Cybersecurity, Cyber insurance, and Small-to-Medium-sized Enterprises: A Systematic Review

Rodney Adriko*, Jason R.C. Nurse

Institute of Cyber Security for Society (iCSS), School of Computing, University of Kent, Canterbury, UK

Abstract

Purpose: This study offers insights into the state-of-research covering cybersecurity, cyber insurance, and Small-to-Medium-sized Enterprises (SMEs). It examines benefits of insurance to an SME's security posture, challenges faced and potential solutions, and outstanding research questions.

Design/methodology/approach: Research objectives were formulated, and the Preferred Reporting Items for Systematic Reviews and Meta-Analyses Protocol (PRISMA) was used to perform a Systematic Literature Review (SLR). Nineteen (19) papers were identified from an initial set of 451.

Findings: Our research underscores the role of cybersecurity in the value proposition of cyber insurance for SMEs. The findings highlight the benefits that cyber insurance offers SMEs including protection against cyber threats, financial assistance, and access to cybersecurity expertise. However, challenges hinder SME's engagement with insurance, including difficulties in understanding cyber risk, lack of cybersecurity knowledge, and complex insurance policies. Researchers recommend solutions, such as risk assessment frameworks and government intervention, to increase cyber insurance uptake/value to SMEs.

Research limitations/implications: There is a need for further research in the risk assessment and cybersecurity practices of SMEs, the influence of government intervention, and the effectiveness of insurers in compensating for losses. Our findings also encourage innovation to address the unique needs of SMEs. These insights can guide future research and contribute to enhancing cyber insurance adoption.

Originality/value: This is the first SLR to comprehensively examine the intersection of cybersecurity and cyber insurance specifically in the context of SMEs.

Keywords: Cyber Insurance; Cybersecurity, SMEs, Information Security, Risk Management, Policies

Paper type: Literature Review

1 Introduction

On a global scale, SMEs constitute a large proportion of companies. According to the World Bank (2022), "formal SMEs contribute up to 40% of national income (GDP) in emerging economies" and represent roughly 90% of all businesses. Since there are varying definitions of SMEs, we adopt GOV.UK (2023) that defines SMEs as business with under 250 employees or with an annual turnover under €50 million or balance sheet total of under €43 million. Considering this prevalence, research has suggested that threats to the security and continuity of SMEs should be treated as a matter of national security (Williams and Manheke, 2012); because any successful attack may cripple them and consequently compromise the economy.

Recent research (Hiscox, 2023) has demonstrated that SMEs are continuously becoming targets of cyber criminals. One reason for this is that they can be used as conduits to reach larger organisations

* Corresponding author.
E-mail address: ra596@kent.ac.uk (R. Adriko)

that they support. This means that SME cybersecurity is not only a concern for SMEs, but all the stakeholders that engage with them. According to reports, however, SMEs are not taking security seriously and many business owners believe that they will not be targeted (Rahmonbek, 2023) and therefore fail to implement controls to reduce their cyber risk (Heidt et al., 2019).

In addressing the evolving landscape of cyber threats, cyber insurance emerges as a pivotal risk management strategy for SMEs. The security of SMEs can be incentivised by cyber insurance in two main ways. First, it encourages, or in some instances mandates, that applicants implement cybersecurity controls. Insurers may require companies to implement controls to obtain the policy or may provide lower premiums if certain controls are found. This can, in turn, increase the overall security posture of the insured (Romanosky et al., 2019; Franke, 2017; Mott et al., 2023). Secondly, cyber insurance might be the difference between survival and collapse in the event of a cyberattack (Agarwal, 2021) because it can provide SMEs with access to relevant missing expertise (Mott et al., 2023). Insurers also provide vital cash flow when a disaster strikes and cover immediate expenses in the aftermath of an attack.

While the overlap between cybersecurity and cyber insurance has been researched for many years, much of it has focused on larger organisations (Chidukwani et al., 2022; Ponsard et al., 2018; Osborn, 2015; Valli et al., 2021; Tsohou et al., 2023). Although some challenges relate to all sizes of organisations, there are SME-specific challenges worth in-depth analysis and thought (Tam et al., 2021). As noted by Heidt et al. (2019), there are often organisational-specific characteristics and constraints that affect SMEs differently, and therefore bundling small businesses in the same category as larger businesses inhibits their ability to learn from solutions proposed in research. From past literature, little research has focused on SME, cyber insurance, and security and as such, SMEs may fail to reap from its benefits to security due to these research gaps.

This research introduces a novel perspective within the cyber insurance literature, distinguishing itself from prior studies in this domain. Rather than concentrating solely on isolated elements, this study offers a comprehensive examination of cybersecurity, cyber insurance, and the specific context of SMEs. For instance, Alahmari and Duncan (2020) conducts a SLR to gain insights into the current landscape of cybersecurity risk management in SMEs, while Junior et al. (2023) investigates the cyber threats, adopted controls, challenges, and constraints encountered by SMEs in bolstering cybersecurity resilience. Similarly, Cremer et al. (2022) delves into cyber risk and security, particularly addressing the challenge of data availability. Additionally, Dambra et al. (2020) categorizes previous cyber insurance research into four distinct areas, focusing on the economic aspects, mathematical models, risk management methodologies, and predictions of cyber events within the realm of cyber insurance. These researchers have primarily focused on understanding cyber insurance and cybersecurity in a generalized context or individually. As such, there has been limited exploration into the interconnectedness of these topics and their implications for SMEs in enhancing cyber resilience. Consequently, SMEs may not fully leverage the benefits of cyber insurance due to these research gaps.

Our research seeks to bridge this critical gap in existing literature by examining the convergence of cybersecurity, cyber insurance, and SMEs. We assess the current state of research on cyber insurance for SMEs, identify knowledge gaps, and propose avenues for future investigation. Through an exploration of the advantages, obstacles, and potential remedies associated with cyber insurance adoption in SMEs, our goal is to provide insights for policymakers, industry stakeholders, and

academics to strengthen cybersecurity resilience within SMEs. It is essential to emphasize that our analysis is centred on the intersection of cybersecurity and cyber insurance specifically within the context of SMEs. This is also a critical novelty of our research.

The aim of this study, therefore, is to summarise the state of research as relates to how SMEs are engaging with cyber insurance with the goal of enhancing it, thereby improving their cybersecurity. We accomplish this through a systematic review of related literature and a precise assessment of the current state of the art in cyber insurance for SMEs. This review is scoped to these areas and examines any research literature – be it technical, IT and management aspects, or social – that is discovered from our systematic search. This research study has four research objectives (ROs):

1. Determine what research has been conducted on cyber insurance for SMEs, including the main topics covered. (RO1)
2. Explore the benefits of cyber insurance and the challenges faced by SMEs while engaging with cyber insurance that prohibits them from fully capitalising on it. (RO2)
3. Identify the approaches proposed to address the challenges faced by SMEs while engaging with cyber insurance. (RO3)
4. Define outstanding problems or unresolved questions in SME cyber insurance research. (RO4)

The remainder of this paper is organised as follows. Section 2 expounds on the PRISMA protocol while Section 3 shows the results of the selection process, along with a comprehensive examination of pertinent articles in relation to our research objectives. Section 4 provides an in-depth analysis of the articles, reflects on the identified issues, and outlines their practical implications. Finally, in Section 5, we provide a summary of our insights for research and practice.

2 Methodology

This systematic literature review (SLR) followed the PRISMA approach (Moher et al., 2009) given its ability to ensure a robust and thorough analysis. PRIMA's effectiveness and utility has been well established in cybersecurity research (Patterson et al., 2023; Naqvi et al., 2023).

2.1 Search Strategy

The study selection process involved searching a selection of electronic databases to identify articles and literature pertaining to cyber insurance in SMEs. The following search query was used:

("cyber insurance" OR "cyber liability insurance" OR "cyber risk insurance" OR "IT Risk insurance") AND (SMEs OR SMBs OR "small and medium-sized enterprises" OR "small to medium-sized enterprises" OR "small and medium-sized businesses")

Variations were made to the keywords of "cyber insurance" and "SMEs" to identify possible synonyms such as *cyber liability insurance* or *cyber risk insurance* for insurance and *SMBs* or *Small and medium-sized businesses* for SMEs. These variations allowed us to collect all relevant articles while avoiding the risk of being too narrow. Minor variations were also made to the search query to ensure conformity with the structure and format of the database searched, but the keywords remained

unchanged. For some databases like Scopus and IEEE, filters were applied to further refine the search to the subject area of Computer Science and Insurance. These searches were conducted in October 2023.

2.2 Eligibility Criteria

The following eligibility criteria were used:

1. Criterion 1 required that articles be peer-reviewed and published in English.
2. If Criterion 1 was met, Criterion 2 required that articles cover the topic of cyber security and cyber insurance, in the context of SMEs.

2.3 Information Sources

The article search was applied to eight key databases i.e., ACM Digital Library, IEEE Xplore, ScienceDirect, Web of Science, Scopus, Taylor and Francis, Springer Link, and JSTOR. Google Scholar was not included because of the limitations of its search functionality, such as a lack of Boolean operator support and inconsistent reproducibility (Gusenbauer and Haddaway, 2020).

2.4 Data Collection

Data was collected in accordance with PRISMA requirements and focused on information directly relevant to the research objectives. For instance, we extract information on research that has been conducted on cyber insurance for SMEs (RO1), the benefits of cyber insurance and challenges faced by SMEs (RO2), the approaches proposed to address these challenges (RO3), and outstanding research questions. (RO4). During this process, we do not presume that the papers selected exclusively address specific issues or areas of cyber security. Instead, we extract data items or information pertinent to our Research Objectives and research focus areas, which encompass cyber security, cyber insurance, and SMEs.

3 Results

3.1 Study Selection

The search yielded 451 papers that were screened in line with the eligibility criteria and a total of 27 duplicated records were removed. A full text review of the remaining 424 papers was conducted to determine their relevance, and those that met the criteria progressed to the next stage. A total of 405 articles were discarded, resulting in a final set of 19 papers being selected through the initial search. Any missing studies were checked by perusing reference lists of the selected articles. These were subjected to the same evaluation criteria, but this process did not yield any papers to be added to the set. This process is visualised in Figure 1.

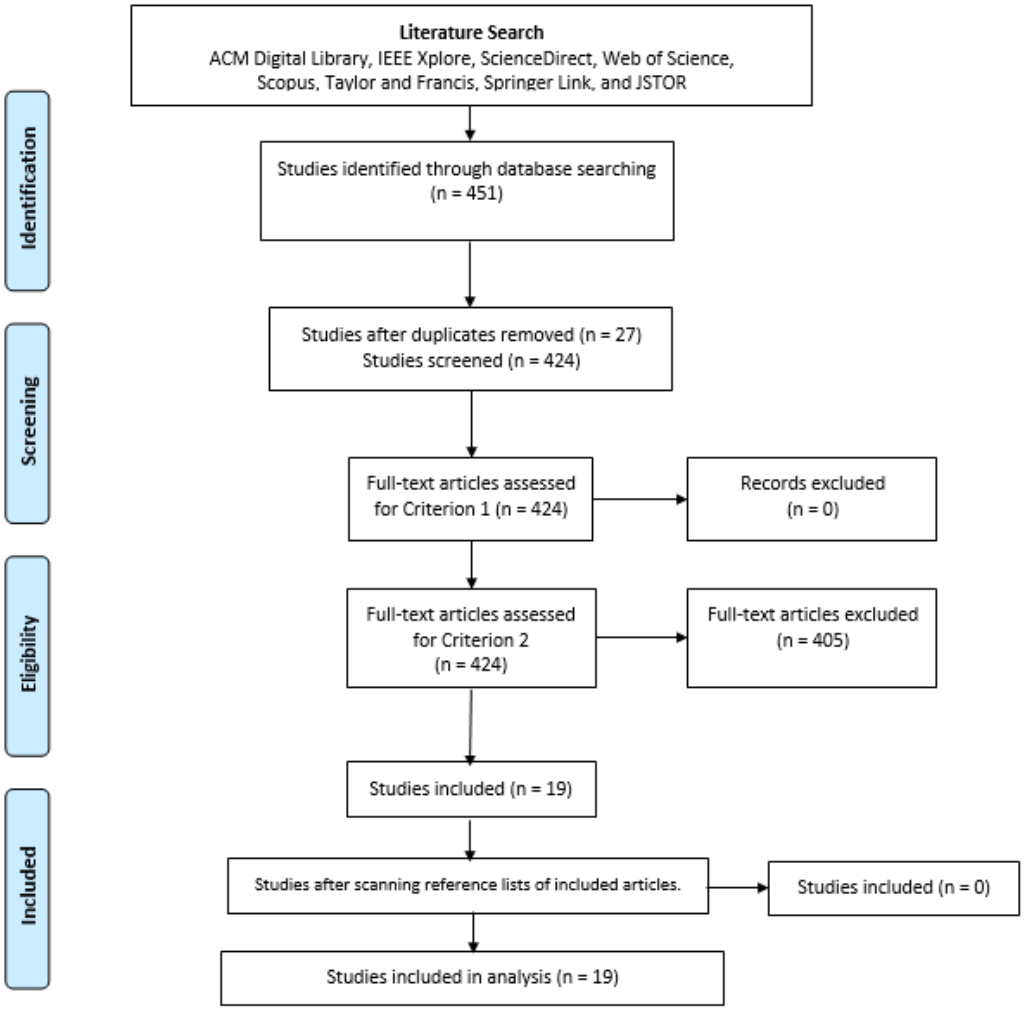

Figure 1: PRISMA flow diagram representing the inclusion process.
Source: Created by author

3.2 Publication Details

The complete list of articles is included in Table 1. For brevity, identification numbers such as P1, P2, etc., are utilized to refer to articles in subsequent sections. The majority (seven) of papers were authored during 2021, followed by 2023 with four papers. The year with the third highest concentration of articles was 2022 and 2018, where 2 of the 19 papers were published.

Paper ID	Study	Paper ID	Study
P1	Lemnitzer (2020)	P11	Valli et al. (2021)
P2	Branley-Bell et al. (2019)	P12	Pisoni (2020)
P3	Tam et al. (2021)	P13	Wang (2019)
P4	Gilbert (2017)	P14	Dacorogna and Kratz (2023)
P5	Armenia et al. (2019)	P15	Fernandez De Arroyabe & Fernandez De Arroyabe (2021)
P6	Cejkova and Nekas (2013)	P16	Eling et al. (2021)
P7	Hoppe et al. (2021)	P17	Bryce (2019)
P8	Cartwright et al. (2023)	P18	Mott et al. (2023)
P9	Kato and Charoenrat (2018)	P19	Skarczinski et al. (2023)
P10	Chiaradonna and Lanchier (2022)		

Table 1: List of research articles reviewed and respective paper IDs.
Source: Created by author

The years 2013, 2017, 2019, and 2020 each had one article. 16 of the included articles are journal articles while three are from conferences.

3.3 Benefits of cyber insurance to SMEs

As mentioned in P3, cyber insurance serves as a safeguard against cyber threats and significantly enhances the ability of SMEs to manage and recover from a breach (P1, P3, P18). This is attributed to the essential financial resources provided by insurance in the aftermath of a cyber-attack (P18, P4). Moreover, SMEs, often constrained by limited resources and time for risk management, can leverage the expertise and peace of mind that cyber insurance affords (P4). According to P18, cyber insurance policies are intricately designed to assist businesses from the moment a breach is discovered, which enables SMEs to tap into the knowledge and experience of insurers in addressing cybersecurity risks (P18).

Cyber insurance is advantageous for proactive risk mitigation as policies generate awareness that cyberattacks may occur (P8). For SMEs specifically, the act of purchasing insurance aids in comprehending their cybersecurity risk profile (P8) and encourages them to explore avenues for reducing risk (P8, P17). Some insurance providers decline to offer policies if policyholders do not possess sufficient cybersecurity measures (P17). By stipulating a reasonable-to-high level of security as a prerequisite for granting coverage, insurers motivate SMEs to prioritize cybersecurity (P17). This not only safeguards SMEs from attacks, but also facilitates their compliance with the security measures necessary to obtain insurance. From a risk and compliance standpoint, P18 asserts that cyber policies guarantee that businesses fulfil the obligations outlined in regulations such as the EU GDPR. This notion is further reinforced by P2 and P17, who affirm that cyber insurance can serve as a mechanism for enhancing cybersecurity through motivating SMEs to allocate more resources to it. As per P6, insured businesses demonstrate a heightened level of controls, suggesting that they could possess greater resilience against cyber threats.

In summary, the papers centre on the significance of cyber insurance for SMEs in order to safeguard against cyber risk and enhance their ability to manage and endure a breach (P1, P3, P18, P4). It not only offers financial assistance, but also encourages investment in controls (P8, P17), raises awareness about cyber threats, and contributes to the development of resilience within SMEs (P6). Through tailoring cyber insurance to SMEs with comprehensive coverage for specific threats (P13), premiums can be utilized to assist clients in gaining knowledge about risks and steering them towards risk mitigation services. Furthermore, cyber insurance can yield positive effects on a company's reputation and its relationships with clients (P15). Breaches associated with the misuse of systems can result in financial compensation to customers (P15), thereby causing damage to corporate reputation (P2, P5) and discouraging the establishment of new businesses. Cyber insurance can offer supplementary protection against security incidents, thereby aiding in the reduction of these risks, and safeguarding an SME's reputation.

3.4 Challenges faced by SMEs while engaging with cyber insurance

None of the papers explicitly examined the challenges associated with cyber insurance in SMEs but they covered this as part of their discussions. Seven papers (P2, P5, P6, P10, P13, P14, and P17) emphasized that SMEs struggle with risk evaluation and assessment. This process is a crucial starting point for assessing the position, potential, and value of cyber insurance, and subsequently obtaining it. Due to inadequate risk assessment, organisations may fail to align their business risks with insurance coverage, resulting in suboptimal benefits (P2). It is also observed in four papers (P1, P9, P14, and P18) that insurers are concerned about the systemic and aggregate risk that may arise from catastrophic events. As a result, they are hesitant to underwrite SMEs owing to their perceived inadequate risk management effort. Researchers have also highlighted difficulty in obtaining claim data and unavailability of historical data for creation of precise premiums, as seen in P1, P2, P3, P13, P17 and P19. P19 suggest that numerous organisations encounter security breaches, yet they fail to disclose to the relevant authorities which casts doubts on the completeness of available data.

Papers have also identified lack of expertise in SMEs to comprehend cyber insurance and cybersecurity. This observation is mentioned in P4, P7, P8, P11, P16, and P18, and is closely related to the deficient knowledge of insurance, as reflected in P2, P12, P13, P14, P17, and P18. It is quite intriguing that authors state that insurers themselves do not have a good grasp of cyber insurance. Over time, the insurance market has become more stringent (Mott et al., 2023), thereby making it challenging to obtain cyber insurance. This hindrance to adoption is highlighted by P18 which states that the hardening process has excluded many prospective insureds due to their inability to implement the required security controls. Pricing of policies remains a significant challenge to SMEs primarily because they cannot afford it. This is described in P8, P9, P13, P16, and P17 and corroborated by Brady (2023). According to Brady (2023), the Q1 2022 saw a 102% rise in the cost of premiums for SMEs, which was primarily attributed to the increasing incidence of ransomware attacks. Moreover, when coupled with budgetary and financial constraints, as mentioned in P16 and P8, it becomes increasingly challenging for SMEs to purchase cyber insurance. Inadequate budgets necessitate the prioritization of spending, but many SMEs still struggle with this (P5 and P14). According to Hiscox (2023), SMEs exhibited a lower level of certainty regarding whether their executive management prioritized cybersecurity.

P2, P3, P13, and P17, address the issue of inadequate transparency in policy coverage, which manifests as a lack of clarity regarding what is included and excluded. This dilemma is exacerbated by the obscure phrasing of policy language, which renders it difficult for SMEs to interpret policies (P2 and P3). Furthermore, the absence of proficiency in cybersecurity among SMEs, acknowledged in P4, P7, P8, P11, P16, and P18, significantly amplifies this challenge. This, in addition to the lack of insurance knowledge reflected in P2, P12, P13, P14, P17 and P18 makes it even more challenging for SMEs. The adaption of cyber insurance among SMEs faces another challenge mentioned in P2 and P3, wherein there are no baseline controls to be implemented to satisfactorily demonstrate their risk management effort and insurability. Consequently, insurers may conduct varying degrees of due diligence, leading to diverse conclusions on the same customer. This complicated assessment process (P1), creates hurdles for new insureds, hindering their ability to quickly acquire insurance. Most IT frameworks are designed to cater to the needs of large-scale customers, making them ill-suited for SMEs looking to contextualize cybersecurity within their operations as highlighted in P3. Different insurers may, therefore, offer varying policies to the same customer because of differences in their respective assessments. Several other challenges are addressed in the articles including Moral Hazard (P13, P17) where policyholders may become lax in their security due to assurance of compensation in the event of loss. Additionally, P7 identifies poor risk culture as a major challenge in this regard.

Finally, public perception of cyber insurance may have been tarnished by recent legal disputes between insurers and major policyholders, such as Mondelez (Evans, 2018) and the University of California (Rundle, 2023) (P1). This cast doubts for SMEs regarding their likelihood of success in making a claim, especially given that as they may not have the financial power – or time (P3) – to take on insurers in case of failure to payout. As a result, insurers have stated that clients are increasingly becoming wary about cyber insurance (Ahmed and Dyson, 2020).

3.5 Approaches and frameworks proposed to address challenges in SMEs' utility of cyber insurance

3.5.1 Frameworks and models proposed

P5, P10, P13, P16, and P19 have presented distinct frameworks for addressing the challenges. While P5 and P13 concentrated on frameworks to tackle cybersecurity investments, P10, P16 and P19 approached the pricing challenge through the prism of effective risk evaluation. P5 proposed a dynamic simulation approach to support the assessment of cyber risks and security investments using the SME Cyber Risk Assessment (SMECRA) tool. This tool facilitates comparison and evaluation of future outcomes of different investment choices allowing prioritization of cybersecurity-related investments. P13 presents a comparable analytical framework to optimize cybersecurity investment and the cyber insurance program which posits that SMEs are best served through an itemized, threat-specific coverage. A fraction of the premium is required to be allocated towards enhancing the clients' risk knowledge and encouraging the implementation of security controls.

P10 proposes a bidirectional percolation model that can effectively model cyber risk and provide precise expressions for the mean and variance of the aggregate loss. This, according to the authors, enables the derivation of an exact expression for insurance premiums, thereby addressing inaccurate premiums and poor pricing. P19 introduces the 'tempered' Generalised Extreme Value (GEV) method, that "models cyber losses based on a comprehensive, large-scale, computer-assisted telephone survey

to differentiate between various organisational characteristics" including size. This model predicts the maximum losses for both large and small organisations, facilitating the determination of extreme loss from a risk event and enabling the evaluation of the insurer's exposure. In P16, a proposal is made for a quantile regression aimed at addressing the pricing challenge and computing claims linked to data breaches. Its objective is to determine the most suitable insurance premium for any organisation. It emphasises that insurers must take into account the firm's size in loss quantification and, therefore, levy a reduced premium for smaller firms.

3.5.2 Other proposals

P1, P3, and P13 suggest making insurance mandatory for all companies regardless of size to ensure optimal value is obtained from cyber insurance. Conversely, P2, P7, and P9 suggest various ways in which governments can partner with the private sector to increase insurance penetration. While P2 does not explicitly require mandating cyber insurance, it suggests legislation in favour of it. P7 recommends that government agencies and company consultants should focus on increasing insurance market penetration. P9 advocates for exploration of opportunities by the government to incentivise SMEs to adopt Business Continuity Management (BCM) through the optimization of financial support mechanisms such as corporate tax deductions or exemptions. It suggests the provision of discounted premiums for SMEs equipped with a documented Business Continuity Plan (BCP) as a viable means of enhancing resilience. Corporate tax deductions proposed by P9 may incentivise insurance but may not be feasible due to its implications on the national income. For example, corporation tax is the fourth biggest revenue source for the UK Treasury (Adam and Miller, 2023).

A recurring theme in P3 and P18 pertains to the development of standards aimed at harmonising minimum controls expected by insurers. This is related to P3's proposal for the creation of a Security Framework, which would allow small businesses to contextualize cybersecurity within their operations. A related proposal is the need for transparency in coverage, highlighted in P2 and P3. Many SMEs find policies hard and may fail to understand them since they are general in nature and mainly focused on larger companies. P1 suggests the implementation of a minimum baseline for what a cyber policy should cover. This would ensure that an SME with the least cybersecurity knowledge would be covered to an extent necessary to cushion them from the effects of an attack. P2 further suggests that standardization of policy wording could potentially mitigate the confusion over coverage. Insurers remain apprehensive about catastrophic events and systemic risk because one catastrophic event could lead to the collapse of an SME. P13 suggest that insurers should practice risk sharing through insurance pools to ensure that catastrophic events do not jeopardize their stability. P14 proposes that insurers should create scenarios that take into account the potential impact of specific events to determine their ability to handle the consequences of such risks and make informed underwriting decisions. P12 emphasizes innovation in insurance through internal innovation, partnering with startups, or investing in companies to drive innovation.

According to P2, there is a persistent demand for further guidance in aspects of insurance, including the provision of a cyber risk mitigation tool for SMEs to enhance their comprehension of risk. This is consistent with the strategy of aligning business risk with insurance proposed in P4 and emphasizes the importance of skilled internal resources. However, data remains a significant challenge in estimating premiums for small and large entities alike. P2, P3 and P13 propose several approaches to facilitate data sharing between insureds and insurers with a view to establishing a repository of breaches and claims data that can be leveraged in assessing risk and estimating premiums.

4 Discussion

This section critically reflects on the review's findings and discusses key insights and avenues for future research. We especially focus on the challenges and propose research questions to address these. This section discusses key insights and presenting avenues for future research.

4.1 Benefits of cyber insurance to SMEs

Research findings from P1, P3, P4, and P18 highlight the fundamental role of cyber insurance in shielding policyholders from the effects of cyber-attacks. Insurers bridge the expertise gap for SMEs, aiding swift recovery from attacks (P4, P18). They also provide coverage and reimbursement for expenses incurred (P4, P18) such as hiring professionals to investigate system failures or breaches of privacy (Niyato et al., 2017). Given the prevalence of cyber-attacks, it is imperative to have appropriate insurance coverage to address budgetary constraints (P8, P16), and limited cybersecurity knowledge in P4, P7, P8, P11, P16, and P18.

P18 asserts that cyber policies guarantee that businesses fulfil the obligations outlined in regulations such as the GDPR. Marotta et al. (2017) contended that costs of informing individuals affected by privacy infringements and providing the necessary support are also covered by cyber insurance. This is a view that is shared with P5. In the realm of risk management, organisations specialized in risk management and compliance have formed alliances with insurers to measure risk (Agarwal, 2021) and ensure compliance. One example is the Security Governance as a Service (SeCaaS) (P17) where an attestation is provided on the compliance and security posture of the policyholder. SMEs can greatly benefit from such an initiative.

By having a robust cyber insurance policy, SMEs can significantly enhance their capacity to confront and respond effectively to cyber risks and incidents (P1, P18). To leverage on the benefits of insurance, SMEs must initiate a claims process but several policy characteristics such as coverage limits, deductibles, and exclusions can influence the likelihood of paying the claim. Despite facing challenges, cyber insurance could stand to be one of the most effective solutions for SMEs to achieve cyber resilience. Future research should therefore explore the impact of cyber insurance on SMEs to assess its actual and perceived utility and effectiveness through the following research question:

- How can the benefits of cyber insurance to SMEs, particularly as it relates to cybersecurity, be best communicated and realised, considering the caveats and nuances to these benefits?

4.2 Challenges faced by SMEs and their proposed solutions

In this subsection, we break the challenges faced by SMEs into three categories i.e., challenges attributed to SMEs, insurers, and challenges that require input from the government and public sector.

4.2.1 Challenge Area 1: Challenges attributed to SMEs

SMEs often have a poor understanding and deficient practices to adequately assess the risks they face (P2, P5, P6, P10, P13, P14, P17). This is the most mentioned challenge and has the potential to influence other challenges, such as poor decisions based on an inadequate risk assessment and non-alignment of cyber insurance to key organisational risks (P4). Many SME owners may not have fully appreciated the risks posed to their businesses by cyber threats (Rawindaran et al., 2023; Chapelle, 2023; P7, P13)

leading them to conclude that there is no need for cyber insurance (P17, P12) due to trust in their own internal capacity. According to Olano (2022), among SMEs (without cyber insurance) surveyed, 38% did not believe they would be a target for a cyber-criminal, while 27% said insurance was irrelevant to their business, and 18% said it was too expensive. Poor risk assessment may be possible because SMEs fail to effectively assess risk due to the difficulty in determining the impact of a loss (Strupczewski, 2021; P14, P17). On the insurer's side, it is difficult to assess the impact of a loss event, as this may vary among companies based on how large or small the company is, and the industry in which it operates (Marotta et al., 2017; Kurmaiev et al., 2020). It is therefore not surprising that many solutions attempt to address the challenge of risk assessment through innovation. There is significant room for collaboration with SMEs to educate them about their risks and to construct an insurance market tailored to their requirements. To address these issues research could explore:

- What factors contribute to the insufficient acknowledgment and understanding of cyber threats among SMEs, leading to a lack of appreciation for the risks posed to their businesses?
- What avenues and strategies can be implemented by cyber insurance firms to elevate SMEs' awareness and understanding of cybersecurity and risks within their specific business contexts, and what constraints or limitations are associated with these initiatives?

Another key challenge is the fact that SMEs have several budgetary constraints that prohibit them from implementing certain controls and, as such, they need to prioritize their investments and expenditures. This may lead to SMEs considering cyber insurance and cybersecurity controls as competing alternatives or one as a substitute for the other. Olano (2022) found that 11% of the SMEs surveyed felt that they did not need cyber insurance because they spent their money on security controls. It is clear from research (Rawindaran et al., 2023) that SMEs face challenges in justifying cybersecurity expenses and prioritization of initiatives (ENISA, 2021; P5, P14) due to several reasons including lack of knowledge (Lake, 2022) emphasised in P4, P7, P8, P11, P16, and P18. As such, it could be inferred that many prioritization decisions made by SMEs are ill informed and deny them the benefits of a robust resilience structure (Yang, 2023) that could be brought about by cyber insurance. P5 attempts to address this issue by utilizing the SMECRA tool which is a simulation method meant to support the evaluation of cyber risks and security investments. A related solution is proposed by P17 through the SeCaaS (Security governance as a Service) model which relies on a trusted third-party to manage the security governance service. This architecture raises concerns about the reliability and trustworthiness of the third party and their ability to keep the insured's data secure. The authors state that the SeCaaS approach does not require any special technical expertise but do not provide detailed information on how the processes are simplified for ease of use. SMECRA proposes a "system-dynamics-based methodology for assessing and evaluating an SME's cybersecurity risk profile and planning investments" for risk mitigation. These gaps leave several research questions to be explored in relation to the use of analytical models in cybersecurity investment appraisal including the following:

- What tools could be developed to empower SMEs in making informed cost-benefit decisions regarding cyber insurance, ensuring alignment with their broader cybersecurity initiatives?

Finally, the lack of knowledge and understanding of cyber insurance and cybersecurity remains a significant challenge among SMEs. These are the second and third most mentioned challenges. As noted in Page et al. (2017), and emphasised in P4 and P18, one of the primary benefits of insurance is that SMEs can benefit from the insurer's expertise in cybersecurity. However, to be able to reap these

benefits, SMEs need to have a good understanding of basic cybersecurity (Oh, 2022) and make informed investment decisions. According to Willard (2023), many brokers can have difficulty explaining cyber insurance to clients who do not have a good understanding of their cyber risk. It has been proven that the market is still in need of cybersecurity talent, yet this talent still lacks, as stated in P4, ISC2 (2022) and Coutinho et al., (2022). As such, solutions like changing of the wording of forms may not necessarily have an impact if insureds do not understand even the basics of cybersecurity. As seen across Page et al., (2017), Lew, (2023), and the articles reviewed (P2, P4, P7, P8, P12, P18), there is still a lack of cybersecurity and cyber insurance knowledge among SMEs. Public engagement and awareness campaigns can be essential in stimulating demand for insurance among SMEs by providing real life examples of the effects of cyber-attacks (Butcher, 2020). Future research in this area can consider:

- What approaches can be employed to persuade SME owners and directors about the critical importance of safeguarding their businesses against cyber-attacks?
- In what ways can insurers – potentially in partnership with cybersecurity firms – create powerful learning tools and awareness materials to educate SMEs on the importance of considering the integration of cyber insurance into their business strategies?

4.2.2 Challenge Area 2: Challenges attributed to insurers

Data access and availability, which is the fourth most mentioned challenge, remains significant, as many companies do not report incidents and breaches for reasons such as reputational damage and fear of exposure. Additionally, many of the available Operational Risk (op-risk) databases such as the Global Operational Loss Database (GOLD) (RiskBusiness, 2023) do not cover SMEs (P19), which may not be beneficial as insurance premiums based on little historical data or data collected from larger companies may not give a good estimation of premiums for SMEs leading to potentially expensive policies (P8, P9, P13, P16, and P17). In 2022, a survey conducted by the European Union (EU, 2022) revealed that 52% of attacked SMEs chose not to notify law enforcement authorities because they "dealt with the situation internally". Additionally, 44% of SMEs considered the incident to be too insignificant to warrant reporting (EU, 2022).

We are beginning to see government intervention in cyber risk management in the form of strict reporting requirements for incidents. The recently passed Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (CISA, 2023) requires that the Cybersecurity and Infrastructure Security Agency (CISA) develop and issue regulations requiring covered entities to report to CISA any covered cyber incidents and ransomware payments within 72 hours from the time the entity reasonably believes the incident occurred. The SEC Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (SEC, 2023) also requires registrants to disclose material cybersecurity incidents they experience, and their risk management practices on an annual basis. This may not directly affect SMEs but can indirectly influence those aspiring to enter public markets or seeking investment from institutions that prioritize transparency and adherence to regulatory standards. Data sharing among stakeholders can potentially unlock the full benefits of cyber insurance, but questions still remain about whether this data can be made available to other players in the market. It is paramount that insurers build meaningful relationships with regulators and industry associations to collect and share incident data and intelligence. This data can be very valuable in the risk assessment and underwriting processes. While data can be useful to estimate the loss and

subsequently the premium (P1, P13, and P19), some of the data that has been used in previous studies has been from unassured sources because the representativeness and completeness of these source databases cannot be assured (Armenia et al., 2021). Furthermore, insurers view data as Intellectual Property or competitive advantage that allows them to better price their policies compared to their competition (Nurse et al., 2020). As such, data sharing remains an outstanding challenge and an area open for research, particularly through:

- What specific barriers impede the availability of SME breach data for insurers, and how may government intervention, particularly through strict reporting requirements for cyber incidents, impact the availability of breach data and the overall cyber risk management for SMEs?
- How can collaborative synergies be established among insurers, cybersecurity firms, regulators, and government entities to facilitate the secure sharing of breach data, particularly on SMEs while ensuring the confidentiality of data and protecting the intellectual property?
- In what ways can operational risk databases be expanded to include a more comprehensive dataset from SMEs, and how would this expansion contribute to enhancing the accuracy of insurance premiums for SMEs?

Systemic risk is the sixth most prevalent challenge and is still a concern to insurers in their aim to underwrite SME risk. Although traditional insurance has demonstrated that a single risk event can affect several organisations, there has not yet been a demonstration of systemic risk events in the cybersecurity realm (Meredith-Miller, 2023). However, the fear of catastrophic risk events and the systemic risk by insurers (P1, P9, P14, and P18) is valid and can be argued to be justifiable based on the effects of non cyber systemic events like the COVID-19 pandemic (Rizwan et al., 2020), the 2008 Financial Crisis (McKibbin and Stoeckel, 2010), and the 9/11 attacks (Hartwig, 2002). In the aftermath of these attacks, over 18,000 SMEs were either shut down or destroyed and the insurance industry was hit with an estimated $40 billion claims (Hartwig, 2002). This worries insurers as a widespread ransomware attack or worm-like malware epidemic could affect several SMEs (Cowbell, 2023; Meredith-Miller, 2023; Pain, 2023). The rapid evolution of cyber threats poses a challenge for insurers in accurately assessing and quantifying extreme cyber risks, thereby restricting the extent of protection they can provide (Pain, 2023). Similar sentiments are shared by one insurer in P18 who states that "...political violence is pretty easy to cover because it doesn't happen that much...If you go cyber... SME, urgh, gets ugly, it's a lot of losses. And then for the big stuff, I don't think they'd be equipped". P13 recommends insurers to practice risk sharing through insurance pools while P14 proposes that insurers should create scenarios that take into account the potential impact of specific events in order to determine their ability to handle the consequences of such risks and make informed underwriting decisions.

Cyber insurance is a relatively new concept that has not yet matured to the level of traditional insurance (P8, P3). Over the past three years, this market has witnessed significant changes in its underwriting methodology, including more stringent control requirements (Mott et al., 2023). This hardening is promoting a level of maturity in the industry owing to more stringent restrictions (P18). However, it has also meant that some organisations including SMEs may not be able to afford cyber insurance (Brady, 2023; Curtis, 2022; P16, P17) due to a heightened level of control requirements. Future research can explore the following research questions.

- How can a maturing cyber insurance industry best work with SMEs that struggle to find insurance coverage?
- What are the specific consequences of systemic risk events within the realm of SME cyber insurance, and how do these events affect aspects such as cyber resilience and business continuity for SMEs?
- How can advanced modelling techniques be employed to assess and quantify systemic risk in SME cybersecurity, considering the intricate interconnectedness and dependencies among different entities?

Innovation in insurance remains relevant as emphasised in P12 and P13 to ensure that organisations, including SMEs can find it valuable. This innovation can come in various forms such as designing SME specific insurance (P13) or developing risk assessment methodologies that accurately compute premiums like in P16. P12 emphasizes the importance of innovation through internal innovation, partnering with startups, or investing in them to drive innovation.

Another related issue that stands out is that the vocabulary used in insurance policies and proposal forms is generally complex (P2 and P3). The risk assessment process for SMEs can be simplified by asking only a few questions to assess prospective policyholders. Some insurers have, however, oversimplified the forms by not asking any question at all, which can hinder the risk assessment process. Insurers are continuously making forms and policies easier to use by using simple language and providing definitions for key terms. Nonetheless, the standardization of policy wording and developing minimum insurance coverage still remains a challenge (MacColl et al., 2023). Some insurers are making the process simpler for repeat insurance customers by requesting for less detail at renewal of policies. The process for first time insureds, however, remains tedious. These queries open several avenues for future research including:

- In what specific ways can insurance products be custom designed to cater to the distinct cybersecurity needs and characteristics of SMEs, ensuring that the onboarding and coverage aligns with the requirements of these organisations?
- What are the challenges encountered in the standardization of insurance policy wording for SMEs, and how can these challenges be effectively addressed to promote consistency and clarity, ultimately fostering greater adoption of cyber insurance within SMEs?

4.2.3 Challenge Area 3: Challenges attributed to Government

P1, P3, and P13 suggest that insurance should be mandated for all companies. The practicality of this recommendation is debatable because there is no certainty that insurers will be able to take up this surge in demand. Although it can be positive, sometimes, legislation may not be the best way forward because organisations may only do it to become compliant. This is demonstrated in the Cyber Essentials Scheme Process Evaluation (GOV.UK, 2023), where the primary motivators for the adoption of Cyber Essentials among government contractors tended to be reactive in nature rather than proactive. Governments have attempted to develop cybersecurity standards specifically for SMEs that are simple and easy to adapt (P18), but these have only worked in the earlier years of release and subsequently dropped. This demonstrates that although standards have been adapted to SMEs, they have not had the desired impact. The Information Systems Audit and Control Association (ISACA) has developed a cyber

risk standard for smaller entities based on the COBIT Framework (ISACA, 2021) but the applicability and use of this standard is yet to be tested. Future research may address the following questions.:

- What role do regulatory frameworks play in addressing cyber risk in SME cyber insurance, and how can the development of guidelines and policies contribute to creating a resilient and sustainable cybersecurity posture for SMEs?
- What potential consequences might arise from legislating mandatory insurance for SMEs, and can insurers effectively manage the increased demand if insurance becomes compulsory?

In contrast to the SLR works of Alahmari and Duncan (2020), Junior et al. (2023), Cremer et al. (2022), and Dambra et al. (2020), which primarily focus on isolated components, this study delves into the interconnected nature of cybersecurity and cyber insurance within the unique context of SMEs. By adopting this approach, our research offers a fresh perspective within the cyber insurance literature, setting itself apart from previous studies. After reflecting on all these articles, there are several unresolved questions in SME cyber insurance research including the following: Firstly; Lack of awareness and understanding: Many SMEs are not fully aware of the importance and benefits of cyber insurance. There is a need to educate and raise awareness among SMEs about cyber risks and the value of cyber insurance for their businesses. However, aspects of the structure of SME training and awareness are not well covered in previous literature. Secondly, SMEs often face financial constraints, and the cost of insurance may be perceived as a barrier. Additionally, SMEs may have unique needs and vulnerabilities that are not adequately addressed by the existing policies. There is a need for more customized coverage options that cater to these specific requirements. Although previous research has demonstrated this in theory, there has not been a practical implementation or introduction of SME specific cyber insurance. Finally, SMEs often lack guidance on the best practices for cyber risk management and insurance. There is a need for benchmarking studies and the development of industry-wide best practices to help SMEs navigate the complex cyber insurance landscape. These outstanding problems and unresolved questions highlight the need for further research and innovation in the field of SME cyber insurance to better cater to the unique needs and challenges faced by SMEs.

4.3 Limitations

It is imperative to acknowledge certain limitations in our work. First, it primarily focuses on cyber insurance for SMEs only and therefore, the conclusions and suggestions should be viewed as for this organisational group. Secondly, the search for relevant articles was executed in October 2023, thereby implying that any research or publications after this date may not have been incorporated into this study. However, we have tried as much as possible to incorporate any more recent research while reflecting on our findings in the discussion section. Finally, the findings and conclusions of this study stem from the selected articles and literature that were scrutinized. It is crucial to acknowledge that the chosen articles were restricted to those addressing insurance within the context of SMEs. As a result, some articles discussing cyber insurance generally (e.g., Dambra et al., (2020); Abdul Hamid et al., (2022); Kesan et al., (2005), Ogut et al., (2005)) encompassing organizations of all or undefined sizes, were deliberately excluded from the study. Although all efforts were made to identify and incorporate a diverse range of sources, the exclusion of Google Scholar could have meant that some papers were missed. These limitations highlight the need for further research and development in SME cyber insurance.

5 Conclusion

In conclusion, this systematic review delves into SME cyber insurance research, exploring topics covered, benefits, challenges, and proposed solutions. It highlights cyber insurance's crucial role for SMEs, providing protection, financial aid, and expertise. However, SMEs face hurdles in understanding cyber risks, dealing with complex policies, and lacking insurance knowledge. Affordability and budget constraints further impede engagement. Researchers propose frameworks, risk models, and government intervention to enhance risk evaluation and transparency.

The review emphasizes the need for additional research in risk assessment, government impact, claims filing, and insurer effectiveness. Ongoing innovation is vital to address SMEs' unique needs. These insights guide future research, aiding effective strategies and policies to boost cyber insurance adoption, fortifying SMEs against evolving cyber risks. They bridge the gap between theory and practice, offering actionable recommendations for policymakers, industry stakeholders, and academia, and contribute to enhancing resilience of SMEs and protecting them from cyber threats. This, in turn, can have a positive impact on society by safeguarding economic activities and preserving trust in digital technologies in SMEs that form a significant portion of companies in several developed economies.

References

Abdul Hamid, N. H. A., Mat Nor, N. I.., Hussain, F. M., Raju, R., Naseer, H., and Ahmad, A. (2022). Barriers and enablers to adoption of cyber insurance in developing countries: An exploratory study of Malaysian organizations. Computers & Security, 122:102893

Adam, S. and Miller, H. (2023). Full expensing and the corporation tax base. https://ifs.org.uk/sites/default/files/2023-10/Full-expensing-and-the-corporation-tax-base.pdf. Accessed 2023-11-11.

Agarwal, P. (2021). Is cyber liability insurance an answer against growing cyber threats? https://www.cii.co.uk/media/10125637/coh_j012913-soup-cyber-liability-insurance-research-report-c3-1.pdf Accessed 2023-11-11.

Ahmed, M. S. and Dyson, B. (2020). Cyber insurers wrestle with war exclusions as state-sponsored attack fears grow. https://www.spglobal.com/marketintelligence/en/news-insights/latestnews-headlines/cyber-insurers-wrestle-with-war-exclusions-as-state-sponsored-attack-fears-grow56743302. Accessed 2023-11-06.

Alahmari, A. and Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pages 1–5.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., and Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, 147:113580.

ABA (2023). Brady, S. (2023). Increasing cyber security incidents transform cyber insurance. https://www. leasinglife.com/features/cyber-insurers-price-out-smes/. Accessed 2023-10-30.

Butcher, I. (2020). Cyber insurance for smes: The five questions that every insurance business needs to ask. https://www.intel.co.uk/content/dam/www/public/emea/uk/en/pdf/a1140852-cyber-insurance-for-smes-whitepaper.pdf. Accessed 2023-11-26.

Chapelle, A. (2023). Smaller Companies Must Embrace Risk Management. *Harvard Business Review*. https://hbr.org/2023/09/smaller-companies-must-embrace-risk-management Accessed 2023-10-10.

Chidukwani, A., Zander, S., and Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, 10:85701– 85719.

CISA (2023). Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet. https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf Accessed 2023-11-11.

CISOMAG (2021). Hardening Cyber Insurance Market Makes Cybersecurity More than a Tech Problem. https://cisomag.com/hardening-cyber-insurance-market-makes-ctbersecurity-more-than-a-tech-problem/. Accessed 2023-10-10.

Coutinho, S., Bollen, A., Weil, C., Sheerin, C., Silvera, D., Donaldson, S., and Rosborough, J. (2022). Cyber security skills in the UK labour market 2023. https://assets.publishing.service.gov.uk/media/64be95f0d4051a00145a91ec/Cyber_security_skills_in_the_UK_labour_market_2023.pdf Accessed 2023-11-11.

Cowbell (2023). Cowbell Defines Approach to Catastrophic Modeling for Cyberattacks on SMEs. https://cowbell.insure/news-events/pr/catastrophic-modeling-for-cyberattacks/. Accessed 2023-11-11.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., and Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3):698–736.

Curtis, H. (2022). Analysis: What's holding back the SME market from taking up cyber insurance? - Insurance Post. https://www.postonline.co.uk/commercial/7950111/ analysis-whats-holding-back-the-sme-market-from-taking-up-cyber-insurance. Accessed 2023-10-10.

Dambra, S., Bilge, L., and Balzarotti, D. (2020). SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap. In 2020 IEEE Symposium on Security and Privacy (SP), pages 1367–1383. ISSN: 2375-1207

Eling, M., Nuessle, D., and Staubli, J. (2021). The impact of artificial intelligence along the insurance value chain and on the insurability of risks. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47(2):205–241.

ENISA (2021). Cybersecurity for SMEs - Challenges and Recommendations. https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes. Accessed 2023-11-08.

EU (2022). SMEs and Cybercrime - May 2022 Eurobarometer survey. https://europa.eu/eurobarometer/surveys/detail/2280. Accessed 2023-10-30.

Evans, S. (2018). Mondelez's NotPetya cyber-attack claim disputed by Zurich: Report - Reinsurance News. https://www.reinsurancene.ws/mondelezs-notpetya-cyber-attack-claim-disputed-by-zurich-report/. Accessed 2023-11-06.

Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security*, 68:130–144.

GOV.UK (2022). Cyber Security Breaches Survey 2022. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022. Accessed 2023-10-30.

GOV.UK (2023). BEIS small and medium enterprises (SMEs) action plan: 2022 to 2025 (accessible webpage). https://www.gov.uk/government/ publications/beis-small-and-medium-enterprises-sme-action-plan-2022-to-2025/beis-small-and-medium-enterprises-smes-action-plan-2022-to-2025-accessible-webpage. Accessed 2023-10-30.

Gusenbauer, M. and Haddaway, N. R. (2020). Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google Scholar, PubMed, and 26 other resources. *Research Synthesis Methods*, 11(2):181–217.

Hartwig, R. P. (2002). September 11, 2001: The First Year. https://www.iii.org/sites/default/files/docs/pdf/sept11paper.pdf Accessed 2023-11-11.

Heidt, M., Gerlach, J. P., and Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, 21(6):1285–1305.

Hiscox (2023). Hiscox cyber readiness report 2023. https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf. Accessed 2023-11-26.

ISACA (2021). Small and Medium Enterprises Seeking to Start a Governance Program Get Tailored Road Map in New COBIT Resource. https://www.isaca.org/about-us/newsroom/pressreleases/2021/small-and-medium-enterprises-seeking-to-start-a-governance-program-in-newcobit-resource. Accessed 2023-10-31.

ISC2 (2022). Cybersecurity Workforce Study. https://www.isc2.org/research. Accessed 202309-08.

Junior, C. R., Becker, I., and Johnson, S. (2023). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. arXiv:2309.17186 [cs].

Kurmaiev, P., Morozova, L., Bondarenko, O., and Husarevych, N. (2020). Cyber insurance: the current situation and prospects of development. *Revista Amazonia Investiga*, 9:65–73.

Lemnitzer, J.M. (2020). Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy*, 6(2):118–136.

Lew, M. (2023). Lack of Cyber Education Leaves Businesses Exposed, with Inadequate Risk Prevention Efforts Making 3 in 4 SMEs a Target. https://www.sme-news.co.uk/lack-of-cyber-educationleaves-businesses-exposed-with-inadequate-risk-prevention-efforts-making-3-in-4-smes-a-target/. Accessed 2023-11-09.

MacColl, J., Nurse, J.R.C, and Sullivan, J. (2023). Cyber Insurance and the Cyber Security Challenge. RUSI Occasional Paper.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., and Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, 24:35–61.

McKibbin, W. J. and Stoeckel, A. (2010). The Global Financial Crisis: Causes and Consequences. *Asian Economic Papers*, 9(1):54–86.

Meredith-Miller, B. (2023). Whitepaper explores cyber risk modeling for SMEs. https://www.propertycasualty360.com/2023/01/17/whitepaper-explores-cyber-risk-modeling-for-smes/. Accessed 2023-11-09.

Moher, D., Liberati, A., Tetzlaff, J., and Altman, D.G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *BMJ*, 339:2535. Publisher: British Medical Journal Publishing Group Section: Research Methods & Reporting.

Mott, G., Turner, S., Nurse, J.R.C., MacColl, J., Sullivan, J., Cartwright, A., and Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. *Computers & Security*, 128:103162.

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., and Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132:103387.

Niyato, D., Hoang, D.T., Wang, P., and Han, Z. (2017). Cyber Insurance for Plug-In Electric Vehicle Charging in Vehicle-to-Grid Systems. *IEEE Network*, 31(2):38–46. Conference Name: IEEE Network.

Nurse, J.R.C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., and Creese, S. (2020). The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, pages 1–8.

Oh, H. (2022). Cyber insurance: what SMEs need to know. https://solcyber.com/ cyber-insurance-what-smes-need-to-know/. Accessed 2023-11-09.

Olano, G. (2022). One in three SMEs have no cyber cover despite rising cyberattacks. https://www.insurancebusinessmag.com/uk/news/cyber/one-in-three-smes-have-no-cyber-cover-despite-rising-cyberattacks-425334.aspx. Accessed 2023-10-10.

Osborn, E. (2015). Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs.

Page, J., Kaur, M., and Waters, E. (2017). Directors' liability survey: Cyber attacks and data loss — a growing concern. *Journal of Data Protection & Privacy*.

Pain, D. (2023). Cyber Risk Accumulation: Fully tackling the insurability challenge. https://www.genevaassociation.org/publication/cyber/cyber-risk-accumulation-fully-tackling-insurability-challenge. Accessed 2023-11-11.

Patterson, C.M., Nurse, J.R.C., and Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, 132:103309.

Ponsard, C., Grandclaudon, J., and Dallons, G. (2018). Towards a Cyber Security Label for SMEs: A European Perspective. pages 426–431.

Rahmonbek, K. (2023). 35 Alarming Small Business Cybersecurity Statistics for 2023 | StrongDM. https://www.strongdm.com/blog/small-business-cyber-security-statistics. Accessed 2023-11-06.

Rawindaran, N., Jayal, A., Prakash, E., and Hewage, C. (2023). 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.

RiskBusiness (2023). GOLD: Global Operational Loss Database by RiskBusiness. http://riskbusiness.com/gold/. Accessed 2023-11-21.

Rizwan, M.S., Ahmad, G., and Ashraf, D. (2020). Systemic risk: The impact of COVID-19. *Finance Research Letters*, 36:101682.

Romanosky, S., Ablon, L., Kuehn, A., and Jones, T.M. (2019). Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk? *Journal of Cybersecurity*, 5(1). Publisher: Oxford Academic.

Rundle, J. (2023). University of California Sues Lloyd's Syndicates Over Cyber Insurance. *Wall Street Journal*. https://www.wsj.com/articles/university-of-california-sues-lloyds-syndicates-over-cyber-insurance-da4675f5 Accessed 2023-10-09.

SEC (2023). SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/news/press-release/2023-139. Accessed 2023-11-16.

Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, 135:105143.

Tam, T., Rao, A., and Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security*, 109:102385.

Tsohou, A., Diamantopoulou, V., Gritzalis, S., and Lambrinoudakis, C. (2023). Cyber insurance: state of the art, trends, and future directions. *International Journal of Information Security*, 22(3):737–748.

Valli, C., Martinus, I., Stanley, J., and Kirby, M. (2021). CyberCheck.me: A Review of a Small to Medium Enterprise Cyber Security Awareness Program. In *Advances in Security, Networks, and Internet of Things*, pages 233–242. Springer, Cham.

Willard, J. (2023). Many SMEs are being left with a gap in coverage for cyber insurance: Cowbell's Cooksley - Reinsurance News. https://www.reinsurancene.ws/many-smes-are-being-left-with-agap-in-coverage-for-cyber-insurance-cowbells-cooksley/. Accessed 2023-11-09.

Williams, P. and Manheke, R. (2012). Small Business - A Cyber Resilience Vulnerability. *International Cyber Resilience conference*.

Woods, D., Agrafiotis, I., Nurse, J.R.C., and Creese, S. (2017). Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications*, 8(1):8.

World Bank (2022). World Bank SME Finance: Development news, research, data. https://www.worldbank.org/en/topic/smefinance. Accessed 2023-10-05.

Yang, Y. (2023). Investing in cybersecurity ensures long-term resilience | Marsh. https://www.marsh.com/content/marsh2/europe/uk/en_gb/services/multinational-client-service/insights/investment-cyber-security-training-resilience.html. Accessed 2023-11-08.