Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 45 (December 2026) PP. 01-28



JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.gaexcellence.com/jistm

CYBERSECURITY READINESS FOR CYBER INSURANCE ADOPTION AMONG SMES: A SYSTEMATIC LITERATURE REVIEW

Hasimah Razak[1]*, Hafiza Abas[2], Ganthan Narayana Samy[3]

[1]Department of Creative Artificial Intelligence, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
hasimah@graduate.utm.my https://orcid.org/0009-0008-5160-2147
[2] Department of Creative Artificial Intelligence, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
hafiza.kl@utm.my https://orcid.org/0000-0003-0137-3127
[3]Department of Business Intelligence, Humanities and Governance, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia
ganthan.kl@utm.my https://orcid.org/0000-0001-6169-3400
*Corresponding Author

Article Info:

Article history:
Received date: 30.09.2026
Revised date: 15.10.2026
Accepted date: 04.11.2026
Published date: 01.12.2026

To cite this document:

Razak, H., Abas, H., & Samy, G. N. (2026). Cybersecurity Readiness for Cyber Insurance Adoption Among SMEs: A Systematic Literature Review. *Journal of Information System and Technology Management, 11* (45), 01-28.

Abstract:

Small and medium-sized enterprises (SMEs) are increasingly dependent on digital technologies to support business operations, creating greater exposure to cyber threats and potential financial losses. Cyber insurance offers a mechanism for transferring certain financial consequences of cyber incidents; however, limited cybersecurity readiness, financial constraints, and insufficient technical expertise may affect the ability of SMEs to adopt appropriate cybersecurity measures and make informed cyber insurance decisions. This systematic literature review aims to identify and synthesise the organisational, technological, and financial factors influencing cybersecurity readiness among SMEs and examine their implications for cyber insurance adoption. The review applies the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, using advanced search strategies in the Scopus and Web of Science databases. Searches were conducted using combinations of the keywords "Cyber Insurance," "Risk Transfer," "Cyber Risk," "Cybersecurity," and "Small and Medium Enterprises," covering publications from January 2022 to August 2026. Following the identification, screening, and eligibility assessment processes, 24 primary studies were included in the final qualitative synthesis. The thematic analysis identified three major themes: (1) Cybersecurity Readiness and Adoption, (2) Cybersecurity Frameworks and Operational Resilience, and (3) Cyber Risk Assessment and Investment Decisions. The findings indicate that cybersecurity awareness, organisational capabilities, security control implementation, operational

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 45 (December 2026) PP. 01-28

resilience, and financial resources are interconnected factors influencing SME cybersecurity preparedness. However, the reviewed studies provide limited direct empirical evidence linking cybersecurity readiness to cyber insurance adoption. The review concludes that a comprehensive approach integrating cybersecurity readiness assessment, operational resilience, and cyber risk investment considerations may provide a foundation for developing a cyber insurance framework tailored to the operational and financial characteristics of SMEs.

DOI: 10.35631/JISTM.1145001

Keywords:

Cyber Insurance, Risk Transfer, Cyber Risk, Cybersecurity, Small Medium Enterprise

© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (http://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact jistm@gaexcllence.com.

Introduction

The digital transformation of society has brought unprecedented opportunities, but it has also exposed organizations and individuals to a rapidly evolving landscape of cyber threats, including ransomware, data breaches, and sophisticated cyber-attacks. As traditional security measures alone are often insufficient to fully protect against these risks, cyber insurance has emerged as a crucial tool for managing and transferring the financial and operational consequences of cyber incidents. Cyber insurance is a contractual agreement between a policyholder and an insurance provider, offering financial protection and support in the event of a cyberattack, and is increasingly recognized as an essential component of comprehensive risk management strategies (Li & Liao, 2023)-(Smyrli et al., 2025). Its adoption has accelerated in recent years, reflecting strong demand from enterprises seeking to safeguard their assets, maintain business continuity, and recover from disruptive incidents. The scope of cyber insurance has expanded to include not only coverage for direct losses but also assistance services, such as incident response and disaster recovery, which are particularly valuable for small and medium-sized enterprises (SMEs) with limited resources (Koch, 2024) (Taskin et al., 2025) .

The significance of cyber insurance in today's digital landscape lies in its ability to complement technical defenses and resilience strategies, providing a safety net when preventive measures fail or are bypassed by increasingly sophisticated attackers (Liu & Zhu, 2026) (Rangu et al., 2023) (Hui et al., 2024) (Zhang et al., 2017) . Insurance providers often require organizations to implement certain security controls before granting coverage, thereby incentivizing the adoption of best practices and enhancing overall cybersecurity posture (Zhang et al., 2017) (Adriko & Nurse, 2024b) . Moreover, the integration of advanced technologies such as Artificial Intelligence (AI) is transforming the cyber insurance industry, enabling more accurate risk assessment, tailored policy plans, and automated claims processing (Alhassani & Alawida, 2025) (Alassaf, Manickam, Odeh, Arfeen, et al., 2025) . Despite its growing importance, the

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 45 (December 2026) PP. 01-28

cyber insurance market faces unique challenges, including the lack of standardized evaluation metrics, pricing inefficiencies, and coverage gaps, which are subjects of ongoing research and development (Paragioudakis et al., 2026) (Alassaf, Manickam, Odeh, ul Arfeen Laghari, et al., 2025) (Jason Nurse et al., 2020) (Marotta et al., 2017) . As digital threats continue to intensify, cyber insurance is poised to play an increasingly vital role in supporting organizations' risk management efforts, ensuring business continuity, and fostering a more resilient digital ecosystem (Smyrli et al., 2025) (Taskin et al., 2025) (Zhang et al., 2017).

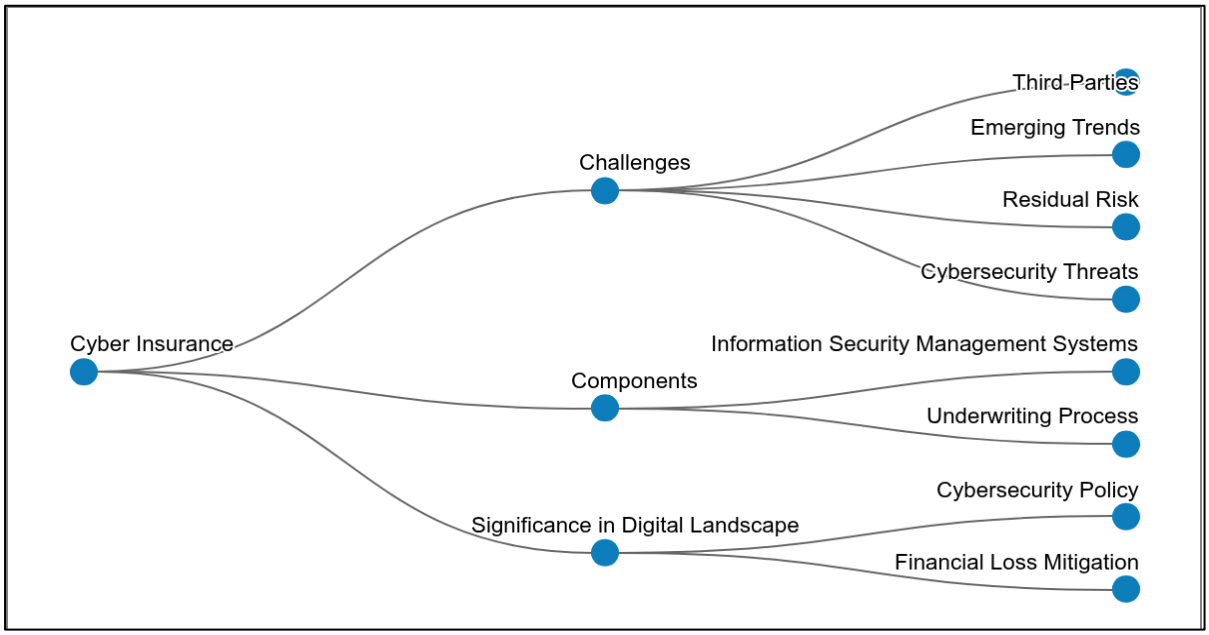


Figure 1.0. Concept Map Of Cyber Insurance: Challenges, Components, And Significance In The Digital Landscape

As illustrated in Figure 1.0, cyber insurance is conceptualised through three key dimensions: challenges, components, and its significance within the digital landscape. The figure highlights third-party risks, emerging trends, residual risks and cybersecurity threats, while emphasising information security management systems, underwriting processes, cybersecurity policies, and financial loss mitigation.

Literature Review

Cyber insurance is a complementary risk-transfer mechanism to cybersecurity investment, designed to cover residual losses that firms cannot fully prevent through technical controls alone. It has grown rapidly as cybercrime costs have risen and traditional commercial general liability policies have narrowed or excluded coverage for electronic data and other cyber harms, yet the market remains underdeveloped relative to the scale of exposure (Zhang et al., 2017) (Marotta et al., 2017) (Romanosky et al., 2019) (Kesan & Hayes, 2017) (Markopoulou, 2021) (Awiszus et al., 2023) .The literature consistently frames cyber insurance as both a financial product and a governance mechanism: firms use it to hedge low-probability, high-impact losses, while insurers use underwriting requirements and pricing to push buyers toward stronger security practices (Majuca et al., 2006) (Franke, 2017). Early work argued that this alignment of incentives could improve social welfare and help correct chronic underinvestment in security caused by interdependent risk and free-riding, and later reviews still present that promise as central to the field (Majuca et al., 2006). At the same time, the strongest cross-

cutting conclusion is that cyber insurance differs from traditional insurance because losses are dynamic, technologically heterogeneous, and often correlated across insureds, making sustainable risk transfer unusually difficult (Marotta et al., 2017) (Biener et al., 2014) (Böhme & Schwartz, 2010) (Awiszus et al., 2023).

A major literature stream examines demand, adoption, and the practical reasons many firms still hesitate to buy coverage. Recent reviews report rising adoption but continued reluctance driven by unclear policy language, high premiums, difficult underwriting, and uncertainty about whether coverage is cost-effective (Haraldsson et al., 2025). Empirical work in Sweden found that insurers impose information-security requirements, decline clients with immature security, and therefore treat cyber insurance not simply as risk transfer but partly as avoidance and mitigation (Franke, 2017). Research focused on Germany similarly found substantial variation in coverages, definitions, and exclusions across policies, with insufficient standardization making it hard for firms to understand what is insured and to build reliable risk-management protocols around those contracts (Cremer et al., 2024). The legal and institutional literature adds that cyber-specific products became necessary because conventional liability forms increasingly exclude cyber losses, while growing third-party liability exposure has made coverage more salient for businesses (Kesan & Hayes, 2017). For SMEs, the evidence suggests both promise and exclusion: insurance can provide financial assistance and access to expertise, but smaller firms often struggle with cyber-risk understanding, policy complexity, affordability, and tougher underwriting in a hardening market (Adriko & Nurse, 2024a).

The supply-side literature is even more unified in identifying pricing and capacity as the market's hardest problems. Across reviews and modeling papers, insurers face sparse and confidential loss data, fast-moving threats, heterogeneous exposure types, and aggregation from common software, shared service providers, and network interdependence (Awiszus et al., 2023) (Haraldsson et al., 2025)(Skeoch & Ioannidis, 2023) These co.nstraints make standard actuarial methods insufficient on their own and explain why cyber pricing models remain immature and weakly validated empirically (Awiszus et al., 2023) (Bardopoulos, 2025). Several papers therefore develop alternative approaches, including copula models for dependent losses, extreme-value methods for severe losses, stochastic diffusion models, and multivariate Hawkes or epidemic-style contagion models for attack propagation and portfolio accumulation (Herath & Herath, 2011) (Skeoch & Ioannidis, 2023) (Bardopoulos, 2025). Recent synthesis organizes the modeling problem into idiosyncratic, systematic, and systemic cyber risks, arguing that classical actuarial frameworks can often handle the first two, whereas systemic risk requires models that explicitly capture contagion and strategic interaction (Awiszus et al., 2023). Even where technical progress is substantial, the literature repeatedly emphasizes that better public or pooled data collection is necessary before pricing accuracy, reinsurance development, and broad market scaling can improve materially (Awiszus et al., 2023) (Skeoch & Ioannidis, 2023) (Bailey, 2020).

Another dominant theme is information asymmetry, especially adverse selection and moral hazard. Reviews across the field identify these as central obstacles to efficient cyber-insurance markets because firms know more than insurers about their own controls, and insureds can change behavior after coverage begins (Haraldsson et al., 2025) (Kesan & Hayes, 2017)(Biener et al., 2014) (Böhme & Schwartz, 2010). Classic economic accounts define adverse selection as high-risk firms disproportionately seeking insurance and moral hazard as weaker post-contract security effort, and these mechanisms are directly relevant to cyber coverage because hidden security posture and hidden effort are pervasive (Acquah, 2026) . Evidence from U.S.

broker data supports the presence of adverse selection: higher-risk firms are more likely both to seek broker assistance and to purchase cyber insurance, while insurers respond primarily by capping coverage rather than pricing risk finely, which constrains total market capacity (Ning, 2026) .Earlier work was more optimistic that rigorous classification and policy provisions could control these frictions, but more recent studies suggest screening remains weakly correlated with true underlying risk and that market hardening reflects unresolved uncertainty rather than full resolution of the asymmetry problem (Majuca et al., 2006) (Ning, 2026) (Adriko & Nurse, 2024a) . Proposed remedies include data-sharing exchanges, premium discounts for stronger controls, official incident reporting, and contract designs that reshape insureds' incentives or risk preferences to reduce moral hazard more directly (Bailey, 2020) (Skeoch & Ioannidis, 2023) (Liu & Zhu, 2022).

Overall, the literature portrays cyber insurance as an important but still imperfect institution. There is broad agreement that it fills a genuine coverage gap, can strengthen resilience, and can create incentives for improved cybersecurity, but there is equally broad agreement that correlated losses, non-stationary threats, ambiguous wordings, limited data, and asymmetric information continue to impede efficient pricing and sustainable capacity (Cremer et al., 2024)(Markopoulou, 2021) (Biener et al., 2014) (Skeoch & Ioannidis, 2023). The market appears to be maturing through stricter underwriting, more differentiated products, and more sophisticated quantitative models, yet the evidence does not support the view that these advances have solved the foundational insurability problem (Awiszus et al., 2023)(Majuca et al., 2006) (Adriko & Nurse, 2024a)(Bardopoulos, 2025). The clearest research agenda points toward standardized policy language, richer loss and exposure databases, stronger insurer–government–research collaboration, better treatment of systemic accumulation, and more tailored products for underserved segments such as SMEs(Kesan & Hayes, 2017) (Bardopoulos, 2025) (Cremer et al., 2024) (Adriko & Nurse, 2024a). In that sense, the cyber insurance literature supports a balanced conclusion: cyber insurance is neither a failed market nor a mature solution, but a necessary and evolving mechanism whose long-term effectiveness depends on better data, clearer contracts, and more credible management of systemic cyber risk.

Research Question

Developing research questions (RQs) is an essential stage in conducting a Systematic Literature Review (SLR), as the questions establish the scope, focus, and direction of the review. Clearly defined RQs guide the identification, selection, and critical evaluation of relevant studies, ensuring that the literature search remains systematic and aligned with the research objectives. The formulation of appropriate questions also helps reduce potential selection bias and supports the collection of relevant evidence. Furthermore, RQs provide a structured basis for organising, analysing, and synthesising findings from the selected literature. This structure enables the identification of recurring patterns, emerging trends, and research gaps while maintaining consistency throughout the review process. Well-articulated RQs also strengthen methodological transparency and reproducibility by allowing subsequent researchers to understand, replicate, or extend the review.

The specification of research questions is recognised as a critical activity during the planning stage of an SLR because it influences the subsequent stages of the review methodology (Kitchenham & Charters, 2021). In accordance with the objective of the present review, Cyber Insurance in SMEs, the PICo framework proposed by (Lockwood et al., 2015) was adopted to

formulate the research questions. PICo comprises three elements: Population (P), Interest (I), and Context (Co). This framework is particulasrly relevant to qualitative evidence synthesis and exploratory reviews because it supports the development of focused research questions by defining the target population, the phenomenon of interest, and the context of the investigation. For the present study, the population comprises small and medium-sized enterprises (SMEs), the interest concerns cybersecurity readiness, cybersecurity frameworks, operational resilience, cyber risk assessment, and investment decisions, while the context relates to cyber risk management and cyber insurance considerations. Based on the three themes identified through the literature review and the application of the PICo framework, three research questions were formulated, as presented below.

- RQ1: What are the key factors influencing cybersecurity readiness and adoption among SMEs in the context of cyber risk management and cyber insurance?
- RQ2: What cybersecurity frameworks and operational resilience practices are proposed or implemented to support cyber risk management among SMEs in the context of cyber insurance?
- RQ3: How do SMEs assess cyber risks and make cybersecurity investment decisions to manage financial exposure and inform cyber insurance considerations?

Material and Methods

This systematic literature review (SLR) was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, an internationally recognised reporting framework designed to enhance the transparency, completeness, and reproducibility of systematic reviews (Page et al., 2021). The PRISMA framework provides a structured approach to documenting the identification, screening, eligibility assessment, and inclusion of relevant studies, thereby facilitating a transparent and methodologically rigorous review process. By integrating predefined eligibility criteria with a systematic search and selection strategy, this study sought to minimise selection bias and ensure a comprehensive synthesis of the available evidence. Scopus and Web of Science (WoS) were selected as the primary bibliographic databases owing to their extensive multidisciplinary coverage, established indexing standards, and accessibility to peer-reviewed scholarly literature relevant to cyber insurance, cybersecurity, and risk transfer.

The review process was organised into four sequential stages: identification, screening, eligibility assessment, and data extraction. During the identification stage, a comprehensive search strategy incorporating predefined keywords, Boolean operators, and relevant search filters was employed to retrieve potentially eligible publications from the selected databases. The screening stage involved removing duplicate records and evaluating the titles and abstracts of the retrieved publications against predetermined inclusion and exclusion criteria. Subsequently, the full texts of potentially relevant articles were systematically assessed to determine their eligibility for inclusion in the final review. Following study selection, data extraction was undertaken to systematically capture, categorise, and synthesise relevant information, including publication characteristics, research methodologies, key findings, and emerging research themes. The extracted evidence was subsequently analysed to identify prevailing research trends, knowledge gaps, and potential directions for future investigation. Through this structured and transparent approach, the review aims to provide a comprehensive evidence base for understanding the role of cyber insurance as a risk transfer mechanism in

cybersecurity risk management, particularly within the context of small and medium-sized enterprises (SMEs).

Identification

The identification phase represents the initial stage of the systematic literature review (SLR), establishing the scope and breadth of the evidence base through a structured and reproducible search strategy. In accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, a comprehensive literature search was conducted using two internationally recognised bibliographic databases, Scopus and Web of Science (WoS), as presented in Table 1. The search strategy incorporated predefined keywords, including "cyber insurance," "cyber liability insurance," "risk transfer," "cybersecurity," and "small medium enterprise," to identify scholarly publications relevant to cyber insurance and cybersecurity risk management among small and medium-sized enterprises (SMEs). The initial search yielded a total of 663 records, comprising 473 publications retrieved from Scopus and 190 from Web of Science. These findings demonstrate the availability of a substantial body of literature addressing cybersecurity, cyber risk management, and insurance-related mechanisms within the SME context, providing an initial evidence base for examining the role of cyber insurance as a risk transfer mechanism.

The selection of Scopus and Web of Science was justified by their established multidisciplinary coverage and complementary indexing capabilities, which facilitate the identification of relevant publications across cybersecurity, insurance, business management, and risk management disciplines. Scopus contributed approximately 71.3% of the retrieved records, compared with 28.7% from Web of Science, indicating a greater retrieval volume from Scopus under the applied search strategy. However, this difference does not necessarily reflect the relative quality or relevance of the indexed publications. Integrating both databases broadened the search coverage and reduced reliance on a single bibliographic source, thereby supporting a more comprehensive identification of potentially relevant studies. The 663 retrieved records subsequently formed the initial dataset for duplicate removal, screening, and eligibility assessment against predefined inclusion and exclusion criteria, ensuring a transparent and systematic selection process aligned with the review objectives.

Table 1: The Search String

Scopus	**TITLE-ABS-KEY (("cyber insurance" OR "cyber liability insurance" OR "cyber risk" OR "risk transfer" OR "cybersecurity") AND ("small medium enterprise" OR SME OR "small business" OR "medium business")) AND (LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (OA , "publisherfullgold")) AND (LIMIT-TO (SUBJAREA , "COMP") OR LIMIT-TO (SUBJAREA , "MULT") OR LIMIT-TO (SUBJAREA , "SOCI") OR LIMIT-TO (SUBJAREA , "BUSI")) AND (LIMIT-TO (PUBYEAR , "2022") OR LIMIT-TO (PUBYEAR , "2023") OR LIMIT-TO (PUBYEAR , "2024") OR**

	LIMIT-TO (PUBYEAR , "2025") OR LIMIT-TO (PUBYEAR , "2026")) **Date of Access: August 2026**
WoS	Refine results for ("cyber insurance" OR "cyber liability insurance" OR "cyber risk" OR "risk transfer" OR "cybersecurity") AND ("small medium enterprise" OR SME OR "small business" OR "medium business") (Topic) and Open Access and 2026 or 2025 or 2024 or 2023 or 2022 (Final Publication Year) and Article (Document Types) and English (Languages) **Date of Access: August 2026**

Screening

Following the identification phase, the 663 retrieved records underwent a systematic screening process based on predefined inclusion and exclusion criteria to ensure their relevance, quality, and alignment with the research objectives. Publications were excluded if they were published before 2022, written in languages other than English, or classified as conference papers, books, or review articles. Additionally, in-press publications, articles outside the subject areas of Computer Science, Business, Management and Accounting, and Social Sciences, and publications not classified as Gold Open Access were excluded. These criteria were established to prioritise recent, accessible, and peer-reviewed journal articles relevant to cyber insurance, cybersecurity, and risk transfer among SMEs.

Consequently, 555 records were excluded, leaving 108 publications comprising 58 records from Scopus and 50 from Web of Science. Subsequently, a deduplication process was performed to identify and remove overlapping records retrieved from both databases. This process eliminated 20 duplicate publications, resulting in 88 unique records retained for subsequent eligibility assessment. The systematic application of these screening criteria enhanced the consistency, transparency, and reproducibility of the study selection process while establishing a focused evidence base for further evaluation.

Table 2: The Selection Criterion is Searching

Criterion	Inclusion	Exclusion
Language	English	Non-English
Time line	2022 – 2026	< 2022
Literature type	Journal (Article)	Conference, Book, Review
Publication Stage	Final	In Press
Subject Area	Computer Science ,Business, Management and Accounting, Social Sciences	Besides Computer Science & Engineering
Open Access	Gold	Besides Gold

Eligibility

Following the screening and deduplication processes, 88 unique articles were retained for eligibility assessment. A comprehensive evaluation was conducted to determine their relevance

and suitability for inclusion in the systematic literature review. Each article was assessed based on its title, abstract, research scope, and full-text availability to ensure alignment with the study objectives, particularly the role of cyber insurance as a risk transfer mechanism in cybersecurity risk management among small and medium-sized enterprises (SMEs). Consequently, 64 articles were excluded due to their focus on unrelated research fields, insufficient relevance of their titles or abstracts to the research objectives, or the unavailability of accessible full texts. These exclusion criteria were systematically applied to ensure that the selected publications provided relevant and sufficient evidence for subsequent qualitative analysis.

Ultimately, 24 articles were retained for the final qualitative synthesis, representing approximately 33% of the 88 records assessed for eligibility. The eligibility assessment established a focused and relevant evidence base, facilitating the systematic examination of existing research findings and the identification of emerging themes, research trends, and knowledge gaps. The selected studies provide a foundation for understanding cyber insurance adoption, cybersecurity risk management practices, and the role of insurance as a risk transfer mechanism among SMEs, thereby informing future research and the development of an appropriate cyber insurance framework.

Data Abstraction and Analysis

An integrative analytical approach was employed to systematically examine and synthesise evidence from the selected studies, facilitating the identification of key themes and subthemes aligned with the research objectives. The analytical process commenced with a comprehensive review of the 24 eligible publications, as detailed in Table 3. Each article was systematically examined to extract relevant information concerning cyber insurance, cybersecurity risk management, and risk transfer mechanisms within the context of small and medium-sized enterprises (SMEs). As illustrated in Figure 2, the extracted evidence was critically evaluated to identify recurring concepts, significant findings, and emerging patterns across the reviewed literature. Particular attention was given to the methodological approaches, analytical perspectives, and principal findings of each study to establish a comprehensive understanding of the existing evidence and its implications for cyber insurance among SMEs.

Subsequently, the authors collaboratively analysed and synthesised the extracted evidence to develop a coherent thematic structure reflecting the key dimensions of cyber insurance within the SME context. Preliminary themes and subthemes were generated through systematic comparison and interpretation of the findings, followed by iterative refinement to ensure their conceptual clarity, consistency, and alignment with the research objectives. Throughout the analytical process, detailed records of interpretations, analytical reflections, and emerging insights were maintained to establish a transparent audit trail and support the traceability of thematic development. The identified themes were subsequently reviewed and refined through collaborative discussions among the research team, with differing interpretations resolved through consensus. This iterative and collaborative process strengthened the credibility, coherence, and methodological rigour of the synthesis, providing an evidence-based foundation for identifying research gaps and informing the development of a cyber insurance framework tailored to the cybersecurity and risk management needs of SMEs.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 45 (December 2026) PP. 01-28

Quality of Appraisal

Following the selection of primary studies, a systematic quality assessment was conducted in accordance with the methodological guidelines proposed by (Kitchenham & Charters, 2021)(Page et al., 2021) to evaluate the methodological rigour, relevance, and credibility of the included publications. The quality assessment framework developed by Anas Abouzahra et al. (Abouzahra et al., 2020) was adopted, comprising six predefined quality assessment (QA) criteria. Each criterion was evaluated using a three-point scoring system: Yes (Y), assigned a score of 1 when the criterion was fully satisfied; Partly (P), assigned a score of 0.5 when the criterion was partially fulfilled or demonstrated certain methodological limitations; and No (N), assigned a score of 0 when the criterion was not satisfied. This structured scoring approach facilitated a consistent and transparent evaluation of the selected studies, enabling quantitative comparison of their methodological quality and supporting the identification of potential limitations within the existing evidence base.

- QA1. Is the purpose of the study clearly stated?
- QA2. Is the interest and the usefulness of the work clearly presented?
- QA3. Is the study methodology clearly established?
- QA4. Are the concepts of the approach clearly defined?
- QA5. Is the work compared and measured with other similar work?
- QA6. Are the limitations of the work clearly mentioned?

The quality assessment (QA) process was systematically conducted using a set of predefined evaluation criteria to ensure the methodological rigour and credibility of the selected studies. Each study was independently evaluated by three experts, who assessed its compliance with the established criteria using a three-point rating scale: Yes (Y), Partly (P), and No (N). The individual ratings were subsequently consolidated to determine an overall quality score for each study. To maintain a consistent standard of methodological quality, a minimum threshold of 3.0 was established, whereby only studies achieving an aggregated quality score exceeding this threshold were retained for subsequent analysis and synthesis. This structured evaluation process facilitated the systematic identification of methodologically sound studies, minimised the inclusion of potentially unreliable evidence, and strengthened the overall credibility and robustness of the review findings.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 45 (December 2026) PP. 01-28

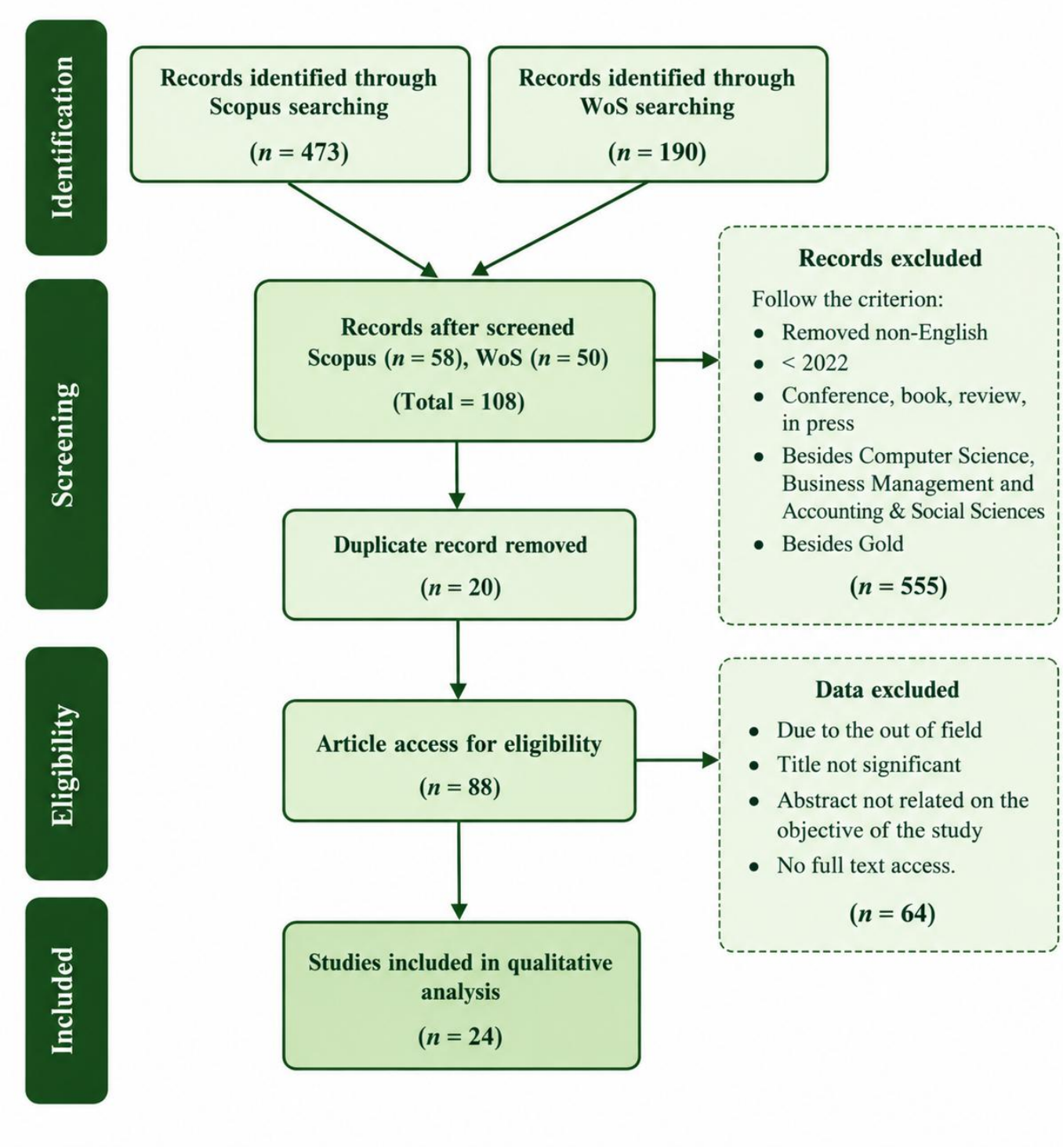


Figure 2.0. Flow Diagram Of The Proposed Searching Study (Kitchenham & Charters, 2021)

Result and Discussion

Quality Assessment Analysis

Based on the systematic quality assessment evaluating all 24 primary papers across six standardized criteria, the review corpus demonstrates a strong overall methodological

foundation, achieving an average quality score of approximately 84% (5.04 out of 6.0). Nearly all selected studies fully met the standards for explicitly defining their core research objectives (QA1) and demonstrating the academic and practical significance of their contributions to small enterprise security (QA2). Furthermore, the majority of papers established transparent methodological designs (QA3) and clearly defined core operational concepts (QA4), spanning rigorous systematic literature reviews, empirical survey analyses, and mathematically formalized resilience models.

The primary variations in quality scores stem from criteria related to comparative evaluation and limitation reporting. A subset of studies received partial ratings for comparative measurement (QA5) because they focused on standalone organizational implementations or localized SME cohorts without directly benchmarking their outcomes against alternative models or previous literature. Similarly, explicit discussion of study limitations and validity threats (QA6) varied, with preliminary exploratory surveys and technical implementations occasionally omitting detailed accounts of potential biases. Nevertheless, the overall high baseline of quality scores confirms that the review corpus provides a reliable, rigorous, and cohesive evidentiary base for synthesizing insights into SME cybersecurity readiness, governance, and technical architecture.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 11 Issue 45 (December 2026) PP. 01-28

Table 3: Number And Details Of Primary Studies Database

Author	Title	QA1	QA2	QA3	QA4	QA5	QA6	Total Mark	Percentage (%)
Quispe-Kobashikawa et al.(Quispe-kobashikawa et al., 2026)	Enhancing Information Security in Technology Small and Medium-Sized Enterprises: A Metrics-Driven Model Based on ISO/IEC 27001:2022 (2026)	1	1	0.5	1	0	0	3.5	58.3
Pawar & Palivela (Pawar et al., 2022)	LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs) (2022)	1	1	1	1	0.5	0	4.5	75.0
Kioskli et al.(Kioskli et al., 2026)	A Human-Centric AI-Enabled Ecosystem for SME Cybersecurity: Cross-Sectoral Practices and Adaptation Framework for Maritime Defence (2026)	1	1	0.5	1	0	0.5	4	66.7
Shabbir et al.(Shabbir et al., 2026)	Cybersecurity Awareness among Women and Youth E-commerce Entrepreneurs in Bangladesh: An Exploratory Factor Analysis (2026)	1	1	0.5	1	0	0	3.5	58.3
Haj Ahmad & Taha (Ahmad, 2026)	Laying the Digital Foundation: Enforcing Minimum Industry 4.0 Standards for New SME Factories in Saudi Arabia (2026)	1	1	0.5	1	1	0	4.5	75.0
Bahmanova & Lace(Bahmanova, 2026)	Predictive Cyber Risk Analytics and Computational Risk Metrics for SME Cyber Resilience Using Time-Series Modelling (2026)	1	1	1	1	1	1	6	100.0
Qazi et al. (Qazi et al., 2026)	Security evaluation framework for cloud ERP systems using NIST and ISO standards (2026)	1	1	1	1	1	1	6	100.0

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 11 Issue 45 (December 2026) PP. 01-28

Türen et al. (Türen et al., 2026)	Agile Resilience in Security for Small and Medium-Sized Businesses (2026)	1	1	0.5	1	1	0.5	5	83.3
Almoaigel & Abuabid (Almoaigel & Abuabid, 2023)	Implementation of Cybersecurity Situation Awareness Model in Saudi SMEs (2023)	1	1	0.5	1	0.5	0	4	66.7
Msomi & Nxumalo (Info et al., 2026)	Assessment of cybersecurity investment and customer trust in SMEs of South Africa (2026)	1	1	0.5	1	0	0	3.5	58.3
Tsiodra et al. (Panaousis, 2023)	Cyber Risk Assessment and Optimization: A Small Business Case Study (2023)	1	1	0.5	1	0.5	0	4	66.7
Manzoor et al. (Id et al., 2024)	Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs (2024)	1	1	0.5	1	1	0	4.5	75.0
Auyporn et al. (Auyporn et al., 2023)	A Study of Distinguishing Factors between SME Adopters versus Non-Adopters of Cybersecurity Standard (2023)	1	1	0.5	1	0	0	3.5	58.3
Maer Matei et al. (Mihaela et al., 2026)	Exploring small business profiles in cybersecurity skills (2026)	1	1	1	1	0.5	0	4.5	75.0
Awan et al. (Awan et al., 2026)	A generative AI-driven cybersecurity framework for small and medium enterprises software development: an ANN-ISM approach (2026)	1	1	1	1	1	1	6	100.0
Bahmanova & Lace (Bahmanova & Lace, 2026)	Key factors shaping collaborative cyber resilience in SMEs through open innovation (2026)	1	1	1	1	0	0	4	66.7
Ilca et al. (Ilca et al., 2023)	Enhancing Cyber-Resilience for Small and Medium-Sized Organizations with	1	1	0.5	1	0.5	1	5	83.3

Journal of Information System and Technology Management
EISSN: 0128-1666
JISTM
Volume 11 Issue 45 (December 2026) PP. 01-28

	Prescriptive Malware Analysis, Detection and Response (2023)								
Soquiat et al.(Soquiat et al., 2026)	Fintech adoption as sustainable finance infrastructure: evidence from SMEs in Batangas province, Philippines (2026)	1	1	0.5	1	0	0	3.5	58.3
Rawindaran et al. (Rawindaran et al., 2023)	Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales (2023)	1	1	0.5	1	0	0	3.5	58.3
Mueck (Mueck, 2026)	ETSI Activities in Artificial Intelligence and Data (2026)	1	1	0.5	1	0	0	3.5	58.3
Perozzo et al. (Perozzo et al., 2023)	CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective (2022)	1	1	1	1	0.5	0	4.5	75.0
Rawindaran et al. (Rawindaran et al., 2025)	Cybersecurity Framework: Addressing Resiliency in Welsh SMEs for Digital Transformation and Industry 5.0 (2025)	1	1	1	1	0.5	0	4.5	75.0
Chan et al.(Chan & Gururajan, 2025)	A Human–AI Collaborative Framework for Cybersecurity Consulting in Capstone Projects for Small Businesses (2025)	1	1	1	1	0.5	0	4.5	75.0
Wan Mohd Ludin et al. (Nur et al., 2024)	Comparative Analysis of Small and Medium-Sized Enterprises Cybersecurity Program Assessment Model (2024)	1	1	0.5	1	1	0	4.5	75.0

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 11 Issue 45 (December 2026) PP. 01-28

Thematic Analysis

The thematic structure of this systematic literature review was established through an inductive analysis of the twenty-fourth included papers to construct a coherent, non-overlapping taxonomy of cyber insurance, small and medium-sized enterprise (SME) and cybersecurity literature. By systematically examining recurring conceptual focus areas, methodological approaches, and core findings across the study corpus, individual contributions were grouped into distinct, academically meaningful categories that reflect primary research trajectories. This synthesis revealed that SME cybersecurity research spans human-centric organizational dynamics, governance and compliance frameworks, and engineering-driven technical safeguards. To capture these dimensions without conceptual overlap, the corpus was synthesized into three major thematic domains: Cybersecurity Readiness and Adoption, Security Cybersecurity Frameworks and Operational Resilience, Cyber Risk Assessment and Investment Decisions. Each article was assigned to a single dominant theme based on its primary research objective, central contribution, and analytical methodology. This thematic organization provides a structured foundation for evaluating how human behavior, governance mechanisms, and technical architectures interact to influence the overall cybersecurity posture and risk profile of resource-constrained enterprise environments.

Table 4: Theme Development Summary

Theme Development Summary	Theme	Focus Area	Number of Articles	Main Research Direction
Theme 1	Cybersecurity Readiness and Adoption	Cybersecurity awareness, skills, organisational preparedness, adoption behaviour, socio-technical factors, and external support.	8	Understanding the factors that enable or constrain SMEs' cybersecurity readiness and adoption of secure practices.
Theme 2	Security Cybersecurity Frameworks and Operational Resilience	Security frameworks, minimum controls, standards, technical solutions, incident prevention,	13	Developing, evaluating, or adapting practical cybersecurity capabilities and operational resilience approaches.

Theme Development Summary	Theme	Focus Area	Number of Articles	Main Research Direction
		detection, response, and recovery.		
Theme 3	Cyber Risk Assessment and Investment Decisions	Cyber risk measurement, predictive analytics, cybersecurity investment, resource allocation, and financial or business outcomes	3	Supporting risk-informed decisions about cybersecurity expenditure and the prioritisation of risk responses.

Cybersecurity Readiness and Adoption

Cybersecurity readiness among small and medium-sized enterprises (SMEs) involves the ability to recognise cyber threats and convert such understanding into suitable security practices. Almoaigel and Abuabid (Almoaigel & Abuabid, 2023) identified a significant positive relationship between cybersecurity situational awareness and the implementation of cybersecurity controls among Saudi SMEs. However, awareness should not be interpreted as evidence that adequate protection has already been established. Auyporn et al. (Auyporn et al., 2023) examined 312 Thai SMEs and found that 204 enterprises (65.4%) had not adopted a cybersecurity standard, while 108 (34.6%) had adopted at least one. Adoption differed according to organisational size, IT usage, security staffing, investment, risk awareness and perceived customer requirements. Shabbir et al. (Shabbir et al., 2026) examined 244 women and youth e-commerce entrepreneurs in Bangladesh and identified related dimensions involving risk perception, digital literacy, security practices, cybersecurity knowledge, training and institutional support. These findings indicate that understanding threats, possessing relevant skills and implementing controls represent connected but distinct aspects of readiness. Perozzo et al. (Perozzo et al., 2023) (Perozzo et al., 2022) provide further explanation through a socio-technical readiness model applied to three manufacturing SMEs in Italy. The study identified contrasting organisational profiles: an enterprise with limited awareness and protection, an enterprise that relied heavily on an external IT provider without sufficient internal oversight, and an enterprise with more developed preparation but remaining weaknesses in protection systems. The cases demonstrate that confidence in existing arrangements does not necessarily reflect actual readiness. Maer Matei et al. (Mihaela et al., 2026) similarly identified disengaged (16%), partially engaged (52%) and proactive (32%) cybersecurity profiles among 9,136 small European companies. Partially engaged enterprises recognised cybersecurity as important but did not invest in employee training, whereas proactive enterprises combined internal capabilities, external expertise and training.

Collectively, these studies support an assessment of readiness that considers management awareness, employee capability, implemented safeguards and evidence of continuing security activities rather than relying on perceived preparedness alone.

Organisational resources, management responsibility and external support influence the capacity of SMEs to adopt and maintain cybersecurity measures. Perozzo et al. (Perozzo et al., 2023) proposed a readiness model incorporating company size, governance, technical skills, business characteristics, dependence on third parties, existing protection systems and legal compliance. The Italian case findings indicate that outsourcing IT activities does not remove the need for internal cybersecurity responsibility or supplier oversight. Similarly, Auyporn et al. (Auyporn et al., 2023) identified differences in cybersecurity-standard adoption associated with security personnel and technology investment. Maer Matei et al. (Mihaela et al., 2026) found that proactive cybersecurity engagement was associated with the availability of relevant expertise and employee training, highlighting the importance of organisational capability beyond management recognition of cyber risks. Rawindaran et al. (Rawindaran et al., 2023) examined 34 SMEs in Wales and identified financial constraints, shortages of specialist knowledge and implementation difficulties as barriers to cybersecurity improvement. The study also considered the relationship between SMEs and government agencies, indicating the relevance of accessible guidance and institutional assistance. Bahmanova and Lace(Bahmanova & Lace, 2026) examined collaborative cyber resilience through a literature review and interviews with representatives of 14 European SMEs. The findings identified technological, human, organisational, financial, regulatory and collaborative factors, with knowledge sharing and external partnerships presented as possible responses to limited internal resources. Shabbir et al. (2026) likewise identified training and institutional support as elements associated with the measured dimensions of cybersecurity awareness. Across these studies, resource limitations help explain why recognising cybersecurity risks may not lead immediately to control adoption. External expertise can assist implementation, but an enterprise still needs to establish responsibility for security decisions and monitor the protection of business information. Readiness assessment should therefore consider whether security measures are supported by suitable personnel, funding, governance arrangements and ongoing oversight.

The relationship between digital adoption and cybersecurity readiness requires further distinction when considering cyber insurance among SMEs. Soquiat et al. (Soquiat et al., 2026) surveyed 349 SMEs in Batangas Province, Philippines, and found substantial utilisation of mobile banking, online banking and e-banking. The study also identified security and data-privacy concerns as barriers to financial-technology utilisation. However, the research examined digital financial services rather than the effectiveness of cybersecurity controls or the adoption of cyber insurance. Digital-service utilisation should therefore be treated as an indication of business dependence on technology, not as proof of cybersecurity readiness. Perozzo et al. (Perozzo et al., 2022) provide a related perspective by distinguishing business-context characteristics from organisational capabilities that management can improve. The proposed socio-technical model considers dependence on online services and third parties alongside governance, technical skills and existing safeguards. Its application to three Italian manufacturing SMEs indicates that businesses with different operating arrangements may require different cybersecurity strategies. Almoaigel and Abuabid (Perozzo et al., 2022) , Auyporn et al. (Auyporn et al., 2023) and Maer Matei et al. (Mihaela et al., 2026) further demonstrate the importance of distinguishing awareness, adoption of standards and investment in practical capabilities. Taken together, the eight selected studies support a multidimensional

understanding of cybersecurity readiness comprising risk awareness, employee skills, organisational resources, governance, implemented controls and access to external assistance. The findings also indicate that readiness assessments should reflect the digital activities and operating conditions of individual SMEs. For the study of Cyber Insurance in SMEs, these dimensions provide a basis for examining whether organisational preparedness is associated with insurance-related decisions. Nevertheless, the selected papers do not establish that stronger cybersecurity readiness directly increases cyber insurance purchasing, determines policy eligibility or reduces insured losses. The relationship between readiness and cyber insurance adoption requires separate empirical investigation.

Cybersecurity Frameworks and Operational Resilience

Cybersecurity frameworks for small and medium-sized enterprises (SMEs) need to provide security requirements that can be implemented with limited financial resources, technical expertise and personnel. Pawar and Palivela (Pawar et al., 2022)(Mihaela et al., 2026) developed the Least Cybersecurity Controls to be Implemented (LCCI) framework to support SMEs in identifying important information assets and introducing security controls according to business priorities. The proposed implementation levels allow enterprises to establish essential protection before expanding cybersecurity activities. Wan Mohd Ludin et al. (Nur et al., 2024) compared cybersecurity assessment models and discussed differences in flexibility, maturity measurement and suitability for smaller organisations. Both studies indicate that selecting a framework requires consideration of the enterprise's operating conditions rather than adopting every requirement without prioritisation. Rawindaran et al. (Rawindaran et al., 2025) similarly examined cybersecurity resilience among Welsh SMEs in the context of digital transformation and Industry 5.0, considering technological, organisational and human factors when developing an enhanced framework. Haj Ahmad and Taha (Ahmad, 2026) proposed a minimum digital-maturity threshold for newly established SME factories in Saudi Arabia, incorporating organisational processes, technology and digital capabilities. Although the proposed threshold addresses industrial digital readiness rather than cybersecurity alone, its consideration of connected systems and organisational preparation is relevant to establishing security-management requirements. Mueck (Mueck, 2026) examined the development of artificial intelligence and data standards by the European Telecommunications Standards Institute (ETSI). The paper describes baseline cybersecurity requirements for AI systems comprising 13 core design principles and 72 trackable principles across five lifecycle phases. Its discussion of data in transit, at rest and in process provides a standards-related perspective on protecting digital operations. However, Mueck (Mueck, 2026) does not empirically evaluate the implementation of these standards in SMEs. Collectively, the studies indicate that cybersecurity frameworks should combine prioritised controls, organisational readiness and relevant technical requirements. The evidence also distinguishes proposed frameworks and standards guidance from demonstrated improvements in SME security outcomes.

Operational resilience extends cybersecurity beyond preventing attacks to include detecting incidents, maintaining essential activities and restoring affected systems. Manzoor et al. (Id et al., 2024) (Mueck, 2026) evaluated open-source security information and event management solutions in simulated SME network environments, considering detection features, processing performance, scalability and compliance-related capabilities. The findings demonstrate the relevance of technical suitability when selecting monitoring tools, particularly where SMEs have limited budgets and specialist personnel. Ilca et al. (Ilca et al., 2023) investigated an integrated open-source approach combining malware analysis, detection and response

functions. The reported testing supports the potential of coordinated tools to assist threat identification, although deployment and maintenance still require appropriate technical capability. Awan et al. (Awan et al., 2026) developed an artificial intelligence-based cybersecurity framework for SME software development, combining an artificial neural network with interpretive structural modelling to support threat identification and the organisation of mitigation measures. These studies address different technical environments but share an emphasis on selecting security measures that SMEs can apply within available resources. Türen et al. (Türen et al., 2026) extend this discussion through an agile resilience framework incorporating incident-response procedures, defined responsibilities, backup arrangements, restoration checks and post-incident improvement. Pawar and Palivela (Pawar et al., 2022) similarly emphasise the identification of critical assets and the prioritisation of controls according to confidentiality, integrity and availability requirements. Bahmanova and Lace (Bahmanova & Lace, 2026) examine resilience through a mathematical model integrating organisational security, cyber risk exposure, cybersecurity capability, incident response, recovery and digital maturity. The model treats resilience as a condition that changes over time rather than a fixed result of a single assessment. Together, these findings indicate that installed security tools represent only one component of operational resilience. Effective incident management also requires assigned responsibilities, procedures for responding to disruptions and arrangements for restoring essential business services. Nevertheless, technical experiments, proposed frameworks and simulated resilience measures do not independently establish sustained improvements in recovery performance across operating SMEs.

The selected studies further indicate that cybersecurity frameworks require continuing improvement as technologies, business activities and organisational capabilities change. Kioskli et al. (Kioskli et al., 2026) proposed a human-centred cybersecurity ecosystem combining tool selection with competency-based training. Reported training outcomes indicate improvements in participant knowledge, although further evaluation is necessary to establish the effectiveness of the proposed approach in different operating environments. Chan et al. (Chan & Gururajan, 2025) (developed a human–AI collaborative consulting framework that connects small businesses with cybersecurity expertise, tools and educational resources. Both studies consider external assistance and employee capability alongside technical protection. Rawindaran et al. (Rawindaran et al., 2025) likewise emphasise continuing improvement across human, organisational and technological dimensions. Bahmanova and Lace (Bahmanova & Lace, 2026) contribute a dynamic assessment approach through mathematical modelling and scenario analysis, illustrating how changes in cyber risk and organisational capability may affect calculated resilience over time. However, simulated outcomes should not be interpreted as observed reductions in incidents or financial losses. Mueck (Mueck, 2026) adds a standards perspective by describing cybersecurity requirements across the AI lifecycle and work on interoperable data solutions. The paper provides relevant guidance for organisations adopting AI and data-driven technologies but does not establish the effectiveness of these requirements through SME implementation results. Across the 13 selected papers, cybersecurity frameworks address several connected activities: identifying minimum controls, assessing digital and organisational capabilities, selecting suitable tools, preparing for incidents, supporting recovery and reviewing security arrangements over time. For research on cyber insurance among SMEs, these activities provide possible dimensions for examining organisational preparedness and operational resilience. However, the reviewed findings do not establish that adopting a particular framework directly increases cyber insurance purchasing, satisfies an insurer's eligibility requirements or reduces insured losses. These insurance-related

relationships require separate empirical investigation before inclusion as validated outcomes of a cyber insurance framework.

Cyber Risk Assessment and Investment Decisions

Cyber risk assessment and investment decisions among small and medium-sized enterprises (SMEs) require consideration of financial limitations, potential incident consequences and the effectiveness of selected security measures. Tsiodra et al. (Panaousis, 2023) developed the CENSOR decision-support framework to examine cybersecurity investment under budget constraints. The framework incorporates uncertainty in vulnerability exploitation, the progression of cyberattacks and the financial consequences of security breaches. Using a small-business case study based on the 2020 Common Weakness Enumeration list of 25 dangerous software weaknesses and the Center for Internet Security Controls, the study compared Set Covering and Knapsack optimisation methods. Within the examined case, the Knapsack method identified control combinations that were more affordable and associated with lower calculated risk than the Set Covering alternatives. The findings also indicated that additional cybersecurity expenditure did not always produce a proportional reduction in estimated risk. Consequently, investment decisions require consideration of the effectiveness and cost of individual controls rather than an assumption that higher expenditure automatically provides greater protection. Bahmanova and Lace (Bahmanova & Lace, 2026) examined cyber risk from a different perspective by developing a mathematical framework that represents organisational resilience as a changing condition. The model integrates company security, cyber risk exposure, cybersecurity capability, incident response and recovery, and digital maturity. An illustrative simulation covering twelve monthly periods showed an increase in the calculated resilience score from 0.548 to 0.731, representing approximately 33.4% growth under the specified assumptions. The framework also supports comparison of alternative cybersecurity scenarios and examination of changes in organisational capability over time. However, the simulated improvement does not demonstrate an equivalent reduction in actual financial losses. Msomi and Nxumalo (Info et al., 2026) investigated cybersecurity investment and customer trust using 375 valid survey responses from SME owners and senior managers in KwaZulu-Natal, South Africa. The study reported a positive relationship between cybersecurity investment and customer trust ($r = 0.312$, $p < 0.001$), with investment explaining 9.7% of the variation in customer trust. These findings indicate that investment decisions may involve business-related considerations beyond technical risk reduction. Nevertheless, customer trust, calculated cyber risk and simulated resilience represent different outcomes and should not be treated as interchangeable measures of cybersecurity investment.

The combined findings also indicate that cyber risk assessment should consider uncertainty and changing organisational conditions when supporting SME investment decisions. Tsiodra et al. (Panaousis, 2023) incorporated uncertainty concerning the time required to exploit vulnerabilities and the financial consequences of attacks into CENSOR. The framework allows alternative security controls to be compared according to estimated risk and available budgets, providing a structured basis for allocating limited financial resources. However, the case-study results depend on the selected vulnerabilities, controls and modelling assumptions. Bahmanova and Lace (Bahmanova & Lace, 2026) similarly identified limitations in assessments that describe cybersecurity capability at only one point in time. The proposed Dynamic Resilience Index combines resilience level, temporal stability and growth to support the examination of organisational conditions across successive periods. Its forecasting component produced small errors when compared with simulated resilience values, but the results do not establish

forecasting accuracy for operating SMEs because the evaluation used synthetic data. Empirical calibration and longitudinal organisational observations remain necessary before applying the model to actual investment decisions. Msomi and Nxumalo (Info et al., 2026) contributed survey-based evidence concerning the relationship between cybersecurity expenditure and business confidence. Participating SMEs reporting investment in secure digital payment systems, data protection and employee cybersecurity awareness also reported stronger customer confidence and perceived business credibility. Nevertheless, the cross-sectional analysis does not demonstrate that individual security measures directly caused improvements in customer trust. The relatively limited proportion of explained variation further indicates that cybersecurity investment is not the only consideration associated with customer confidence. Across the three studies, investment decisions can be examined through complementary dimensions comprising estimated cyber risk, control-selection costs, organisational resilience and business-related outcomes. For cyber insurance research, these findings provide a basis for investigating whether SMEs can identify significant cyber risks, allocate resources to appropriate safeguards and evaluate potential consequences of cyber incidents. However, the selected studies do not directly establish how cybersecurity expenditure affects insurance purchasing, premium affordability, policy eligibility or insured losses. Such relationships require separate empirical investigation before cybersecurity investment indicators can be incorporated into a validated cyber insurance framework for SMEs.

Conclusion

This systematic literature review examined cybersecurity readiness for cyber insurance adoption among small and medium-sized enterprises (SMEs), with particular attention to the factors influencing cybersecurity preparedness, the suitability of cybersecurity frameworks and operational resilience practices, and the role of cyber risk assessment in investment decisions. The review applied the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to identify and assess English-language, Gold Open Access journal articles published between January 2022 and August 2026. Advanced searches of the Scopus and Web of Science databases identified 663 records, of which 24 primary studies were retained for qualitative synthesis following screening, duplicate removal and eligibility assessment. The review addressed three research questions concerning the factors influencing cybersecurity readiness and adoption, the cybersecurity frameworks and resilience practices relevant to SMEs, and the approaches used to assess cyber risks and allocate cybersecurity resources.

The thematic synthesis identified three interconnected areas: Cybersecurity Readiness and Adoption, Cybersecurity Frameworks and Operational Resilience, and Cyber Risk Assessment and Investment Decisions. The first theme indicates that cybersecurity awareness alone is insufficient to establish organisational readiness. Employee skills, management responsibility, available resources, implemented safeguards and external support also influence the ability of SMEs to adopt and maintain cybersecurity practices. The second theme highlights the importance of selecting cybersecurity frameworks and technical controls that reflect organisational size, operational requirements and available capabilities. Operational resilience also requires incident detection, response procedures, recovery arrangements and continuous improvement rather than reliance on preventive technologies alone. The third theme demonstrates the relevance of structured cyber risk assessment and cost-effective resource allocation, particularly where financial constraints limit cybersecurity investment. Across the selected studies, survey research, organisational case studies, framework development, technical evaluations and mathematical modelling provide different perspectives on SME

cybersecurity preparedness. However, evidence derived from proposed frameworks and simulated models should be distinguished from outcomes demonstrated through implementation in operating enterprises.

The principal contribution of this review is the integration of fragmented cybersecurity findings into three thematic dimensions relevant to the investigation of cyber insurance adoption among SMEs. The synthesis provides a structured basis for examining organisational preparedness through cybersecurity awareness and capability, operational resilience through the implementation and maintenance of suitable controls, and financial preparedness through cyber risk assessment and investment decisions. These dimensions may assist SME owners and managers in identifying cybersecurity gaps, prioritising essential safeguards and considering the financial consequences of cyber incidents. The findings may also inform the development of targeted cybersecurity guidance, training programmes and support mechanisms for SMEs with limited internal expertise. For cyber insurance research, the thematic structure identifies potential factors for subsequent investigation of insurance awareness, purchasing decisions, affordability and coverage requirements. Nevertheless, the reviewed studies provide limited direct empirical evidence establishing how cybersecurity readiness influences cyber insurance adoption. Consequently, the proposed thematic dimensions should be regarded as a foundation for further investigation rather than a validated model of insurance purchasing behaviour.

The review is subject to limitations arising from its restriction to Scopus and Web of Science, English-language publications, Gold Open Access journal articles and the January 2022–August 2026 publication period. These criteria may have excluded relevant studies published in other languages, databases, publication formats or access categories. Differences in research methods, geographical settings and organisational characteristics also limit direct comparison across the included studies. Future research should examine the relationship between cybersecurity readiness and actual cyber insurance adoption through empirical investigation involving SME owners, cybersecurity professionals and insurance practitioners. Particular attention should be given to the influence of security capabilities, risk perception, premium affordability, policy requirements and perceived insurance benefits on purchasing decisions. Further studies should also evaluate whether cybersecurity readiness assessments can support the development of a practical cyber insurance framework that reflects the operational and financial conditions of SMEs. Overall, this systematic review establishes an evidence-based foundation for connecting cybersecurity preparedness with future research on cyber insurance adoption, while identifying the empirical work required to clarify that relationship and support more informed cyber risk management decisions among SMEs.

Acknowledgements: The authors would like to express their sincere gratitude to University Teknologi Malaysia (UTM) for providing the necessary resources and support throughout the course of this research. Special appreciation is extended to colleagues and peers who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.

Funding Statement: No Funding

Conflict of Interest Statement: The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the Journal of Information System and Technology Management (JISTM).

Ethics Statement: This study did not involve any human participants, animals, or sensitive data requiring ethical approval. The authors confirm that the research was conducted in accordance with accepted academic integrity and ethical publishing standards.

Author Contribution Statement: All authors contributed significantly to the development of this manuscript. Hasimah Razak was responsible for the conceptualization, methodology, and overall supervision of the study. Dr Hafiza Abas handled data collection, analysis, and interpretation of results. Dr Ganthan Narayana Samy contributed to the literature review, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript prior to submission.

References

Abouzahra, A., Sabraoui, A., & Afdel, K. (2020). Model composition in Model Driven Engineering: A systematic literature review. Information and Software Technology, 125(May), 106316. https://doi.org/10.1016/j.infsof.2020.106316

Acquah, E. (2026). Adverse Selection and Moral Hazards: Information Asymmetry as a Source of Market Failures in Insurance and Finance. American Journal of Applied Statistics and Economics. https://doi.org/10.54536/ajase.v5i1.6099

Adriko, R., & Nurse, J. (2024a). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review. Inf. Comput. Secur., 32, 691–710. https://doi.org/10.1108/ics-01-2024-0025

Adriko, R., & Nurse, J. R. C. (2024b). Does Cyber Insurance Promote Cyber Security Best Practice? An Analysis Based on Insurance Application Forms. Digital Threats: Research and Practice, 5(3). https://doi.org/10.1145/3676283

Ahmad, K. H. (2026). Laying the Digital Foundation : Enforcing Minimum Industry 4 . 0 Standards for New SME Factories in Saudi Arabia. 1–20.

Alassaf, N., Manickam, S., Odeh, A., Arfeen, S. U., & Anbar, M. (2025). The Future of AI in Cybersecurity Insurance. In Cybersecurity Insurance Frameworks and Innovations in the AI Era (pp. 139–178). IGI Global. https://doi.org/10.4018/979-8-3373-1977-3.ch006

Alassaf, N., Manickam, S., Odeh, A., ul Arfeen Laghari, S., Anbar, M., Aboshgifa, A., & Belhaj, N. (2025). Leveraging AI to Establish Cybersecurity Insurance Benchmarks and Guidelines: Standards in Cybersecurity Insurance. In AI-Driven Cybersecurity Insurance: Innovations in Risk, Governance, and Digital Resilience (pp. 111–150). IGI Global. https://doi.org/10.4018/979-8-3373-5545-0.ch005

Alhassani, M., & Alawida, M. (2025). Re-Shaping the World of Cyber Insurance: A New Era of AI in the Cyber World. In Cybersecurity Insurance Frameworks and Innovations in the AI Era (pp. 1–20). IGI Global. https://doi.org/10.4018/979-8-3373-1977-3.ch001

Almoaigel, M. F., & Abuabid, A. (2023). Implementation of Cybersecurity Situation Awareness Model in Saudi SMEs. 14(11), 1082–1092.

Auyporn, W., Piromsopa, K., & Chaiyawat, T. (2023). A Study of Distinguishing Factors between SME Adopters versus Non-Adopters of Cybersecurity Standard. 1(1).

Awan, M., Alam, A., Khan, R. A., & Alwageed, H. S. (2026). OPEN A generative AI-driven cybersecurity framework for small and medium enterprises software development : an ANN-ISM approach. 1–41.

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2023). Modeling and pricing cyber insurance. European Actuarial Journal, 13(1). https://doi.org/10.1007/s13385-023-00341-9

Bahmanova, A. (2026). Predictive Cyber Risk Analytics and Computational Risk Metrics for SME Cyber Resilience Using Time-Series Modelling.

Bahmanova, A., & Lace, N. (2026). Journal of Open Innovation : Technology , Market , and Complexity Key factors shaping collaborative cyber resilience in SMEs through open innovation. Journal of Open Innovation: Technology, Market, and Complexity, 12(1), 100715. https://doi.org/10.1016/j.joitmc.2026.100715

Bailey, L. (2020). Mitigating Moral Hazard in Cyber-Risk Insurance. https://consensus.app/papers/mitigating-moral-hazard-in-cyberrisk-insurance-bailey/6f7952ad3ee151bd85c1373b88f6f9e4/

Bardopoulos, J. (2025). Cyber-insurance pricing models. British Actuarial Journal, 30. https://doi.org/10.1017/s1357321724000205

Biener, C., Eling, M., & Wirfs, J. H. (2014). Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance - Issues and Practice, 40, 131–158. https://doi.org/10.1057/gpp.2014.19

Böhme, R., & Schwartz, G. (2010). Modeling Cyber-Insurance: Towards a Unifying Framework. https://consensus.app/papers/modeling-cyberinsurance-towards-a-unifying-framework-böhme-schwartz/500c91826638542fa5a8f29e1866f927/

Chan, K. C., & Gururajan, R. (2025). A Human – AI Collaborative Framework for Cybersecurity Consulting in Capstone Projects for Small Businesses.

Cremer, F., Sheehan, B., Fortmann, M., Mullins, M., Murphy, F., & Materne, S. (2024). Bridging the cyber protection gap: An investigation into the efficacy of the German cyber insurance market. Risk Management and Insurance Review, 27(1), 57–87. https://doi.org/10.1111/rmir.12261

Franke, U. (2017). The cyber insurance market in Sweden. Computers and Security, 68. https://doi.org/10.1016/j.cose.2017.04.010

Haraldsson, A.-L., Padyab, A., & Salek, A. Al. (2025). Bridging the Gap Between Businesses and Insurers: A Systematic Review of Cyber Insurance Research. International Journal of Information Security and Cybercrime. https://doi.org/10.19107/ijisc.2025.02.01

Herath, H., & Herath, T. (2011). Copula Based Actuarial Model for Pricing Cyber-Insurance Policies. 2. https://consensus.app/papers/copula-based-actuarial-model-for-pricing-cyberinsurance-herath-herath/e84be1ef0b0b5ef4abd8eff10baed72e/

Hui, W., Hui, K.-L., & Yue, W. T. (2024). Cyber Insurance and Post-Breach Services: A Normative Analysis. Service Science, 16(2), 124–141. https://doi.org/10.1287/serv.2021.0120

Id, J. M., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget : Evaluating security and performance of open-source SIEM solutions for SMEs. 1–24. https://doi.org/10.1371/journal.pone.0301183

Ilca, L. F., Lucian, P., & Balan, T. C. (2023). Enhancing Cyber-Resilience for Small and Medium-Sized and Response.

Info, A., On, R., On, R., On, A., Print, I., & Online, I. (2026). Assessment of cybersecurity investment and customer trust in SMEs of South Africa. https://doi.org/10.21511/ppm.24(3).2026.06

Jason Nurse, R. C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., & Creese, S. (2020). The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020. https://doi.org/10.1109/CyberSA49311.2020.9139703

Kesan, J., & Hayes, C. (2017). Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment. Minnesota Law Review. https://doi.org/10.2139/ssrn.2924854

Kioskli, K., Seralidou, E., Mallouli, W., Koutras, D., Tomás, P., & Kallergis, D. (2026). A Human-Centric AI-Enabled Ecosystem for SME Cybersecurity : Cross-Sectoral Practices and Adaptation Framework for Maritime Defence. 1–19.

Kitchenham, B., & Charters, S. M. (2021). Guidelines for performing Systematic Literature Reviews in Software Engineering Guidelines for performing Systematic Literature Reviews in Software Engineering. October.

Koch, R. (2024). Current developments in cyber insurance. Zeitschrift fur die gesamte Versicherungswissenschaft, 113(1), 11–53. https://doi.org/10.3790/zverswiss.2024.1430501

Li, Z., & Liao, Q. (2023). Does Cyber-Insurance Benefit the Insured or the Attacker? – A Game of Cyber-Insurance. In F. J., K. T., & H. Y. (Eds.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes

in Bioinformatics): Vol. 14167 LNCS (pp. 23–42). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-50670-3_2

Liu, S., & Zhu, Q. (2022). Mitigating Moral Hazard in Cyber Insurance Using Risk Preference Design. ArXiv, abs/2203.12001. https://doi.org/10.48550/arxiv.2203.12001

Liu, S., & Zhu, Q. (2026). Cyber Insurance for Cyber Resilience. In Autonomous Cyber Resilience (pp. 139–181). wiley. https://doi.org/10.1002/9781394215416.ch06

Lockwood, C., Munn, Z., & Porritt, K. (2015). Qualitative research synthesis: Methodological guidance for systematic reviewers utilizing meta-aggregation. International Journal of Evidence-Based Healthcare, 13(3), 179–187. https://doi.org/10.1097/XEB.0000000000000062

Majuca, R., Yurcik, W., & Kesan, J. (2006). The Evolution of Cyberinsurance. ArXiv, abs/cs/0601020. https://doi.org/10.48550/arxiv.cs/0601020

Markopoulou, D. (2021). Cyber-insurance in EU policy-making: Regulatory options, the market's challenges and the US example. Comput. Law Secur. Rev., 43, 105627. https://doi.org/10.1016/j.clsr.2021.105627

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. Computer Science Review, 24, 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001

Mihaela, M., Matei, M., & Năstasă, A. (2026). Exploring small business profiles in cybersecurity skills. 17(1), 87–110. https://doi.org/10.47743/ejes-2026-0104

Mueck, M. (2026). ETSI Activities in Artificial Intelligence and Data. 14, 255–258. https://doi.org/10.13052/jicts2245-800X.1425

Ning, D. (2026). Selection and Screening in Cyber Insurance Markets. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.6147910

Nur, W., Wan, E., Ludin, M., Mohd, M., Fariza, W., & Fauzi, P. (2024). Comparative Analysis of Small and Medium-Sized Enterprises Cybersecurity Program Assessment Model. 15(8), 796–804.

Page, M. J., McKenzie, J. E., Bossuyt, P., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The prisma 2020 statement: An updated guideline for reporting systematic reviews. Medicina Fluminensis, 57(4), 444–465. https://doi.org/10.21860/medflum2021_264903

Panaousis, E. (2023). Cyber Risk Assessment and Optimization : A Small Business Case Study. IEEE Access, 11(April), 44467–44481. https://doi.org/10.1109/ACCESS.2023.3272670

Paragioudakis, A., Komninos, N., Smyrlis, M., Spanoudakis, G., & Kloukinas, C. (2026). Risk management for cyber insurance: a survey for data-driven approaches with the use of AI. International Journal of Information Security, 25(4). https://doi.org/10.1007/s10207-026-01275-5

Pawar, S., Palivela, H., & Ph, D. (2022). International Journal of Information Management Data Insights LCCI : A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

Perozzo, H., Ravarini, A., & Zaghloul, F. (2022). Assessing Cybersecurity Readiness within SMEs: Proposal of a Socio-Technical based Model. CEUR Workshop Proceedings, 3239, 22–32.

Perozzo, H., Zaghloul, F., & Ravarini, A. (2023). CyberSecurity Readiness : A Model for SMEs based on the Socio-Technical Perspective. 33, 53–66.

Qazi, A., Arshad, S., Ali, A., & Jadoon, K. (2026). Security evaluation framework for cloud ERP systems using NIST and ISO standards. 1–18.

Quispe-kobashikawa, G., Zuloaga-estrada, C., Mansilla-lopez, J., & Garcia-nunez, A. D. (2026). Enhancing Information Security in Technology Small and Medium-Sized Enterprises : A Metrics-Driven Model Based on ISO / IEC. 16(2), 34316–34326.

Rangu, C. M., Pană, N., & Șcheau, M. C. (2023). Cyber Risk Insurance Framework Considerations. In Contributions to Finance and Accounting: Vol. Part F1313 (pp. 383–401). Springer Nature. https://doi.org/10.1007/978-3-031-34082-6_15

Rawindaran, N., Jayal, A., & Prakash, E. (2025). Cybersecurity Framework : Addressing Resiliency in Welsh SMEs for Digital Transformation and Industry 5 . 0.

Rawindaran, N., Jayal, A., Prakash, E., Hewage, C., & Cf, C. (2023). International Journal of Information Perspective of small and medium enterprise (SME ' s) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. International Journal of Information Management Data Insights, 3(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? Journal of Cybersecurity, 5(1). https://doi.org/10.1093/cybsec/tyz002

Shabbir, M. S., Karim, F., Zayed, N. M., Monir, S., Bipasha, M. S., Edeh, F. O., Alhebri, A., Jaradat, M., & Bansal, A. (2026). Cybersecurity Awareness among Women and Youth E-commerce Entrepreneurs in Bangladesh : An Exploratory Factor Analysis. 16(5), 333–346.

Skeoch, H., & Ioannidis, C. (2023). The barriers to sustainable risk transfer in the cyber-insurance market. J. Cybersecur., 10. https://doi.org/10.1093/cybsec/tyae003

Smyrli, D., Kakariaris, V., & Smyrlis, M. (2025). Cyber Insurance in Emerging European Markets: A Case Study of Greece and Cyprus. Proceedings of the 2025 IEEE International Conference on Cyber Security and Resilience, CSR 2025, 789–794. https://doi.org/10.1109/CSR64739.2025.11129995

Soquiat, M. M., Lumbera, M. L., & Abing, R. A. N. (2026). Fintech adoption as sustainable finance infrastructure : evidence from SMEs in Batangas province , Philippines. July, 1–6. https://doi.org/10.3389/fhumd.2026.1813050

Taskin, N., Özkeleş Yıldırım, A., Ercan, H. D., Wynn, M., & Metin, B. (2025). Cyber Insurance Adoption and Digitalisation in Small and Medium-Sized Enterprises. Information (Switzerland), 16(1). https://doi.org/10.3390/info16010066

Türen, S. H., Eustace, K., & Islam, R. (2026). Agile Resilience in Security for Small and Medium-Sized Businesses. 1–27.

Zhang, R., Zhu, Q., & Hayel, Y. (2017). A Bi-Level Game Approach to Attack-Aware Cyber Insurance of Computer Networks. IEEE Journal on Selected Areas in Communications, 35(3), 779–794. https://doi.org/10.1109/JSAC.2017.2672378