or comparable terms. Furthermore, it provides advanced features, including collocation search, fuzzy search, wildcard search, and Boolean operators. Upon completing the Text Search Query, articles containing critical information will be extracted, and the primary topics will be identified.

IV. Result

The present investigation produced a total of 150 data entries. Before conducting any survey, it is critical to eradicate any occurrences of redundancy. After removing duplicate entries, the residual records amounted to 75. Screening is performed in the initial analysis phase using NVivo, employing the combination of the terms "SETA + SME + IMPORTANT + CHALLENGE." Consequently, 57 records were identified as being extraneous for this evaluation. The number of articles included in the second screening was 18, as determined by combining the criteria "SETA + SME + CHALLENGE." The papers excluded from the exhaustive text analysis lacked empirical data and were not pertinent to the subject under investigation. As a result, 57 articles remained for examination. As modified from [14], [21], Fig. 1 illustrates the screening procedure. The remaining 57 articles were then subjected to a thorough text analysis to extract relevant data and insights related to the research topic. The screening procedure outlined in Fig. 1 helped to streamline the selection process and ensure that only the most pertinent articles were included in the study. By focusing on articles that met the "SETA + SME + CHALLENGE" criteria, the researchers gathered valuable information that contributed to the overall research findings. The systematic approach to screening and analyzing articles helped maintain the study's rigor and validity.

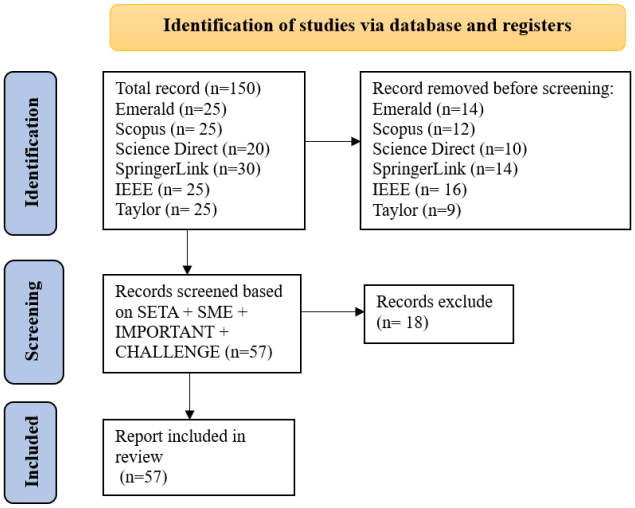

Fig. 1. The SLR screening process.

A. Finding

The field of Cybersecurity Programmes in SMEs is vast and encompasses numerous perspectives. As a result, the NVivo analytic software was employed to examine the fundamental components of cybersecurity management. Examining these fifty articles entailed the implementation of NVivo inquiry methodologies, such as Word Frequency and Text Search. As a result, these papers encompass two fundamental perspectives regarding the Cybersecurity SETA Programmes of SMEs: the importance of the SETA program and the challenges it presents. The two main perspectives discussed in this study are Cybersecurity Programmes in Small and Medium Enterprises (SMEs). This section shall explore the categories above,

commencing with the variety most frequently alluded to in the literature.

The primary aim is to utilize NVivo to identify and classify each phrase occurrence. Coding involves the methodical categorization of data to recognize recurring patterns or themes. The occurrences of the phrases "SETA," "SME," and "IMPORTANT" are identified and encoded for subsequent analysis in this instance. The result visualization in Table I provides a methodical summary of the coded phrases. This visual representation clearly explains the frequency and distribution of these key phrases within the dataset. By analyzing the patterns and themes that emerge from the coded data, researchers can gain valuable insights into the underlying concepts and trends present in the text. Overall, using NVivo for coding and analysis proves to be an effective tool in uncovering meaningful information from the data.

TABLE I. TOTAL REFERENCES BASED ON TERM

Title	Year	References based on the term
Challenges and strategies of contemporary cybersecurity awareness training in Swedish SMEs: A qualitative study [56]	2025	40
Implementation of methods to raise employees' cybersecurity awareness in small businesses [55]	2025	30
Harnessing the Right Talent for SETA Programs: Cybersecurity Roles and Competencies that Make a Difference [57]	2024	27
Employee Cybersecurity Awareness Training Programs Customized for SME Contexts to Reduce Human-Error-Related Security Incidents [58]	2024	61
An Exploratory Investigation into Sustaining Cybersecurity Protection Through the Implementation of SETA [59]	2024	32
Analysis of Information Security in a Corporate Environment – a Human Perspective [60]	2024	12
Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness [23]	2024	45
The critical success factors for Security Education, Training and Awareness (SETA) Programmes [22]	2023	50
Security culture and security education, training, and awareness (SETA) influence information security management [54]	2023	30
The Perspective of Small and Medium Enterprises SME's) and their relationship with the Government in overcoming Cybersecurity Challenges and barriers in Wales [25]	2023	43
Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailers [34]	2023	20
The effect of IT security issues on the implementation of Industry 4.0 in SMEs: Barriers and challenges [16]	2023	16
Survey and Lessons Learned on Raising SME Awareness about Cybersecurity [37]	2023	14
A Framework for The Planning and Management of Cybersecurity Projects [53] in Small and Medium-Sized Enterprises [39]	2023	19
Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach [40]	2023	13
The Impact of Industrial Revolution 4.0 and the Future of the Workforce: A Study on Malaysian IT Professionals [45]	2023	10
A Quest for Research and Knowledge Gaps in Cybersecurity Awareness for Small and Medium-Sized Enterprises [47]	2023	18
Cyber Risk Assessment and Optimization: A Small Business Case Study [48]	2023	4
Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies [49]	2023	9
Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime [24]	2022	40
Surround yourself with your betters: Recommendations for adopting Industry 4.0 technologies in SMEs [30]	2022	24
Cybersecurity for Small and Medium-sized Enterprises (SMEs) [36]	2022	5
Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises [41]	2022	26
A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations [50]	2022	6
Cyber-Security culture Towards Digital Marketing Communications among Small and Medium-Sized (SME) Entrepreneurs [27]	2021	8
A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs [28]	2021	35
Cyber risk management in SMEs: Insights from industry surveys [35]	2021	16
Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment [38]	2021	7
The Role of Trust in the Digital Interactive Model for SME Speed Internationalization [42]	2021	11
A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises [44]	2021	7
Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal [46]	2021	15
A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises [51]	2021	1
The Need for Information Security Management for SMEs [26]	2020	18
Factors Affecting SME Owners in Adopting ICT in Business Using Thematic Analysis [29]	2020	23
Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence [32]	2020	9
Organizational cybersecurity readiness in the ICT sector: A Quanti-Qualitative assessment [33]	2020	9
I am not usually the one who handles it: Exploring the disconnect between corporate security policies and actual security practices in SMEs [43]	2020	7
A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses [52]	2020	1
Developing cybersecurity education and awareness programs for small- and medium-sized enterprises (SMEs) [31]	2019	23

1) Importance of SETA SME: 57 journal articles out of 75 submitted in NVivo contain references and content pertinent to the "IMPORTANT SETA SME." Using the acronym "SETA SME" to represent a unique subject or idea is highly probable in 39 of the 75 scholarly articles. NVivo facilitates the

classification and analysis of content by subjects or keywords. It appears to have identified publications relevant to the subject matter or engaged in discussions regarding the importance of "SETA SME." In academic articles, the reference count represents the number of citations or sources incorporated within the respective work. The observed diversity among these articles may indicate discrepancies in the depth of investigation, the complexity of the topics explored, or the extent to which each article depends on external sources to support its claims. The findings underscore the significance of SETA within the SME sector, as evidenced by the substantial body of literature devoted to this subject. This body of literature highlights the SETA's impact on small and medium enterprises, showcasing its relevance and importance in driving growth and innovation in this sector. By delving into the various perspectives and research findings presented in these articles, a more comprehensive understanding of SETA SME can be achieved, ultimately leading to informed decision-making and strategic planning for businesses operating within this realm. As such, continued exploration and analysis of this topic will undoubtedly contribute to SMEs' ongoing development and success worldwide.

2) Challenge in SETA SME: The central focus was the convergence of SETA and SMEs, which represented a targeted investigation into the challenges faced by SMEs in the context of security training and education awareness initiatives. Once the criteria were applied, NVivo ascertained that out of the 75 publications examined, 15 specifically addressed challenges associated with SETA in SMEs. As shown in Table II, this phase presumably involved the application of automatic coding or manual annotation to identify instances in which challenges were explicitly addressed in the selected publications. Further analysis and scrutiny may be conducted using the selected subset of 19 articles. The extensive array of challenges identified in the literature, including but not limited to limited resources, regulatory obstacles, and other distinctive concerns, may necessitate the application of theme analysis.

TABLE II. CHALLENGE OF THE SETA IN SME

Challenges	Term based on the article
Cybersecurity threats	40
IT risk management	38
Gaps in established frameworks	36
Cultural issues	35
Technical hurdles	30
Limited resources and expertise in SMEs	24
Awareness and knowledge gap	20
Lack of support and commitment	17
Sustaining digital projects across various domains	15
Limited Rapid ICT development poses	10

V. DISCUSSION

This study contributes to the field by presenting a taxonomy of challenges SMEs face in implementing Security Education, Training, and Awareness (SETA) programs, derived from a systematic review of 57 empirical studies. These challenges are categorized into six domains: financial constraints, human resource limitations, management support, cultural resistance, technical infrastructure gaps, and legal/data protection concerns. For instance, financial and personnel shortages remain persistent across global contexts, limiting SMEs' ability to adopt sustained cybersecurity practices [15], [60].

Additionally, this review reveals that SMEs often lack clear frameworks for assessing cybersecurity risk and executing structured training protocols, leading to inconsistent adoption of best practices such as secure password management and software updates [6], [58].

Based on thematic coding using NVivo, we also provide empirical insights into common barriers SMEs face during SETA implementation, many of which stem from poor management buy-in and low employee engagement. This reinforces previous findings that organizational culture significantly impacts the success of cybersecurity training programs [17], [57].

Crucially, the study proposes practical recommendations tailored to SME environments. These include prioritizing modular SETA programs to reduce costs, integrating role-specific cybersecurity training, leveraging government-supported platforms like CyberSAFE Malaysia, and establishing clearer metrics for evaluating training effectiveness. As SMEs remain underrepresented in cybersecurity research, our findings also identify a research gap in longitudinal evaluations of SETA effectiveness, an area where future studies should focus.

TABLE III. TAXONOMY OF SETA IMPLEMENTATION CHALLENGES IN SMES AND PRACTICAL RECOMMENDATIONS

Challenge Category	Key Issues Identified	Practical Recommendations
Financial Constraints	Limited budgets for cybersecurity tools, training, or staff	Use modular or free SETA tools (e.g., CyberSAFE Malaysia); apply for national funding grants
Human Resource Limitations	Lack of skilled cybersecurity staff	Upskill existing staff; partner with external consultants or universities
Management Support	Low executive commitment; no budget or time allocation	Integrate cybersecurity goals into business KPIs; awareness sessions for decision-makers
Cultural Resistance	Employee apathy, change resistance	Gamify training; link cyber hygiene to personal/workplace safety
Technical Infrastructure Gaps	Outdated systems, lack of firewalls, insecure networks	Adopt cloud-based SME-friendly cybersecurity solutions
Legal/Data Protection Concerns	Lack of awareness of local/international data laws	Include regulatory compliance modules in SETA training programs

Table III summarizes a taxonomy of key challenges SMEs face in implementing Security Education, Training, and Awareness (SETA) programs, along with practical recommendations to overcome each challenge. The challenges

are grouped into six categories: financial constraints, limited human resources, lack of management support, cultural resistance, technical infrastructure gaps, and legal/data protection issues. For each category, the table outlines actionable solutions such as adopting low-cost training tools, partnering with external experts, integrating cybersecurity into business KPIs, engaging employees through personalized training, leveraging cloud-based security solutions, and including legal compliance in SETA content. This structured framework serves as a practical guide for SMEs and policymakers to strengthen cybersecurity readiness in resource-constrained environments.

This review not only confirms the importance of SETA in SMEs but also maps out the landscape of specific barriers, provides a taxonomy for future research, and offers actionable recommendations for industry practitioners and policymakers.

VI. Conclusion

This study conducted a systematic literature review (SLR) to explore the importance and challenges of implementing Security Education, Training, and Awareness (SETA) programs in Small and Medium Enterprises (SMEs), particularly within the Malaysian context. Drawing from 57 relevant academic sources, the study developed a taxonomy of six major challenge areas: financial, human resource, management, cultural, technical, and legal, providing both academic clarity and practical recommendations for improving cybersecurity practices in SMEs.

One of the central contributions of this research lies in synthesizing fragmented insights into a cohesive framework, which can guide policymakers and SME decision-makers in designing more tailored and effective SETA initiatives. The findings underscore the need for modular, cost-effective, and context-sensitive training, especially given SMEs' limitations in budget, staffing, and technical infrastructure.

However, it is important to acknowledge that this study remains descriptive in nature, as it is based solely on secondary data from published literature. The study does not include empirical validation with actual SME stakeholders, such as through surveys, interviews, or field studies. This is a notable limitation, as the practical relevance and applicability of the proposed taxonomy and recommendations could vary when applied to real-world SME contexts.

VII. Future Work

To address this gap, future research should incorporate empirical methods to validate the SLR findings. Mixed-method approaches—such as interviews with SME managers, surveys assessing SETA adoption, or pilot testing of tailored training models—can help confirm the practical relevance of the challenges and recommendations identified. Collaborations with local SMEs, government agencies, and cybersecurity training providers would also enable researchers to co-create field-tested frameworks that bridge the divide between academic theory and practical implementation.

By extending this research into applied settings, scholars and practitioners can more effectively support the cybersecurity resilience of SMEs, ensuring that SETA programs are not only theoretically sound but also operationally viable and sustainable in real-world business environments.

Acknowledgment

This work was supported by the Yayasan Canselor UNITEN Community Energy Grant. The authors thank Yayasan Canselor UNITEN for funding that enabled the systematic review and analysis presented in this paper. The support was instrumental in advancing the study of cybersecurity awareness and SETA implementation in the SME sector. The authors also acknowledge Universiti Tenaga Nasional (UNITEN) for institutional support throughout the research process.

References

[1] EC-Council, "Cybersecurity awareness in Malaysia."

[2] International Trade Administration, "MALAYSIA CYBERSECURITY."

[3] Cyber Security Malaysia, "Power of ISMS: Driving Value & Growth for SMEs in Malaysia," 2021.

[4] Ethan Yeo, "Invest in Cyber Security, SMEs Urged," The Sun, Sep. 04, 2023.

[5] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees' information security awareness in private and public organizations: A systematic literature review," Comput Secur, vol. 106, p. 102267, Jul. 2021, doi: 10.1016/j.cose.2021.102267.

[6] Aiza Azreen Ahmad, "Building Trusted, Secure and Ethical Digital Environment for Malaysian SMEs," The Edge Malaysia, Jul. 16, 2021.

[7] L.-W. Wong, V.-H. Lee, G. W.-H. Tan, K.-B. Ooi, and A. Sohal, "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities," Int J Inf Manage, vol. 66, p. 102520, Oct. 2022, doi: 10.1016/j.ijinfomgt.2022.102520.

[8] S. Hu, C. Hsu, and Z. Zhou, "The impact of SETA event attributes on employees' security-related Intentions: An event system theory perspective," Comput Secur, vol. 109, p. 102404, Oct. 2021, doi: 10.1016/j.cose.2021.102404.

[9] Cyber Security Malaysia, "Program Galakan Pemerkasan Keselamatan Siber Kepada PKS."

[10] Mohd Nazer Apau and Sabariah Ahmad, "Information Security Guidelines for Small & Medium Enterprises (SMEs)," 2020.

[11] S. R. Hamidi, A. A. Aziz, S. M. Shuhidan, A. A. Aziz, and M. Mokhsin, "SMEs maturity model assessment of IR4.0 digital transformation," Advances in Intelligent Systems and Computing, vol. 739, pp. 721–732, 2018, doi: 10.1007/978-981-10-8612-0_75.

[12] Chubb Insurance Malaysia Berhad, "How SMEs can protect themselves from cyber risks." Accessed: Sep. 15, 2023. [Online]. Available: https://www.chubb.com/my-en/articles/business/how-smes-can-protect-themselves-from-cyber-risks.html

[13] A. Santos-Olmo, L. Sánchez, I. Caballero, S. Camacho, and E. Fernandez-Medina, "The Importance of the Security Culture in SMEs as Regards the Correct Management of the Security of Their Assets," Future Internet, vol. 8, no. 4, p. 30, Jul. 2016, doi: 10.3390/fi8030030.

[14] Amrita V. Nair, "Accelerating Small and Medium-Sized Enterprise (SME) Digitalisation in Malaysia," 2023.

[15] Daniella Balaban, "Security Challenges of SMEs (Small to Medium Enterprises)."

[16] M. F. Arroyabe, C. F. A. Arranz, I. F. de Arroyabe, and J. C. F. de Arroyabe, "The effect of IT security issues on the implementation of Industry 4.0 in SMEs: Barriers and challenges," Technol Forecast Soc Change, vol. 199, no. December 2023, p. 123051, 2024, doi: 10.1016/j.techfore.2023.123051.

[17] S. Saeed, S. A. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," Sensors, vol. 23, no. 16, p. 7273, Aug. 2023, doi: 10.3390/s23167273.

[18] M. F. Arroyabe, C. F. A. Arranz, I. F. de Arroyabe, and J. C. F. de Arroyabe, "The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges," Technol Forecast Soc Change, vol. 199, p. 123051, Feb. 2024, doi: 10.1016/j.techfore.2023.123051.

[19] D. Tranfield, D. Denyer, and P. Smart, "Towards a Methodology for Developing Evidence‐Informed Management Knowledge using Systematic Review," British Journal of Management, vol. 14, no. 3, pp. 207‐222, Sep. 2003, doi: 10.1111/1467-8551.00375.

[20] A. Fink, Conducting Research Literature Reviews: From the Internet to Paper., Fifth. Sage Publications, 2020.

[21] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," BMJ, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.

[22] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "Critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: an empirical comparison of practitioner perspectives," Information & Computer Security, Aug. 2023, doi: 10.1108/ICS-08-2022-0133.

[23] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model," Information Technology and People, vol. 36, no. 8, pp. 94–125, 2023, doi: 10.1108/ITP-07-2022-0515.

[24] N. Rawindaran, A. Jayal, and E. Prakash, "Exploration of the Impact of Cybersecurity Awareness on Small and Medium Enterprises (SMEs) in Wales Using Intelligent Software to Combat Cybercrime," Computers, vol. 11, no. 12, 2022, doi: 10.3390/computers11120174.

[25] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "Perspective of small and medium enterprises (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales," International Journal of Information Management Data Insights, vol. 3, no. 2, p. 100191, 2023, doi: 10.1016/j.jjimei.2023.100191.

[26] M. I. Khan, S. Tanwar, and A. Rana, "The need for information security management for SMEs," Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020, pp. 328–332, 2020, doi: 10.1109/SMART50582.2020.9337108.

[27] A. H. Adleena Huzaizi, S. N. A. Ahmad Tajuddin, K. A. Bahari, K. A. Manan, and N. N. Abd Mubin, "Cyber-Security Culture towards Digital Marketing Communications among Small and Medium-Sized (SME) Entrepreneurs," Asian Culture and History, vol. 13, no. 2, p. 20, 2021, doi: 10.5539/ach.v13n2p20.

[28] M. Van Haastrecht, I. Sarhan, A. Shojaifar, L. Baumgartner, W. Mallouli, and M. Spruit, "A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs," ACM International Conference Proceeding Series, 2021, doi: 10.1145/3465481.3469199.

[29] A. N. A. Rozmi, P. N. E. Nohuddin, A. R. A. Hadi, M. I. A. Bakar, and A. I. Nordin, "Factors affecting SME owners in adopting ICT in business using thematic analysis," International Journal of Advanced Computer Science and Applications, vol. 11, no. 7, pp. 208–218, 2020, doi: 10.14569/IJACSA.2020.0110727.

[30] O. F. Grooss, M. Presser, and T. Tambo, "Surround yourself with your betters: Recommendations for adopting Industry 4.0 technologies in SMEs," Digital Business, vol. 2, no. 2, p. 100046, 2022, doi: 10.1016/j.digbus.2022.100046.

[31] M. Bada and J. R. C. Nurse, "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)," Information and Computer Security, vol. 27, no. 3, pp. 393–410, 2019, doi: 10.1108/ICS-07-2018-0080.

[32] Awareness, Data Analytics and Assessment, Cyber SA 2020, 2020, doi: 10.1109/CyberSA49311.2020.9139638.

[33] M. Neri, F. Niccolini, and L. Martino, "Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment," Information and Computer Security, 2023, doi: 10.1108/ICS-05-2023-0084.

[34] A. Sukumar, H. A. Mahdiraji, and V. Jafari-Sadeghi, "Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailers," Risk Analysis, vol. 43, no. 10, pp. 2082–2098, 2023, doi: 10.1111/risa 14092.

[35] F. Hoppe, N. Gatzert, and P. Gruner, "Cyber risk management in SMEs: insights from industry surveys," Journal of Risk Finance, vol. 22, no. 3–4, pp. 240–260, 2021, doi: 10.1108/JRF-02-2020-0024.

[36] V. Arya, "Cybersecurity for Small and Medium-sized Enterprises (SMEs)," vol. 5, pp. 7–10, 2022.

[37] [37] C. Ponsard, J. Grandclaudon, and S. Bal, "Survey and Lessons Learned on Raising SME Awareness about Cybersecurity," International Conference on Information Systems Security and Privacy, no. Icissp, pp. 558–563, 2019, doi: 10.5220/0007574305580563.

[38] C. Boletsis, R. Halvorsrud, J. B. Pickering, S. Phillips, and M. Surridge, "Cybersecurity for SMEs: Introducing the human element into socio-technical cybersecurity risk assessment," VISIGRAPP 2021 - Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, vol. 3, no. Visigrapp, pp. 266–274, 2021, doi: 10.5220/0010332902660274.

[39] B. Von Skarczinski et al., "A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises," Information and Computer Security, vol. 3, no. 2, pp. 10–37, 2023, doi: 10.1145/3465481.3469199.

[40] K. AL-Dosari and N. Fetais, "Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach," Electronics (Switzerland), vol. 12, no. 17, 2023, doi: 10.3390/electronics12173629.

[41] C. Ashley and M. Preiksaitis, "Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises," Business Management Research and Applications: A Cross-Disciplinary Journal, vol. 1, no. 2, pp. 109–157, 2022, [Online]. Available: https://bmrajournal.columbiasouthern.edu/index.php/bmra/article/view/3421

[42] A. Mohamad, A. Mohd Rizal, H. Khalid, and T. H. Char Fei, "The Role of Trust in the Digital Interactive Model for SME Speed Internationalisation," International Conference on Research and Innovation in Information Systems, ICRIIS, pp. 1–6, 2021, doi: 10.1109/ICRIIS53035.2021.9617095.

[43] M. Sadok, S. Alter, and P. Bednar, "It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs," Information and Computer Security, vol. 28, no. 3, pp. 467–483, 2020, doi: 10.1108/ICS-01-2019-0010.

[44] A. Emer, M. Unterhofer, and E. Rauch, "A Cybersecurity Assessment Model for Small and Medium-Sized Enterprises," IEEE Engineering Management Review, vol. 49, no. 2, pp. 98–109, 2021, doi: 10.1109/EMR.2021.3078077.

[45] M. H. Husin, N. F. Ibrahim, N. A. Abdullah, S. M. Syed-Mohamad, N. H. Samsudin, and L. Tan, "The Impact of Industrial Revolution 4.0 and the Future of the Workforce: A Study on Malaysian IT Professionals," Soc Sci Comput Rev, vol. 41, no. 5, pp. 1671–1690, 2023, doi: 10.1177/08944393221117268.

[46] Mário Antunes, Marisa Maximiano, Ricardo Gomes, and Daniel Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," Journal of CyberSecurity and Privacy, pp. 219–238, 2021.

[47] S. Chaudhary, V. Gkioulos, and S. Katsikas, "A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises," Comput Sci Rev, vol. 50, no. 830929, p. 100592, 2023, doi: 10.1016/j.cosrev.2023.100592.

[48] M. Tsiodra, S. Panda, M. Chronopoulos, and E. Panaousis, "Cyber Risk Assessment and Optimization: A Small Business Case Study," IEEE Access, vol. 11, no. April, pp. 44467–44481, 2023, doi: 10.1109/ACCESS.2023.3272670.

[49] A. Cartwright, E. Cartwright, and E. S. Edun, "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies," Comput Secur, vol. 131, 2023, doi: 10.1016/j.cose.2023.103288.

[50] A. Chidukwani, S. Zander, and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus, and Recommendations," IEEE Access, vol. 10, no. August, pp. 85701–85719, 2022, doi 10.1109/ACCESS.2022.3197899.

[51] N. Huaman et al., A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. [Online].

Available: https://www.usenix.org/conference/usenixsecurity21/presentation/huaman

[52] T. Ncubukezi, L. Mwansa, and F. Rocaries, "A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses," 2020 15th International Conference for Internet Technology and Secured Transactions, ICITST 2020, 2020, doi: 10.23919/ICITST51030.2020.9351339.

[53] M. Figueredo Franco, F. Martins Lacerda, and B. Stiller, "A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises," Revista de Gestão e Projetos, vol. 13, no. 3, pp. 10–37, 2022, doi: 10.5585/gep.v13i3.23083.

[54] Heyasat, H., Mubarak, S., Evans, N. Security Culture and Security Education, Training and Awareness (SETA) Influencing Information Security Management. In: Daimi, K., Al Sadoon, A. (eds) Proceedings of the Second International Conference on Innovations in Computing Research (ICR'23). Lecture Notes in Networks and Systems, 2023. vol 721. Springer, Cham. https://doi.org/10.1007/978-3-031-35308-6_28

[55] Jonas Schweizer, "Implementation of methods to raise employees' cybersecurity awareness in small businesses."Information Systems, Social aspects. 2025. , p. 86, iv

[56] Tabassum, Jinia. "Challenges and strategies of contemporary cybersecurity awareness training in Swedish SMEs: A qualitative study."Information Systems, Social aspects. 2025. , p. 86, iv

[57] Charalambous, A., & Stavrou, E. Harnessing the Right Talent for SETA Programs: Cybersecurity Roles and Competencies that Make a Difference. 2024. , 130-144. https://doi.org/10.1007/978-3-031-72563-0_10.

[58] Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. Employee Cybersecurity Awareness Training Programs Customized for SME Contexts to Reduce Human-Error Related Security Incidents. Journal of Knowledge Learning and Science Technology ISSN: 2024. 2959-6386 (online). https://doi.org/10.60087/jklst.vol3.n3.p382-409.

[59] A., Huda, M., Brayyich, M., Haroon, N., Khan, A., & Verma, R. An Exploratory Investigation into Sustaining Cybersecurity Protection Through the Implementation of SETA. 2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 292-296. https://doi.org/10.1109/ETNCC63262.2024.10767573.

[60] Tick, A., & Szabó-Harka, N. Analysis of Information Security in a Corporate Environment – a Human Perspective. 2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI), 2-24. 000469-000474. https://doi.org/10.1109/SAMI60510.2024.10432889.