Computers & Security 163 (2026) 104818

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full Length Article

Cybersecurity and Cyber insurance for Small to Medium-sized Enterprises (SMEs): Perceptions, challenges and decision-making dynamics

Rodney Adriko [*], Jason R.C. Nurse

Institute of Cyber Security for Society (iCSS) and School of Computing, University of Kent, Canterbury, Kent CT2 7NF, UK

ARTICLE INFO

Keywords:
Cybersecurity
SMEs
SMBs
Information security
Cyber insurance
Risk management
Standards and controls
Decision-making
Psychology
Risk perception

ABSTRACT

Cyber insurance is increasingly positioned as a complementary tool for managing cyber risk, yet Small to Medium-Sized Enterprises (SMEs) remain underrepresented in its adoption. This study investigates the perceptions, decision-making dynamics, and support needs of SMEs regarding cyber insurance, drawing on 38 semi-structured interviews with SMEs, insurers, brokers, and other relevant stakeholders. The findings reveal that many SMEs deprioritise cyber insurance; not because they dismiss its importance outright, but due to a combination of limited awareness, concerns over cost, and a perception that its value is minimal unless required by clients or regulators. This hesitation is further shaped by several key barriers: complex policy language, a lack of trust in insurers, and unclear internal ownership of cybersecurity responsibilities. Despite these challenges, the study identifies promising strategies to boost adoption. These include simplifying policy structures, fostering trust through collaborative awareness efforts, introducing financial incentives tailored to SME budgets, and offering accessible, user-friendly tools that help businesses assess their cyber risks and insurance needs. By identifying actionable strategies and addressing both cultural and structural barriers, this study contributes to efforts to enhance cybersecurity resilience in the SME sector.

1. Introduction

Small-to-Medium-sized Enterprises (SMEs), defined as businesses with fewer than 250 employees and an annual turnover under £50 million (GOV.UK, 2023), play a critical role in the economy. However, the interconnectedness of today's digital landscape has increased the vulnerability of all organisations ((Verizon, 2024a) including SMEs) to a wide array of cyber threats. According to the Databarracks (2024), cyber incidents were the primary cause of IT downtime (24%) and data loss (46%) in 2024. The impacts of cyber-attacks can be severe, especially for SMEs (Acora, 2024; Munich Re, 2024) with limited resources (FSB, 2024; Rawindaran et al., 2023) and could potentially lead to business collapse (FSB, 2024; Howden, 2024a; IFAC, 2023; Huang et al., 2023). As threats become more sophisticated (Allan, 2023; WEF, 2024), the need for adequate cybersecurity controls cannot be overstated. Several controls can be adopted to deal with cyber risk and cyber insurance has emerged as a vital tool to cushion businesses from the impacts of attacks.

Cyber insurance is designed to mitigate the financial risks associated with cyber incidents by covering costs related to data breaches, business interruption, and legal liabilities, among others (Mott et al., 2023; Gilbert, 2017). As part of their service offering, many insurers provide security services to their policyholders including incident response and recovery, and regular scanning and security awareness (Mott et al., 2023; MacColl et al., 2021). The expertise and advice from insurers stand to be a key benefit for SMEs (Mott et al., 2023; Gilbert, 2017) especially due to their lack of cybersecurity expertise (Valli et al., 2021; Cartwright et al., 2023; Hoppe et al., 2021). This means that although cyber insurance is designed to reduce the impact of cyber incidents, the advice and awareness activities can also have a positive impact on the likelihood of a risk event materialising. Despite its potential benefits, many SMEs remain hesitant to invest in cyber insurance (Wilson and McDonald, 2024) as demonstrated by the low insurance penetration (GlobalDataFinancialServices, 2024; Rafferty, 2024). When SMEs are making decisions whether to purchase cyber insurance alongside investment in cybersecurity controls, it is often not straightforward (Wilson and McDonald, 2024; Osborn and Simpson, 2018) with some experts describing this process as a disaster (Curtis, 2024). This process can be influenced by several factors, including the SME's understanding of cybersecurity, risk perception, and the organisation's overall cybersecurity strategy (Wilson and McDonald, 2024; Rawindaran et al.,

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

https://doi.org/10.1016/j.cose.2025.104818
Received 6 July 2025; Received in revised form 28 November 2025; Accepted 26 December 2025
Available online 29 December 2025

2023).

As seen with large enterprises, the complexity and variety of available cyber insurance products can be overwhelming (Branley-Bell et al., 2022; Tam et al., 2021). This challenge is magnified for SMEs where limited resources (Eskins and McCabe, 2024) and cyber expertise can lead to confusion and uncertainty among decision makers (Wilson and McDonald, 2024) and in turn, affect their ability to make informed decisions. In the absence of a clear understanding of an SME's cyber risk profile and how insurance can complement the existing cyber risk management effort, difficulties may arise when SMEs attempt to align their insurance choices with their broader cybersecurity goals. Such confusion can result in two problematic outcomes: either SMEs forego cyber insurance altogether leaving themselves exposed to potentially devastating cyber incidents (Chidukwani et al., 2022), or they purchase policies that inadequately address their specific risks. However, it is essential to acknowledge that choosing not to purchase cyber insurance may also be a well-considered and rational decision. In practice, some SMEs may indeed opt out of cyber insurance as a deliberate, rational choice if they have strong security controls or deem the premiums unjustifiable. However, foregoing insurance without a thorough risk assessment can leave critical gaps, just as purchasing an ill-suited policy can waste resources. Due to this, the focus should shift from whether SMEs purchase cyber insurance to how they can make well-informed, data-driven decisions regarding cyber insurance that align with their broader cyber risk management initiative.

In this research, we seek to understand the decision-making dynamics of SMEs regarding cyber insurance and identify how they can be better supported to make more informed choices that align with their overall cyber risk management approach. Specifically, we aim to address the following Research Question (RQ):

- *How do SMEs make decisions regarding cyber insurance, and how can those decisions be better informed and aligned with their broader cybersecurity initiatives?*

For the purposes of this study, we consider "decision-making" to encompass the entire process by which an SME understands its cyber risk, evaluates cyber insurance alongside other countermeasures, and ultimately chooses whether and how to incorporate cyber insurance into its cybersecurity strategy.

To effectively address this RQ, we break down the research into three Research Objective (ROs).

- Firstly, we explore the perceptions and understanding of SMEs in relation to cybersecurity, with a particular focus on cyber insurance (RO1). We examine how SMEs perceive cyber risk and cyber insurance, and their level of understanding of the role that cyber insurance can play in their risk management efforts. Insights from this exploration help identify barriers that prevent SMEs from fully integrating cyber insurance into their cyber risk management strategy.
- Secondly, we investigate how SMEs make decisions regarding cyber insurance and cybersecurity (RO2). We accomplish this through an examination of their decision-making process and the roles and influences of different stakeholders. Understanding these dynamics is important for development of effective strategies to enhance decision making, ensuring that SMEs can effectively manage their cyber risk.
- Finally, we explore what solutions, strategies, and tools may be used to enable SMEs to make better informed decisions about cyber insurance (RO3). We posit that by providing SMEs with the knowledge and resources they need; they can make decisions that protect their businesses from cyber threats and support their long-term growth and sustainability.

To achieve these ROs and to facilitate a deeper understanding of the phenomenon under study (Paulus and Lester, 2022; Guthrie, 2024), we use a qualitative research methodology centred on conducting in-depth interviews with various stakeholders including SME representatives, insurers, insurance brokers, IT service providers, and researchers. While this approach does not offer statistical generalisability, it allows for an in-depth understanding of the nuanced, context-dependent barriers SMEs face, particularly in interpreting cyber risk, navigating complex insurance offerings, and engaging with service providers. This approach has been used in several academic papers like Mott et al. (2023) and Alshaikh (2020), among others. The transcripts are analysed using thematic analysis, which has proven effective in exploring individuals' experiences in previous studies such as Patterson et al. (2024) and Paulus and Lester (2022). It allows us to identify and categorise themes and concepts, thereby extracting meaning and insight from participants' responses (Kibiswa, 2019).

In the sections that follow, we review the literature on SME cyber risk and insurance (Section 2), explain our methodology (Section 3), present our findings (Section 4), and discuss implications for policy, industry, and research (Sections 5 and 6).

2. Literature review

The rapid evolution of the technology and digital landscape has led to an increased attack surface and threat profile of SMEs and exposed them to several cyber threats (Verizon, 2024a). Despite their critical role in the global economy (Rawindaran et al., 2023; FSB, 2024), contributing up to 40% of the national income of emerging countries (World Bank, 2022), SMEs often lack the resources and expertise to adequately protect themselves against cyber risks (Arroyabe et al., 2024; Hornetsecurity, 2024; Analysys Mason, 2022). This has led to increased interest in cyber insurance (Cowbell, 2020) as a risk management mechanism to cushion them from the impacts of such incidents (Affinity, 2024). However, the decision-making processes of SMEs concerning cyber insurance remain intricate and influenced by several factors, including their overall cybersecurity strategies (Wilson and McDonald, 2024; Rawindaran et al., 2023; Osborn and Simpson, 2018). Additionally, several challenges impede SMEs' engagement with insurance, such as difficulties in comprehending cyber risks (Aremnia et al., 2021), limited cybersecurity knowledge (Cartwright et al., 2023; Hoppe et al., 2021), and complex insurance policies (Branley-Bell et al., 2022; Tam et al., 2021) among others.

2.1. Cybersecurity challenges faced by SMEs

According to Bada et al. (2015) and Coker (2024), many SMEs are underprepared for cyber threats, often due to a lack of awareness (Maggiani, 2024; Wood, 2024; Cowbell, 2023) and understanding of the risks involved (Adriko and Nurse, 2024b; Hornetsecurity, 2024). Due to this, fewer resources are typically allocated to cybersecurity by SMEs compared to larger enterprises (Rawindaran et al., 2023; NEBRC, 2024), making them attractive targets for cybercriminals (Denning, 2022; Sharp, 2023). This view is corroborated by Hiscox (2024) and Verizon (2024a), that found that criminals were increasingly targeting small businesses with many reporting significant financial and operational disruptions. SMEs also continue to be targeted by opportunistic cyber criminals since many of them play a critical role in the supply chain of larger entities. According to Orange Cyberdefense's Cy-Xplorer report (Orange, 2024), SMEs suffered cyber extortion attacks 4.2 times more often than larger enterprises. This was attributed to the shift in threat actors' strategies from highly targeted attacks to opportunistic, less specific targeting (Orange, 2024) against the worst guarded victims (Howden, 2024b).

Munich Re (2024)'s Global Cyber Risk and Insurance Survey revealed that 87% of respondents questioned their organisations' readiness to handle cyber threats (up from 83% in 2022). SMEs struggle to respond to these attacks, and their cybersecurity landscape is further complicated by the absence of dedicated IT staff and heavy reliance on outsourced services, which creates a dependency on external service providers. According to the UK Cyber Security Breaches Survey, 2025 (GOV.UK, 2025), only 14% of small businesses assess the cybersecurity risks they are exposed to by their direct suppliers, and only 7% consider the risks within their broader supply chain. As such, many SMEs adopt a reactive rather than proactive approach to cybersecurity and risk management where controls are only applied after an incident has occurred (Renaud and Shepherd, 2018). This can lead to inadequate protection and increased vulnerability, highlighting the importance of implementing more structured and integrated cyber risk management strategies.

2.2. The role of cyber insurance in cyber risk management

Risk transfer through cyber insurance continues to position itself as a vital component of risk management for businesses of all sizes, offering protection against the consequences of cyber incidents (Mott et al., 2023; Gilbert, 2017). For SMEs, cyber insurance can be particularly valuable, as it could be the difference between survival and business collapse (Agarwal, 2021). Research has demonstrated that apart from covering direct costs, such as data recovery and legal fees (Biener et al., 2015; Marotta et al., 2017), cyber insurance also supports businesses in maintaining operations and keeping the business running during and after a cyber incident. According to CRAG (2024), investing in cyber insurance is a strategic choice that protects the organisation's data and systems while also securing the future of the organisation. A similar conclusion is reached by Anscombe (2024a) who posits that cyber insurance not only serves as a safety net, but also as a driving force for enhancing security practices and standards.

Despite these advantages, the adoption of cyber insurance remains limited (GlobalDataFinancialServices, 2024). According to ENISA (2023), 3 out of 4 Operators of Essential Services (OESs) do not buy cyber insurance. Relatedly, Franke et al. (2021) found that cyber insurance was never used to cover incidents in essential services. For SMEs specifically, the UK Cyber Security Breaches Survey 2025 (GOV.UK, 2025) revealed that <12% of SMEs had a specific cyber insurance policy while 45% had it as part of a wider insurance policy. This low adoption can be attributed to the perceived complexity of cyber insurance (Branley-Bell et al., 2022; Tam et al., 2021), a lack of awareness (Wang, 2019; Dacorogna and Kratz, 2023), and uncertainty about its benefits (Marotta et al., 2017). As a result, SMEs may struggle to determine if cyber insurance is suitable for their needs and will often view it as a "last resort" rather than an integral part of their cybersecurity strategy. Olan (2022) reveals that many SMEs perceive cyber insurance as a substitute for robust cybersecurity practices, rather than a complementary practice. This can often lead to a false sense of protection and increased exposure as businesses may want to over-rely on insurance without investing in cybersecurity controls. This can have a negative net effect as it can drive up premiums and hinder SMEs from obtaining cyber insurance (Mott et al., 2023). According to Delinea (2023), SMEs were more likely to be denied cyber insurance coverage compared to larger enterprises, with rejection rates of 28% versus 8% primarily due to the absence of adequate security protocols within the SME.

2.3. Decision-making processes in SMES regarding cyber insurance

While considering adoption of cybersecurity controls, many internal and external factors can influence the decision-making process of organisations including SMEs (Hasani et al., 2023). These can range from financial considerations, legal and regulatory considerations, risk considerations, and the level of cybersecurity awareness among decision makers, among others (Hornetsecurity, 2024; Rawindaran et al., 2023; Hasani et al., 2023; Osborn and Simpson, 2018). As stated in Anscombe (2024b), informed and knowledgeable leaders at the helm are essential for safeguarding the organisation and optimal cyber insurance coverage. According to Aremnia et al. (2021) and Chiaradonna and Lanchier (2022), SMEs often struggle with understanding the specific risks they face and how cyber insurance can mitigate them as they lack a formalised risk assessment process (Wang, 2019) which can lead to either over insuring or under insuring. Furthermore, due to several constraints, the expertise to evaluate the technical details of cyber insurance policies lacks among SMEs because they often involve technical jargon and complex terms that are difficult for non-experts to understand (Woods, 2018). This may result in decisions that may not be fully aligned with their actual risk exposure (Herath and Herath, 2021).

Established decision-making theories can provide more insight into why SME cyber insurance decisions can deviate from purely rational expectations. Classical economic models based on Expected Utility Theory (EUT) suggest that a risk-averse SME would weigh the expected costs of the insurance premiums against the expected benefits of coverage, theoretically choosing the combination of self-protection and insurance that maximises expected utility. However, in practice, low cyber insurance uptake indicates that other factors are at play and as such, standard EUT models cannot fully explain why many SMEs forgo insurance even when it appears economically beneficial (Joshi et al., 2025). Behavioural frameworks offer a potential explanation. Prospect Theory, for instance, posits that decision-makers overweight certain, immediate losses relative to uncertain future losses. Applied to this context, SMEs may place disproportionate emphasis on the immediate cost of insurance premiums and undervalue the abstract or unknown probability of a cyber incident (Joshi et al., 2025). Managers typically make decisions with limited information and simplified reasoning. As a result, their perceptions of risk differ from normative models; they tend to prioritise avoiding threats that could endanger the survival of their business rather than estimating the probability of all possible losses (March and Shapira, 1987).

Empirical studies support these behavioural tendencies; de Smidt and Botzen (2018) found that even professional risk managers tend to underestimate cyber risks and thus underappreciate insurance. This bias is likely to be even more pronounced in SME owners. Likewise, modelling by Oğüt et al. (2011) demonstrates that when cyber risks are correlated and losses are difficult to verify, firms may under-invest in both security measures and insurance relative to socially optimal levels. These theoretical perspectives underscore that SME decisions around cyber insurance are influenced not only by tangible factors (like cost and coverage specifics) but also by cognitive biases and heuristics. Understanding this interplay is crucial to designing interventions that address both the rational and behavioural drivers of SME decision-making.

While the above insights into SME decision drivers are valuable, they often stop short of linking decision dynamics to broader policy or ecosystem-level interventions. There is a need for studies that explore how SME decisions can be influenced not only by internal understanding but also by structural supports and coordinated external actors. In other words, beyond identifying why SMEs struggle with these decisions, research should examine what can be done at the ecosystem level (insurers, government, advisors) to facilitate better outcomes.

2.4. Aligning cyber insurance with broader cybersecurity strategies

Integrating cyber insurance with cybersecurity strategies is essential for ensuring comprehensive protection against cyber risks. According to Eling and Schnell (2016), cyber insurance should not be viewed in isolation but as part of the broader risk management framework. SMEs that successfully integrate cyber insurance with their cybersecurity strategies typically adopt an integrated approach to risk management that involves not only purchasing insurance but also investing in robust security controls (Mukhopadhyay et al., 2013). Insurance policies, such as those linked to achieving the Cyber Essentials (IASME, 2024) certification offer additional value by requiring applicants to implement controls before obtaining coverage. Many insurers make use of proposal forms to gain an initial understanding of the controls implemented by an applicant (Adriko and Nurse, 2024a). GOV.UK (2024b) highlighted that organisations with Cyber Essentials were 92% less likely to file a claim on their cyber insurance compared to those without. Furthermore, insurers like Coalition report that they have assisted policyholders in resolving 74,000 vulnerabilities, resulting in a 64% reduction in claims (Anscombe, 2024b). These successes highlight the importance of aligning cyber insurance with cybersecurity efforts to maximise the effectiveness of both. SMEs that integrate cybersecurity with insurance strategies are better equipped to manage the impact of cyber incidents and can recover quicker. However, this necessitates viewing cyber insurance as a complement to, rather than a substitute for, other cybersecurity measures (Olan, 2022).

2.5. *Gaps in the literature and research direction*

While existing literature has explored related themes, none fully accomplishes the specific Research Objectives (ROs) of this study, particularly in the context of SMEs. Much of the literature remains fragmented, often focusing narrowly on either cost, awareness, or regulatory issues in isolation. There is limited work that explores how multiple stakeholders interact to shape SME decision-making, particularly the role of brokers and service providers in translating policy options into action. Branley-Bell et al. (2022) and Tam et al. (2021) discuss challenges and trends in cybersecurity and insurance but lack focus on SMEs, overlooking their unique perceptions, decision-making processes, and the need for actionable solutions. Hoppe et al. (2021) address cyber insurance adoption from an SME perspective but focus primarily on financial risk management and fail to explore decision-making or provide practical tools. Similarly, Wilson and McDonald (2024) and Osborn and Simpson (2018) analyse cybersecurity and risk management using behavioural economics but do not tailor their insights to the specific needs of SMEs. Rawindaran et al. (2023), Hasani et al. (2023), and Mukhopadhyay et al. (2013) overlook SME-specific decision-making and strategies, while Eling and Schnell (2016) identify adoption factors but do not delve into decision-making or propose comprehensive solutions.

It is worth noting that a small number of empirical studies in the information systems and security domains have examined cyber insurance adoption via qualitative methods. For example, Branley-Bell et al. (2022) conducted in-depth interviews with stakeholders and found that high complexity and lack of standardisation in policies, along with limited awareness were significant barriers to cyber insurance uptake (Branley-Bell et al., 2022). However, their work did not specifically concentrate on SMEs. In another study, a stakeholder analysis by industry experts highlighted the need for more insight into the end-user (SME) perspective of cyber insurance, as consumers of cyber insurance were largely ‘out of scope’ in that research (Woods and Simpson, 2017). Osborn and Simpson (2018) provided evidence from a UK case study that SMEs often only engage with cybersecurity (including considerations of insurance) when external pressures such as client demands force their hand. These findings reinforce the importance of our SME-focused approach. Our study directly engages SME decision-makers (and those influencing them) to build upon these insights, moving beyond simply validating known barriers to proposing viable, context-sensitive solutions that align with SME capacities and needs.

Collectively, these gaps in prior studies underscores the need for research that addresses the unique challenges SMEs face in understanding, adopting, and utilising cyber insurance as part of their risk management strategies. This study addresses these gaps by focusing on how SMEs interpret cyber risks, navigate insurance decisions, and interact with various actors in their ecosystem. In doing so, it seeks not only to validate known concerns but to generate new insights into decision-making dynamics and the structural misalignments that persist between SME needs and insurer offerings. Ultimately, our research is driven by a critical void in the literature: understanding how to move from identifying barriers to proposing actionable solutions that can guide SMEs to make well-informed cyber insurance decisions aligned with their broader cybersecurity posture.

3. Methodology

In order to address the Research Objectives, we adopted a qualitative research design to understand the perception of SMEs on cyber insurance, explore the decision-making processes of SMEs concerning cyber insurance and its alignment with broader cybersecurity initiatives, and investigate ways to better equip SMEs to make informed cyber risk management decisions. This qualitative approach allowed for an in-depth investigation of the perceptions, motivations, and constraints across different stakeholders. Given the complex, context-dependent nature of cybersecurity decision-making, and the relatively limited empirical work on the lived experiences of SMEs in this domain, a qualitative methodology was deemed appropriate (Paulus and Lester, 2022; Guthrie, 2024). Although this approach does not provide statistical generalisability, it facilitates a rich, contextual understanding of the complex barriers SMEs face—particularly in interpreting cyber risks, navigating intricate insurance products, and interacting with service providers. This methodological approach has been adopted in prior studies such as Mott et al. (2023) and Alshaikh (2020), demonstrating its value in exploring cybersecurity related challenges.

This study adhered to strict ethical guidelines to protect the rights and confidentiality of participants. Ethical approval was obtained from the University of Kent's Ethics Review Board prior to the commencement of interviews. All participants were required to provide informed consent, and every effort was taken to ensure their anonymity through pseudonyms and the removal of any identifiable information from the interview transcripts. The findings of this study stem from the integration of insights from multiple participants with an aim of improving the overall perceptions and decision-making of SMEs, rather than providing an in-depth analysis of specific organisational processes and individual cases.

We defined four participant categories for this study, reflecting the multi-stakeholder environment of SME cyber insurance decisions:

i. SMEs: Owners, managers, or IT/security officers of small and medium businesses (both those who have cyber insurance and those who do not).
ii. Insurers/Brokers: Underwriters, brokers, or account managers serving SME clients.
iii. Third-party Service Providers: Managed Service Providers, consultants, vendors, or government bodies offering cybersecurity solutions and support to SMEs.
iv. Researchers/Academics: Experts with published work or policy experience in SME cybersecurity or cyber insurance

The participant groups were carefully selected to provide a well-rounded understanding of the factors influencing cyber insurance decisions among SMEs. A total of 38 participants were recruited, ensuring balanced representation from all the key stakeholders. Participants were recruited using purposive and snowball sampling methods. Initial SME participants were approached via local business networks, industry associations, and referrals, while insurer, broker, and service provider experts were identified through professional contacts in the cybersecurity and insurance communities. Academic interviewees were invited based on their known expertise and involvement in SME cybersecurity research initiatives. This recruitment strategy ensured a diverse and knowledgeable sample; all invitees received detailed study information and consented prior to participation. Of these, 14 were from different SMEs, representing a range of sectors, varying in size from micro-enterprises (1–10 employees) to mid-sized firms (~150 employees), and geographically spread across the UK, US and Australia. To further strengthen the study, we included insurers and brokers, who offer critical insights from the provider side; highlighting how cyber insurance products are designed, marketed, and tailored to SMEs, as well as their views on SME preparedness. Third-party service providers, such as cybersecurity consultancies, Managed Service Providers and government entities were also engaged due to their close operational relationships with SMEs. Their input added practical context on the real-world challenges and security postures SMEs typically exhibit. Additionally, academics with expertise in cyber insurance and SME risk management were included to contribute theoretical grounding and to offer an independent expert viewpoint on SME cyber risk challenges. This multi-stakeholder approach enabled the study to overcome SME recruitment challenges and capture a more complete picture of the decision-making ecosystem surrounding cyber insurance in the SME context.

Furthermore, the inclusion of both insured (6) and uninsured (7) SMEs brings balance to the study by capturing diverse perspectives of those with firsthand experience navigating or interacting with cyber insurance processes and those who have opted not to engage. This contrast allows for a more nuanced understanding of the motivations, perceived benefits, and barriers influencing SME decision-making on cyber insurance. The small SME sample size used in this study is consistent with similar research that employs qualitative techniques, where participants are selected based on their relevant experience. For example, Waelchli and Walter (2025) conducted semi-structured interviews with eight participants, chosen for their expertise in cybersecurity, to explore ways to reduce human susceptibility to social engineering. Similarly, van der Kleij et al. (2022) used a sample of ten participants from three organisations, whose experience provided valuable insights into management's decision-making when facing cyber threats. In another study, Ahmad et al. (2014) utilised eleven participants to investigate measures for preventing knowledge leakage, with the sample size deemed appropriate given the specialised knowledge of the participants. Other studies, such as those by van de Weijer et al. (2024), Branley-Bell et al. (2022), and Zanke et al. (2024), also support the use of small sample sizes when participants have the necessary expertise to inform the research topic. These precedents justify the choice of a small sample in this study, as it allows for in-depth exploration of the topic (Tables 1 and 2).

Data was collected from participants through semi-structured interviews conducted via video conferencing software lasting approximately 30 to 45 min. While the interviews were relatively brief, we ensured depth by using focused open-ended questions and probing follow-ups on critical topics. Pilot interviews were conducted with one SME, one insurer, one third-party service provider, and one academic researcher to refine the questions, ensuring that we could cover the breadth of issues within the time frame without compromising depth. These semi-structured interviews allowed us to explore the nuances of SMEs' awareness and understanding of cyber risks within their specific business contexts. Interview guides were tailored to participant category but aligned to the same three research objectives (RO1–RO3). Interview questions were open-ended to enable participants to describe their experiences in their own words. For example, SME participants were asked to describe their most recent insurance decision, whether it impacted their security posture, any perceived barriers, and who they consulted in the process. Service providers were asked how they support SMEs with cyber risk management and how insurance is positioned within that support. Participants were interviewed between May 2024 and May 2025 and audio-recorded with permission and transcribed verbatim. Pilot interviews were conducted to refine the questions, and an interview protocol was followed, to ensure that all key topics were addressed. For the interview protocols, see Appendix C–F.

Table 1
Interview participants by category.

Category	Number
SMEs	14
Third-Party Service Providers	10
Insurers	7
Academia/Researchers	7
Total	**38**

Table 2
Interview participants by industry.

Industry	Number
Insurance	7
Government	7
Academia	6
Cyber Security	6
Professional Services	5
Not for Profit	3
Financial Services	1
Wholesale and Retail Trade	1
Manufacturing	1
Construction	1
Total	**38**

The collected data was analysed using thematic analysis, a method well-suited for identifying, analysing, and reporting patterns (themes) within qualitative data. Thematic analysis was chosen to systematically identify common themes that show the participants' views, experiences, and decisions using the six-phase process described by Braun and Clarke (2006). The interview transcripts were analysed and read by the lead researcher to become familiar with the data, developing initial codes and themes using NVivo software with attention to data relevant to our research objectives. The transcripts were analysed with the codes and themes being reviewed and refined to ensure they accurately represented the data acquired from the participants. This involved checking the themes against the coded data extracts and the entire data set to ensure coherence. These refinements were informed by discussions within the research team and a comprehensive review of relevant literature. Major themes were developed and collectively agreed upon by the authors, ensuring they were deeply rooted in the data and offered valuable perspectives on the research objectives. This iterative approach, like that used in studies such as Patterson et al. (2024) and Paulus and Lester (2022), included checking the themes against coded data extracts and the entire data set for coherence. See Appendix B for the detailed codebook and themes.

Policy and practice recommendations in the Discussions section were developed using a synthesis-based interpretive framework (Yanow, 2000; Dunn, 2018). Rather than treating recommendations as neutral outputs, we interpreted them as situated in the lived realities of SMEs and shaped by the broader ecosystem of insurers, regulators, and intermediaries. Emerging themes were critically assessed against three criteria:

1. **Feasibility** – Can SMEs realistically act on this recommendation given their constraints?
2. **Scalability** – Can insurers or policymakers implement this widely across many SMEs?
3. **Alignment** – Does it align with existing regulatory or market efforts and incentives?

This allowed us to go beyond thematic description and move toward actionable, ecosystem-aware interventions.

4. Results

This section presents the detailed findings of this study based on the three Research Objectives (ROs): (1) exploring SMEs' understanding and perceptions about cyber insurance; (2) exploring the decision-making process; and (3) identifying strategies and tools to enable SMEs to make better decisions.

4.1. SMEs' understanding and perceptions about cyber insurance (RO1)

The analysis of interview data generated four key themes in understanding how SMEs perceive and understand cyber insurance and cybersecurity at large.

4.1.1. Perceived value and necessity of cyber insurance

Compared to immediate business needs such as hiring staff, expanding services, or meeting tax obligations, many SMEs perceive cybersecurity as a secondary concern and an unnecessary expense. This perspective stems from SMEs' limited budgets and competing operational demands, which force them to focus on visible, immediate concerns over cyber threats that they deem a less tangible risk. In many cases, cyber insurance is often deprioritised unless explicitly required by clients or contracts. One participant explained: *"As a small business, my main focus is on things I must have, like liability insurance, making payroll, and ensuring VAT returns are on time. Cyber just does not make the list unless it's forced"* (P24). This reflects behavioural patterns in Prospect Theory, where SMEs discount abstract cyber risks and prioritise immediate operational pressures, leading to underestimation of long-term exposure.

This deprioritisation is also driven by the perception that cybersecurity is a theoretical risk, with many SMEs lacking the direct experience or evidence to appreciate its value and urgency. Without a clear understanding of how cyber incidents could impact their business operations, SMEs often view cyber insurance as unnecessary with no immediate value. These perspectives highlight a gap in SME's awareness of the value of insurance as a safeguard for business continuity which contributes to their hesitancy to invest in measures like cyber insurance.

4.1.2. Risk perception and responsibility

The analysis reveals a cultural barrier within many SMEs, particularly those led by entrepreneurs who tend to adopt an optimistic, reactive approach rather than engaging in formal risk management practices. This mindset often leads them to defer proactive measures, assuming they can deal with the problems as they come. One participant noted: *"Many small business owners think, 'If something happens, I will deal with it then, rather than planning ahead"* (P25). Such attitudes may reflect a broader underestimation of risks, which limits the adoption of comprehensive cybersecurity strategies. Compounding this issue is a widespread belief among SMEs that their size makes them an unlikely target for cybercriminals. This misconception fosters a false sense of security, as stated by P13: *"Why would someone attack us? We're not big enough to matter"* (P13). However, this disregards the growing trend of cybercriminals targeting SMEs due to their perceived weaker defences and critical role in the supply chain, leaving them vulnerable to significant financial and operational damage. Furthermore, some SMEs tend to believe that their cybersecurity responsibilities have been offloaded to their third parties, such as IT service or cloud providers, reducing their perceived need to invest in security controls or cyber insurance. One participant noted: *"There's this feeling that if you're paying someone else to manage your IT, then the responsibility lies with them if something goes wrong"* (P20). This perception not only delays action but also overlooks critical gaps in coverage and accountability. This misunderstanding is exacerbated by assumptions by some SMEs that insurance policies of their service providers extend to their own operations. One participant shared: *"We thought our cloud service provider's insurance would protect us if there was a breach, but it turned out their policy only covers their infrastructure, not our data"* (P17). Such misinterpretations may suggest the need for clearer communication and education to help SMEs understand the limitations of third-party services and the importance of managing their own cyber risks.

4.1.3. Trust and efficacy of insurance brokers and underwriters

One of the most significant factors influencing trust in insurance providers is the perception that insurers may not honour claims, a concern amplified by media reports of high-profile claim denials. This scepticism fosters hesitation among SMEs, as reflected in the sentiment: *"There's this narrative that cyber insurance doesn't pay claims, and while it's not entirely true, it makes people hesitant to invest in it"* (P10). According to P28*, "You may think you're covered, but the real question is whether or not you can successfully collect on the policy. While I haven't dealt with cyber insurance claims yet, I anticipate that collecting on them could be challenging."* For some, this distrust leads to a questioning of cyber insurance's value, with participants expressing concerns like: "*There's probably always the assumption that you have to be very careful… to cross every 't', dot every 'i', because they may not help you in the event of a claim. I feel like that's a big worry at the board level."* (P19).

The role of insurance brokers is crucial in bridging the trust gap between SMEs and insurers as they can enhance confidence in cyber insurance as part of a broader risk management strategy. However, not all participants view insurance brokers as impartial advisors. Concerns about potential bias, as one participant noted, *"You have to wonder sometimes—are they really looking out for you or just pushing what they're told to sell?"* (P25), highlight the need for insurance brokers to prioritise transparent and client-focused communication. Insurers must focus on building credibility through clear claims processes and reliable service delivery while insurance brokers should emphasise impartiality and prioritise tailored advice to reassure SMEs of the tangible value and reliability of cyber insurance.

4.1.4. Barriers to adoption

Many SMEs lack awareness or a clear understanding of what cyber insurance covers and how it aligns with their broader risk management strategies. This knowledge gap often creates confusion and hesitation, with one participant noting, *"They don't really know what they're asking for… they let us guide them, but even then, they're not sure what it actually covers"* (P12). This uncertainty is further compounded by common misconceptions, such as the false assumption that existing General Liability or Business Insurance policies include adequate coverage for cyber incidents. Another misunderstanding among some SMEs is the belief that purchasing cyber insurance eliminates the need for other protective measures, such as security controls or employee training. This overreliance on insurance as a "silver bullet" solution was highlighted by one participant: *"A few think cyber insurance is a silver bullet—that it replaces the need for firewalls or training their staff. It's not"* (P25). Such misconceptions can undermine comprehensive cybersecurity strategies, leaving SMEs vulnerable to potential threats. Financial constraints further amplify the reluctance to decide on adopting cyber insurance. For many SMEs, the cost is perceived as a significant burden and non-essential expenditure, particularly for smaller businesses with limited budgets.

Addressing these barriers requires clear communication from insurers to dispel misconceptions about coverage and the role of cyber insurance in broader security strategies. Enhanced education efforts therefore appear crucial to ensure SMEs understand that cyber insurance complements, rather than replaces, other cybersecurity measures.

4.1.5. Role and influence of cyber insurance on cybersecurity behaviour among SMEs

This study reveals that cyber insurance can be a meaningful driver of improved cybersecurity behaviours among SMEs, though the degree of influence varies significantly depending on insurer practices, SME maturity, and awareness. Many SME participants reported that the process of applying for cyber insurance serves as a form of informal audit, prompting reflection on their existing security posture. As P32 explained: *"The cyber insurance process grills you as if you're getting certified for ISO or PCI DSS… it's first a self-assessment with a big questionnaire… the more you say 'no', the higher the insurance cost. So, you try to improve your controls year on year."* This introspection often leads to the implementation of baseline technical controls. P30 emphasised that insurers require clear evidence of such protections. This connection between risk assessment and premium pricing illustrates how insurance can indirectly drive cybersecurity enhancements.

Several participants acknowledged the practical support provided by insurers. Tools like risk assessment portals, checklists, and access to advisory services were valued as they helped SMEs self-evaluate and implement necessary controls. P19 noted: *"Insurers provide tools… portals that help you assess your risk… and access to professionals when you have specific issues."* The participants also praised the educational role of insurers. P18 highlighted the use of free phishing awareness training, while P36 remarked on the structured checklists that prompted internal audit; *"They have a list of 250 questions… it really gets these companies thinking, do I have this covered or not?"*. These tools and requirements serve as indirect yet effective reinforcements of security standards, even if not formally mandated.

The findings further suggest that many of the improvements prompted by cyber insurance mirror the requirements of Cyber Essentials, particularly in areas like access control (MFA, password hygiene), secure configuration (patching and software updates), and firewall/router management. For instance, P1 and P10 mentioned improvements in password management and MFA adoption; P12 and P33 noted insurers increasingly demanding up-to-date software and patch management.

> *"So, I would say, the two main ones that improve are Password management and using multi factor authentication… I would say are the biggest signs of improvement as a result of cyber insurance." (P1)*
>
> *"A lot of [insurance] come down to real basic things like… MFA on all remote endpoints…" (P10)*
>
> *"So yeah, if a business is… trying to get a quote [for cyber insurance], you say… do you patch or do you use Windows XP?… Well, you've gotta put those in place." (P12)*

However, not all impacts were viewed positively. Concerns emerged regarding overreliance on insurance as a substitute for proactive cybersecurity. P35 warned: *"Cyber insurance can… lead to a sort of not like negligence… but you don't pay attention as much… we're covered, so we don't need to worry about it so much."* Similarly, P17 critiqued insurers who offer policies with little to no requirements suggesting that insurance policies that do not ask them to do anything are just enabling them.

Despite these caveats, participants like P31 and P37 expressed optimism. P31 emphasised the value of collaboration between insurers and Managed Service Providers (MSPs), while P37 noted that even awareness of cyber insurance can spark more proactive cybersecurity considerations.

4.2. Decision-making dynamics regarding cyber insurance (RO2)

Under RO2, we examined how SMEs navigate the decision of whether to obtain cyber insurance, including who is involved, what information they rely on, and what triggers or checkpoints influence the decision. From the analysis, the decision-making process of SMEs regarding cyber insurance involves evaluating whether it aligns with their business needs and overall risk posture. Several themes emerged around the Influence of External Factors, Internal Business Considerations, Product and Service Specific Factors, and Risk Perception and Management.

4.2.1. Influence of external factors

Insurance brokers play a pivotal role in SME decision-making by acting as intermediaries who simplify policy complexities and provide tailored recommendations. As P28 noted, *"We rely on insurance brokers to tell us what we need because we don't have the time or expertise to figure it out ourselves"* (P28). For many SMEs, this guidance is invaluable, as insurance brokers break down complex policy details and demonstrate the relevance of cyber insurance to specific business risks. However, some SMEs voiced reservations about the objectivity of insurance brokers, raising doubts about whether the guidance offered genuinely reflects their best interests. Despite this scepticism, SMEs with long-standing relationships with insurance brokers through previous engagements tend to trust their recommendations. One participant shared, *"We've been with the same broker for years. If they say we need cyber insurance, I trust them. They know our business and wouldn't recommend something unnecessary"* (P17). IT service providers also play an influential role in guiding SMEs, often providing technical insights and advice on appropriate insurance options.

For many SMEs, the decision to purchase cyber insurance can be reactive, often in response to incidents within their business or industry. *"If you know a company similar to yours that's been breached and you see how awful it is, you might decide to buy cyber insurance. It's a strong motivator"* (P25). Similarly, firsthand experiences with cyber incidents often lead SMEs to adopt a more proactive stance including purchasing cyber insurance or enhancing internal controls, as one participant reflected: *"We had a minor breach a few years ago. It was enough to make us realise we needed to get serious about managing our risks"* (P19). External mandates also drive adoption, particularly when client requirements or supply chain contracts stipulate cyber insurance. In such cases, SMEs are often compelled to prioritise insurance, as noted by one participant: *"We had a major client that required us to have cyber insurance as part of the contract. Otherwise, we wouldn't have considered it"* (P26). It is evident that external client and industry pressures functioned as salient risk signals that recalibrated SMEs' subjective assessments of exposure, consistent with behavioural decision models. These findings underscore the importance of external influences in shaping SME decisions on cyber insurance, highlighting the need for trusted intermediaries and tangible risk awareness to drive initiative-taking risk management.

4.2.2. Internal business considerations

A recurring challenge in the decision-making process for SMEs regarding cyber insurance is the need to balance competing financial priorities. With limited budgets, SMEs often focus on revenue-generating activities or maintaining daily operations. This sentiment underscores the perception that cyber insurance is non-essential unless its benefits directly impact immediate business outcomes. Financial trade-offs frequently favour tangible investments like equipment upgrades over the perceived uncertainty of insurance. This mirrors Expected Utility Theory, where the certain cost of premiums becomes more salient than uncertain future benefits, prompting SMEs to avoid an immediate loss. One participant explained, *"When you're choosing between upgrading your equipment or paying for insurance that you might never need, the equipment wins every time"* (P20). These choices reflect the pressing nature of daily operational demands, which often overshadow potential cyber risks. Even when SMEs recognise the importance of cybersecurity, their ability to effectively address it is constrained by resource limitations. Without dedicated IT teams, cybersecurity responsibilities are frequently fragmented among existing staff or outsourced. This creates gaps in their expertise and preparedness to make cybersecurity decisions. Resource constraints mean that often, SMEs take a reactive approach where cybersecurity only comes into focus after an incident has occurred.

4.2.3. Risk perception and management

SMEs often underestimate their vulnerability to cyber threats, often perceiving such risks as primarily relevant to larger enterprises. This misconception leads many to deprioritise cybersecurity and cyber insurance investments. As one participant noted, *"SMEs think, 'We're too small to be a target,' so they don't take it seriously until something happens"* (P15). This reactive mindset leaves SMEs exposed to the devastating consequences that could have been mitigated. However, this perception of risk varies widely depending on the industry, the sensitivity of the data handled, and the extent of an SME's reliance on digital systems. SMEs operating in highly regulated industries or handling sensitive client information are more likely to recognise the importance of robust cybersecurity measures. One participant highlighted, *"We deal with sensitive client data, so the risk is very real for us. It's not just about avoiding fines—it's about maintaining client trust"* (P17). For such businesses, the stakes extend beyond compliance to the preservation of reputation and client relationships. Conversely, SMEs with less exposure to sensitive data or lower digital dependency tend to view cyber risks as less pressing, often leading to deprioritised investments in cybersecurity and insurance. This cost-benefit assessment underscores the need for tailored awareness campaigns that help SMEs better understand their specific risk profiles and the potential impacts of cyber incidents.

4.2.4. Product and service specific factors

For many SMEs, the complexity and perceived exclusivity of standalone cyber insurance policies present significant barriers to adoption. Insurance proposal forms often require detailed technical knowledge, which many SMEs lack, creating confusion and reluctance. This impedes their decision-making process. As one participant noted, *"The forms are too long and ask for technical details we don't understand. If they were simpler, we'd be more confident about completing them"* (P19). This lack of clarity often forces SMEs to rely on insurance brokers for guidance, with another participant explaining, *"The policies are so complicated… you basically have to trust your broker because it's impossible to understand on your own"* (P25). Beyond complexity, hidden exclusions and conditions within policy documents further undermine trust in cyber insurance products. Participants highlighted concerns about ambiguous language, as one remarked, *"It's hard to know what's actually covered and what's not because the exclusions are buried in technical terms"* (P22). Ambiguity and complexity increase perceived uncertainty, which Prospect Theory predicts suppresses uptake due to heightened cognitive load and aversion to unclear outcomes. These issues contribute to scepticism among SMEs, making them hesitant to adopt policies since they are difficult to evaluate and reach a decisive opinion.

Some participants suggested that bundling cyber insurance with existing insurance products, such as professional indemnity or public liability coverage, mitigates these challenges. By integrating cyber insurance into familiar frameworks, SMEs can bypass the need to navigate standalone policies. One participant shared, *"My insurer offered cyber insurance as part of my professional indemnity and public liability insurance. I didn't specifically look for it, but it was included, and that made it easier to say yes"* (P24).

In summary, the results indicate that many SMEs' decisions regarding cyber insurance and cybersecurity are heavily influenced by external factors beyond their control. This is primarily due to a limited understanding of these concepts, which hinders their ability to make informed decisions. Consequently, there is a pressing need to establish a framework that enables SMEs to make independent decisions, free from the external pressures of IT service providers, business partners, insurers, or insurance brokers who may have conflicting interests. The next section explores the proposed strategies and solutions to enable SMEs to take ownership of their decision-making process.

4.3. Strategies and solutions to support SMES in decision-making (RO3)

Through the analysis, several key strategies emerged, including education and awareness initiatives, simplified insurance products, financial incentives, practical tools, and collaborative efforts.

4.3.1. Education and awareness

Participants emphasised the critical need for training programs specifically tailored to SMEs to enhance their understanding of cyber risks. Such initiatives are not only instrumental in empowering SMEs but also serve as a pathway to better risk management and decision making. As one participant noted, *"We need proper training programs to help small businesses understand cyber risks. It's not just about selling insurance; it's about teaching them how to protect themselves first"* (P22). To address the awareness gaps, various training channels were proposed, including workshops, webinars, local SME forums, and industry-specific guides designed to simplify complex cybersecurity concepts and enhance decision making. These formats can provide SMEs with accessible and actionable knowledge. One participant highlighted that *"Most small businesses don't really know where to start with cybersecurity. If they had access to clear guidance and examples, it would make a huge difference"* (P18). It is evident from the analysis that insurers and brokers play a crucial role in educating SMEs about cyber insurance. Their ability to translate complex information about cyber insurance into clear and practical advice positions them as trusted sources of guidance. These findings underscore the importance of collaborative educational initiatives that engage multiple stakeholders.

4.3.2. Collaborations and partnerships

Participants emphasised the critical importance of coordinated efforts among insurers, government agencies, industry associations, and trusted intermediaries to address knowledge gaps, provide resources, and build trust in cyber insurance products. These partnerships are seen as essential for enhancing awareness, informed decision-making and encouraging adoption among SMEs. The credibility and reach of government-led efforts in promoting cybersecurity awareness and adoption was highlighted by the participants. Government agencies were recognised as important stakeholders in encouraging SME engagement with cyber insurance as one participant explained, *"If insurers and the government worked together to provide training or tax incentives, it would help SMEs take this more seriously"* (P22). Industry associations were also recognised as effective intermediaries for disseminating information and advice and promoting best practices. One participant noted, *"Our industry association regularly shares updates about risks and tools we can use. It's one of the few places where we get practical advice"* (P26).

Participants expressed an ardent desire for more proactive engagement from insurers. Regular communication, tailored advice, and support in identifying risks and coverage gaps were seen as ways insurers could shift from being transactional providers to trusted partners. As one participant stated, *"If insurers engaged with us more, helping us understand risks and offering advice on prevention, it would build a stronger relationship"* (P15). Insurance brokers and IT service providers were also recognised as key stakeholders due to their ability to provide personalised advice and explain complex concepts. The long-term relationships some SMEs had with their insurance brokers further enhanced this trust, as P12 explained, *"We trust our broker to tell us what we need. They've been with us for years, so their advice really carries weight"* (P17). The need for joint awareness campaigns involving multiple stakeholders, including insurers, government agencies, and industry leaders, was strongly emphasised. These campaigns could create consistent messaging about the importance of cyber insurance and its role in broader cyber risk management.

4.3.3. Technology and innovation

This theme highlights the critical role of modern tools, and innovative approaches in addressing SME cybersecurity. Participants noted the potential of automated risk calculators and self-assessment platforms to make risk assessment more accessible and actionable for smaller businesses. One participant noted, *"If there were tools that could show us what our risks are and how serious they could be, it would make decisions about cybersecurity much easier"* (P21). SMEs often operate with a limited understanding of how cyber risks could impact their business operations, which can result in either overconfidence or reluctance to invest in cyber insurance. Participants highlighted the value of tools that simplify the risk evaluation process, with one explaining, *"We don't really know how to evaluate our risks. If there was something to guide us through, it would make deciding on insurance easier"* (P17). This is a salient point for the security industry, including those that engage with cyber insurance.

Additionally, tools capable of calculating the financial impact of potential breaches were seen as critical for making risks more tangible and guiding informed decisions. As one participant stated, *"If there were tools that could calculate the financial impact of a breach, it would make risks feel more real and guide us toward the right protections"* (P18). These insights highlight the need for user-friendly, intuitive tools designed specifically for SMEs. Such innovations can help bridge knowledge gaps, demystify cyber risks, and encourage SMEs to adopt proactive cybersecurity measures, including the consideration of cyber insurance.

4.3.4. Policy and regulatory measures

Participants highlighted the importance of clear, government-backed standards to guide SMEs in implementing basic cybersecurity measures. Many SMEs lack the expertise to identify the necessary protections, and standardised requirements could provide a structured starting point. Participants also suggested that bundling cyber insurance with certifications such as Cyber Essentials could encourage adoption of cybersecurity and ease decision making. As one participant explained, *"If insurance was tied to achieving a certification, it would push us to invest in cybersecurity because we'd get something tangible in return"* (P22). This integration could allow insurers to reward SMEs for meeting these standards, enhancing risk management. Mandating cyber insurance in specific contexts such as critical supply chains, regulated industries, or government contracts was seen as another driver of adoption. Participants reported that external mandates were key motivators for considering cyber insurance. By aligning insurance with certifications and regulatory requirements, stakeholders can create a cohesive strategy that encourages broader adoption of both preventative measures and lead to effective decisions around cyber insurance.

4.3.5. Incentives and financial support

Cost remains a significant barrier for SMEs in adopting cyber insurance. Participants emphasised the need for financial incentives, such as tax credits or subsidies, to make these investments more accessible and alleviate affordability concerns. One participant explained, *"If there were tax breaks for having cyber insurance or meeting cybersecurity standards, it would be a big motivator"* (P22). Linking financial rewards to achieving security certifications was also highlighted as an effective strategy to encourage SMEs to adopt recognised cybersecurity frameworks. By tying discounts or incentives to certification, stakeholders can create a dual benefit of improved security and reduced costs. As one participant noted, *"If there were discounts or incentives for getting certified, it would push more businesses to invest in cybersecurity"* (P20). These suggestions underscore the importance of integrating financial support mechanisms into cybersecurity and insurance strategies to address cost-related hesitancy among SMEs.

4.3.6. Simplification and accessibility

The complex and technical language used in cyber insurance policies and proposal forms emerged as a significant barrier for SMEs. Many participants found it difficult to understand the details of coverage, exclusions, and claims processes, resulting in hesitation to adopt such policies. One participant highlighted this challenge, stating, *"The policies are so complicated… you basically have to trust your broker. Simplifying this would help a lot"* (P25). Participants strongly advocated for the use of plain, non-technical language in policy documentation to improve clarity, build trust and improve decision making. SMEs also highlighted the need for modular insurance options that allow them to select specific coverages based on their unique risks and budgets. As one participant explained, *"It would help if we could pick and choose what we need, rather than paying for things that don't apply to our business"* (P19). The value of simplified outlines and visual aids, such as infographics or comparison charts, was also emphasised. These tools can help SMEs quickly assess whether a policy aligns with their needs and make the decision-making process more straightforward.

Bundling cyber insurance with existing policies, such as general liability or professional indemnity insurance, was identified as another effective way to reduce complexity and enhance accessibility. This approach that integrates cyber insurance into familiar frameworks was found to increase the perceived value of insurance packages, as SMEs feel they are getting additional coverage at a lower cost. One participant described their experience, stating, *"It was bundled into my liability insurance, so I didn't even realise I had cyber coverage until my broker pointed it out. It made me feel more secure without having to spend extra"* (P26). Predictable pricing was another priority for SMEs, who stressed the importance of clear and transparent cost structures that can aid decision making. *"Knowing exactly what we're paying for and how much it will cost upfront would make decisions easier"* (P12), a participant noted. Additionally, participants highlighted the need for flexible and scalable solutions specifically designed for SMEs, rather than products adapted from larger organisations. These insights point to the importance of tailoring cyber insurance products to the unique needs of SMEs. Simplifying policies, providing modular options, integrating with existing products, and ensuring transparency in pricing are critical steps to aid decision making and enhance accessibility.

5. Discussion

The study highlights the challenges and opportunities SMEs face in integrating cyber insurance into their broader cyber risk management strategies. It underscores the perceptions, decision-making processes, and barriers SMEs encounter, offering strategies to support them. To synthesise these findings, we organised the determinants of SME cyber insurance decision-making into a conceptual table that presents the categories, influences, and examples from the data (Table 3).

By structuring the findings in this way, we move beyond a descriptive account of stakeholder quotes and provide a conceptual framework that can inform future empirical work and policy interventions.

5.1. SMEs' understanding and perceptions about cyber insurance (RO1)

This study reveals that many SMEs do not perceive cyber insurance as a critical business need, often prioritising immediate operational expenses over intangible protections. This aligns with Branley-Bell et al. (2022), who noted that the lack of a direct link between perceived threats and business continuity diminishes SMEs' urgency in adopting cyber risk management practices. From a decision-theoretic perspective, financial constraints create a reference point that amplifies loss aversion. SMEs overweight the certain, immediate cost of paying premiums relative to the uncertain and future-oriented benefits of coverage. Prospect Theory predicts this behaviour, illustrating why cyber insurance may be deprioritised even among SMEs who recognise their cyber exposure. The hesitancy to invest in cyber insurance unless mandated by external factors further illustrates the reactive nature of SME decision-making. SMEs often view cyber insurance as a "nice-to-have" rather than a necessity, especially if they have not directly experienced cyber incidents. This disconnect between perceived risk and actual vulnerability was also observed by Adriko and Nurse (2024b), who found that SMEs tend to deprioritise cybersecurity investments unless faced with an imminent threat. However, while these patterns are clear, it is important not to conflate them with evidence of incorrect risk perception. As Slovic (1987) argues, risk perception is inherently probabilistic and difficult to verify through qualitative data. What our findings suggest is not that SMEs are wrong about their risk, but rather that they often operate without formal models or data-informed assessments to guide their decisions. Their risk perceptions are therefore shaped more by intuition, anecdotal experience, and external triggers than by structured analysis. The broader context underscores the growing relevance of cyber insurance. With the rising number of SME attacks (Horowitz, 2024), the need for improved resilience is well established. Collins (2023) and Gohil (2023) argue that cyber insurance is no longer a luxury but an essential safeguard for SMEs.

The findings also reveal cultural barriers within SMEs where optimism and ad-hoc problem solving overshadow structured risk

Table 3
Determinants of SME cyber insurance decision-making.

Category	Determinants / Influences	Directional Influence	Aligned Research Objective (s)	Examples / Evidence from Study
Perceptions & Awareness	Risk perception (low vs. high); limited awareness of insurance coverage; trust in insurers	Mixed	RO1	SMEs viewing themselves as “too small to matter”; misconceptions about provider liability
Barriers	High-cost relative to SME budgets; complex policy language; lack of in-house expertise	Negative	RO1	Complaints about lengthy forms and exclusions; cost seen as competing with operational expenses
Decision-Making Dynamics	Internal: budget trade-offs, leadership attitudes External: client/ regulatory requirements, competitor breaches, broker advice	Mixed	RO2	SMEs prioritising payroll or equipment over cyber cover; adoption triggered by client mandates
Stakeholder Ecosystem	Influence of brokers, IT providers, insurers, and regulators	Mixed	RO2	Brokers simplifying terms but sometimes distrusted; IT providers shaping SME choices
Decision Outcomes	1. Adoption of cyber insurance 2. Rejection of cyber insurance 3. Partial/ minimal cover	Neutral (outcome types)	RO3	Bundled policies in liability insurance; some SMEs choosing not to purchase at all
Moderators	SME maturity, existing security posture, clarity of insurer requirements, structural supports	Positive	RO2, RO3	More mature SMEs qualifying more easily; mandates shaping insurance adoption
Strategies & Enablers	Education/ awareness programs; simplified policies; financial incentives; tools/self-assessments; collaborations	Positive	RO3	Requests for tax incentives; demand for user-friendly risk calculators; calls for joint campaigns

management practices. Many SMEs mistakenly believe that cyber threats are primarily targeted at larger enterprises (Verizon, 2024b; Olney, 2023), a misconception that Chidukwani et al. (2022) described as a “pervasive underestimation of SMEs’ vulnerability to cyberattacks”. However, even when SMEs acknowledge the potential costs of cyber incidents, their assessments tend to lack grounding in detailed exposure analysis. The Cyber Security Breaches Survey (GOV.UK, 2024a) highlights that many SMEs do not fully understand their level of cyber risk exposure, leading to either overconfidence in their defences or a diminished sense of urgency to adopt cyber insurance. Additionally, the perceived transfer of responsibility to outsourced IT providers diminishes the urgency for SMEs to independently address cybersecurity risks. This misplaced reliance creates a false sense of security, as noted by Wilson and McDonald (2024), who argue that such assumptions contribute to poor preparation and unclear accountability in the event of a breach.

Distrust in insurance providers also poses a challenge among SMEs. Media coverage of denied claims has increased scepticism about the efficacy and reliability of cyber insurance. This mistrust (Tam et al., 2021) undermines confidence in cyber insurance especially when high-profile claims are denied or underpaid. However, an argument against the notion that media coverage of denied claims is purely detrimental to the perception of cyber insurance could focus on the broader perspective of improving the industry's standards, transparency, and risk awareness. Rather than fostering scepticism, media coverage of denied cyber insurance claims can increase awareness and drive improvements. It highlights the importance of understanding policy exclusions, coverage limits, and the need for strong cybersecurity practices. It can also be a potential motivator for insurers to refine their offerings, and prompt organisations to enhance their cybersecurity measures to meet policy requirements. In fact, insurers do make payouts; Jones (2024) noted that over 52% of claims were paid without requiring out-of-pocket expenses from policyholders. Thus, the perception of widespread denial may be overstated, but perception, regardless of accuracy, still heavily influences SME behaviour. Insurance brokers positioned to bridge the trust gap, face challenges in gaining the confidence of SMEs. While some SMEs rely on brokers, others question their impartiality, fearing that advice may be driven more by sales targets than by a genuine understanding of the SME's risk mitigation needs. This dynamic reinforces the need for transparent, education-oriented engagement. When brokers succeed in demystifying complex terms and tailoring coverage, they can play a crucial role in building trust and fostering informed decision-making. However, a recent econometric study on cybersecurity investment and incidents indicates that the concern regarding small firms underinvesting in cybersecurity may not be justified (Dinkova et al., 2024).

A consistent theme across interviews is the lack of awareness about what cyber insurance covers, and how it integrates with existing cyber risk management efforts. SMEs frequently misunderstand insurance as a substitute rather than a complement to technical controls (Efeoghene, 2024) or assume incorrectly that General Liability Insurance includes cyber coverage (Mukhopadhyay et al., 2013). Cost perceptions further compound the issue. Even when interested in insurance, many SMEs consider it prohibitively expensive. Valli et al., (2021) identify cost as one of the most cited reasons for cybersecurity underinvestment in SMEs, suggesting a need for more affordable, flexible offerings. Collectively, these findings highlight that rather than a simple lack of interest, SMEs’ hesitancy often stems from a misalignment between perceived value, operational realities, and available guidance.

5.1.1. *Cyber insurance as a catalyst for SME cybersecurity*

The findings of this study suggest that cyber insurance can serve as a driver of improved cybersecurity practices in SMEs. This aligns with previous research, which indicates that the process of applying for cyber insurance often prompts firms to assess and improve their cybersecurity measures (Mott et al., 2023). This requirement can yield indirect benefits since the very act of applying for coverage could prompt investment in better cyber defences and tools, thus enhancing the security posture. Industry practice also supports these findings. Insurers commonly assess prospective clients’ safeguards such as enforcing Multi-Factor Authentication or regular backups and reward those with stronger controls through improved coverage terms or lower premiums (Romanosky et al., 2019; Mott et al., 2023; Franke, 2017). This creates a market incentive for SMEs to strengthen their cyber hygiene to qualify as a “good risk”. Insurers and industry bodies often emphasise that clients who obtain cyber insurance benefit from access to various security resources, from threat awareness training to incident response support, which can improve their overall cybersecurity readiness (Gilbert, 2017;

MacColl et al., 2021). The availability of cyber insurance has contributed to elevating cybersecurity as a priority for SMEs, pushing them to take security more seriously as corroborated by previous studies like Cartwright et al. (2023).

As stated by some participants, despite its potential, the influence of cyber insurance on SME security is not universally positive. A critical moderating factor is the insurer's own practices and requirements. This study found considerable variation in how different insurers structure their policies; some impose rigorous questionnaires and demand evidence of alignment with cybersecurity frameworks (e.g., ISO 27001), while others offer policies with less stringent checks. This variability is mirrored in research by Romanosky et al. (2019), and Adriko and Nurse (2024b), who highlight that the quality of cybersecurity risk assessments varies widely among insurers, which in turn affects the cybersecurity outcomes for SMEs. In cases where insurers' requirements are minimal, an SME can obtain coverage without substantially improving its security, which is problematic. Another key factor influencing the effectiveness of cyber insurance is the maturity and awareness level of the SME itself. SMEs that have already invested in cybersecurity measures are more likely to experience positive outcomes from purchasing cyber insurance than less mature firms. This aligns with findings by Brady (2023), who noted that SMEs with limited cybersecurity capabilities often struggle to meet the insurer requirements, and as such, may not experience the full benefits of insurance.

Further, the moral hazard problem highlighted in previous literature also emerged in our findings. Several SMEs reported that insurance coverage made them complacent about cybersecurity. This is consistent with the findings of Tam et al. (2021) and Bryce (2018), who argue that the presence of insurance can reduce the perceived need for proactive risk management, as organisations may assume that their insurance will cover any losses resulting from cyber incidents. Our study echoes this concern, where participants admitted that having insurance gave them a false sense of security, leading them to meet only the minimum requirements rather than engaging in continuous improvement.

Interestingly, the study also found that external business drivers, such as compliance with regulations or the need to meet client requirements, were more influential in shaping SME cybersecurity behaviours than the presence of insurance itself. This finding supports previous research by GOV.UK (2023) who observed that SMEs are often motivated to improve their cybersecurity by contractual obligations or regulatory requirements rather than by the threat of a cyber-attack or the availability of insurance. In particular, many SMEs in this study reported that they sought cyber insurance or improved their security measures primarily because they were required to do so by their clients or to comply with industry regulations. This indicates that external pressures, such as the need to demonstrate cybersecurity resilience to clients or regulators can be effective in driving meaningful behaviour change among SMEs.

5.2. Decision-making dynamics regarding cyber insurance (RO2)

This study reveals that the decision-making process of SMEs regarding cyber insurance is complex and influenced by a range of internal and external factors. One of the most consistently cited challenges was the fact that SMEs operate under significant financial constraints. Participants frequently emphasised that revenue-generating activities take precedence over perceived non-essential expenditures like cyber insurance. Valli et al. (2021) similarly highlighted cost as a primary inhibitor of cybersecurity investments, underscoring the urgent need for affordable and accessible solutions tailored to SMEs. However, this does not reflect a lack of concern. Instead, it reflects how SMEs balance competing risks with limited capacity. Interestingly, while many SMEs cite the high cost of cyber insurance as a barrier, comparative data suggests that insurance premiums are relatively modest when weighed against potential losses. Kapani (2024) reports average ransomware demands of £147,044, while annual premiums for SME cyber insurance average £3715. These figures indicate that many SMEs do have the capacity to invest in cyber risk mitigation but often lack clarity or confidence in its Return On Investment. This disconnect underscores the importance of risk perception, trust, and understanding in shaping spending decisions.

Additionally, the lack of dedicated IT teams within SMEs further fragments responsibility for cybersecurity with tasks distributed among staff who may lack the necessary expertise. This increases reliance on external advice as decision-making is often left to managers with limited technical knowledge. As predicted by Prospect Theory, under ambiguous conditions, individuals avoid committing to options with unclear outcomes. Participants noted a reliance on external advice from brokers and IT service providers to navigate the complexities of cyber insurance policies. As previous studies have shown (Adriko and Nurse, 2024b; Tam et al., 2021), SMEs depend on these actors to interpret technical jargon, explain exclusions, and tailor products to their context. However, several participants questioned the impartiality of brokers, suggesting that advice may be motivated by sales targets rather than objective assessment of need. Mukhopadhyay et al. (2013) and Hoppe et al. (2021) argue that simplifying policy language and offering modular options could help address this barrier. Our findings support this but also reveal a nuance; while some SMEs favour modularity, others prefer bundled options for their simplicity. This tension between modularity and bundling reflects diverse risk appetites and underscores the need for flexible product design that aligns with SME capabilities and preferences.

External factors such as client mandates, supply chain requirements, and sector-specific regulations often play a critical role in shaping SME decisions. These requirements act as external "risk signals" that realign SMEs' subjective risk assessments. Such salient cues can re-weight perceived exposure, shifting insurance from a discretionary cost to a necessary business safeguard. For instance, many SMEs only consider cyber insurance when required to secure contracts, a trend consistent with Osborn and Simpson (2018). These external mandates directly impact the types of business opportunities available to SMEs and carry tangible financial implications for their revenues. Similarly, regulatory requirements serve as an additional enforcement mechanism, compelling SMEs to align with specified cybersecurity standards. Participants confirmed that insurance is sometimes pursued only to secure contracts or meet procurement criteria but acknowledged that such mandates often prompt deeper reflection on cyber risk.

Risk perception also significantly affects SME decision-making. Many SMEs underestimate their susceptibility to cyber threats, operating under the assumption that smaller businesses are less attractive targets (Rawindaran et al., 2023). This leads to a deprioritisation of cyber insurance and cybersecurity investments. However, this perception can rapidly change especially when SMEs have seen breaches on their competitors or industry-wide incidents since they make the threat of cyberattacks more tangible. This behaviour reflects patterns identified in Chidukwani et al. (2022), where external examples often lead SMEs to reevaluate their vulnerability and preparedness and consider options to manage their cyber risk. Importantly, SMEs that handle sensitive data or operate in regulated environments expressed a greater perceived need for cyber insurance. This reinforces the idea that context matters in cyber risk decisions and as such, "one-size-fits-all" interventions are unlikely to succeed. Instead, support mechanisms must recognise this diversity and help SMEs align decisions with their unique operational realities.

5.3. Strategies and solutions to support SMEs in decision-making (RO3)

This study identifies a set of practical, stakeholder-informed strategies to address the challenges SMEs face in making informed decisions about cyber insurance. One of the most frequently mentioned gaps was the lack of foundational knowledge about cybersecurity and the role of insurance. Many SMEs viewed insurance as a non-essential cost, especially in the absence of a direct threat. Addressing this requires targeted awareness-building initiatives, such as brief training sessions, industry-specific guidance, and digital outreach campaigns. Valli et al. (2021) highlight that education is a key enabler of proactive security behaviours in SMEs. However, the training must be time-efficient, context-relevant, and accessible via formats that minimise disruption particularly for time-constrained, resource-limited firms. The complexity in insurance policies and proposal forms remains a significant barrier to adoption. Participants frequently expressed difficulty understanding policy details, exclusions, and technical requirements in proposal forms. To overcome this, insurers could simplify documentation, introduce visual aids, and offer modular policy structures. This aligns with Mukhopadhyay et al. (2013), who argue that accessible policy design can improve adoption. However, product design should be choice-driven, offering SMEs the ability to select either route based on preference and capacity.

The findings of this study underscore the need for joint awareness campaigns involving insurers, government agencies, and industry leaders. Recent initiatives, such as the NCSC's partnership with the Association of British Insurers (ABI) and British Insurance Brokers' Association (BIBA) (NCSC, 2024), emphasise consistent messaging and practical tools to support businesses, particularly SMEs, in managing cyber risk. Participants felt that such efforts lend credibility, address fragmented communication, and help standardise expectations. However, sustained collaboration is difficult. Stakeholders operate under divergent incentives as insurers prioritise risk transfer, governments focus on resilience, and SMEs are cost sensitive. Without clear coordination mechanisms, joint efforts risk inconsistency or dilution. We acknowledge this challenge and propose that any campaign must have clearly defined roles, funding commitments, and shared impact metrics to remain effective and SME-centric.

Digital tools such as risk calculators and cyber-readiness self-assessments were seen as potentially transformative but only if usability and affordability are prioritised. Participants appreciated tools that converted abstract risks into tangible numbers, helping them visualise potential losses. Cartwright et al. (2023) shows that such tools can support informed decisions but also note that many SMEs find them difficult to use without guidance. To bridge this gap, simplified "lite" versions with visual outputs and limited input fields can be developed. Additionally, bundling such tools with broker consultations or insurer onboarding can support uptake. However, unless cost and complexity are addressed, such innovations risk low adoption particularly among micro and early-stage enterprises. Financial incentives also emerged as another recurring theme with participants advocating for tax credits, policy discounts, and subsidies for SMEs that meet cybersecurity thresholds or obtain certifications like Cyber Essentials. These incentives align with findings from Wilson and McDonald (2024), who emphasise the role of financial signals in shaping behaviour. However, their impact is constrained by awareness, access, and administrative effort. Smaller firms may be unaware of available incentives or unable to navigate claim processes. Additionally, reliance on state funding introduces uncertainty, as programs may be short-lived or unevenly distributed across regions. Thus, while incentives hold promise, they must be paired with clear guidance, automated eligibility checks, and durable funding streams.

Standardised guidelines and regulatory frameworks can also provide SMEs with a clear roadmap for cybersecurity and insurance adoption. Some participants supported mandatory cyber insurance within certain supply chains or government tenders. Others advocated for integrating insurance into existing frameworks such as Cyber Essentials. For example, insurers could offer coverage bundled with compliance to Cyber Essentials or similar frameworks, as seen in studies like Eling and Schnell (2016), which highlight the effectiveness of linking insurance with preventive measures. Standardised guidelines and regulatory frameworks, however, have limitations including the financial and administrative burdens of compliance. Additionally, mandatory requirements risk becoming only a "box-ticking exercises," where achieving certification takes precedence over meaningful cybersecurity improvements. This concern is supported by Arntzen (2022), who found that ISO/IEC 27001 certification was negatively associated with the cybersecurity performance of power grid operators in Norway, suggesting that certification alone may offer a false sense of security if not accompanied by ongoing engagement and context-sensitive implementation. Success of this initiative requires sufficient support, awareness, and enforcement, without which SMEs may struggle to meet the standards.

5.4. *Alignment with decision-making theories and prior research*

A striking observation from our study is how closely SME behaviour aligns with patterns predicted by behavioural economics and decision-making theories. By incorporating Expected Utility Theory and Prospect Theory into the interpretation of these findings, the study reveals that SME cyber insurance decisions are shaped not only by financial considerations but by behavioural dynamics related to perceived risk, loss aversion, policy ambiguity, and external cues. Many SMEs exhibited decision patterns that Prospect Theory would predict i.e. they demonstrated strong loss aversion to the certain cost of insurance premiums while underweighting the potential losses from cyber incidents. This is evidenced by quotes like "It feels like paying for something that might never happen" (P28) – a mindset consistent with prospect theory's value function. Our findings echo Joshi et al. (2025), who contrasted resource allocations under expected utility vs. prospect theory.. SMEs in practice leaned toward the prospect-theoretic behaviour, investing less in insurance and more in immediate needs. While expected utility models might suggest more SMEs should buy insurance given the growing risk, the reality is that cognitive biases and heuristics significantly shape SME risk responses. Our study also resonates with March and Shapira's (1987) observation that managers' perceptions of risk differ from academic risk models. SME owners often framed cyber risks in terms of survival and thresholds rather than probabilistic trade-offs. For many SMEs, a cyber incident is not cognitively evaluated until it seems like a probable disaster. Thus, insurance, which deals in hypotheticals and probabilities, does not naturally fit their decision frame unless external forces like a recent incident or a client mandate kicks in.

Another area of alignment is with empirical studies that have explored related questions. For example, Branley-Bell et al. (2022) found that policy complexity and lack of standardisation were significant barriers to cyber insurance uptake. Our findings not only corroborate this but also extend it by showing the consequence; SMEs, when confused or distrustful, default to inaction. Our work thus underscores the practical impact of the issues Branley-Bell et al. (2022) identified. Similarly, Woods and Simpson (2017)'s stakeholder analysis called for more insight into SME perceptions which our study directly answers, providing a ground-level view of SME attitudes and perceptions. In line with Osborn and Simpson (2018), who observed that external pressures often drive SME cybersecurity decisions, we found client requirements and industry expectations to be crucial triggers for action. This consistency suggests that certain findings about SME behaviour (e.g., reactive posture, influence of external forces) are robust across contexts and studies, giving us confidence in targeting these areas for intervention.

At the same time, our study offers novel insights and tensions that contribute to the literature. One such contribution is highlighting the discrepancy between SMEs' acknowledgment of cyber risk and their translation of that acknowledgment into decision action. Many SME interviewees agreed that cyber threats are real, yet they compartmentalised this knowledge away from decision-making ("…but it's not a priority right now"). This gap between awareness and action is a nuance not deeply explored in earlier works that primarily focus on awareness levels. We show that raising awareness alone may not suffice and that it must be coupled with compelling decision triggers or facilitators. In theoretical terms, this reflects a knowing-doing gap since cognitive awareness does not automatically result in behaviour change, especially under constraints and competing priorities.

5.5. Practical implications

This research offers actionable insights for multiple stakeholders aiming to improve SME engagement with cyber insurance and their overall cybersecurity resilience. By addressing the challenges and barriers identified, the study informs targeted interventions that can drive meaningful change in SMEs' perception of cyber insurance and their decision-making process.

Firstly, insurers and brokers should take note that addressing SMEs' concerns about trust and complexity is not just customer-friendly but also essential for market growth. The traditional insurance approach of lengthy policies and cautious wording is backfiring in the SME segment by eroding confidence. Our recommendation is for insurers to experiment with radical simplification for this market including short policy summaries, clear examples of claim scenarios, and perhaps even pre-approvals of claims in common scenarios (to demonstrate reliability). Some insurers have also begun providing claims pledge statements which could help alleviate scepticism like that voiced by P28 ("will they pay out when needed?"). Additionally, integrating brokers more tightly into the education process can pay dividends. Brokers are already the de facto risk advisors for many SMEs – formalising training for brokers on how to communicate cyber risk (perhaps borrowing techniques from financial advisors who explain complex instruments in simple terms) could improve broker-SME dialogues. Our data showed that SMEs respond well when brokers make the effort to contextualise and personalise the risk (e.g., P28's story of the broker breaking it down). In fact, these narratives hint at the potential of storytelling as an educational tool; brokers and insurers might collect and share anonymised "claims stories" of SMEs, which are far more relatable to an SME owner than abstract statistics (Branley-Bell et al., 2022). By doing so, they tap into a more emotional and concrete understanding that enhances decision making.

For IT service providers and cybersecurity consultants, our findings highlight an opportunity to expand their role as bridges between SMEs and insurers. These providers often have the trust of SMEs in technical matters meaning that if they endorse cyber insurance or insurers, they can influence SMEs who might tune out an insurance salesperson. Some MSPs in our study were already doing this in an ad-hoc way but there is room to systematise it. For example, MSPs could include a "cyber risk review" in their quarterly reports to clients, including a section on residual risks that insurance could cover. This approach positions insurance as part of the holistic solution the MSP is delivering, rather than a separate, unrelated product. It also aligns with findings by de Smidt and Botzen (2018) that improving communication and awareness can enhance insurance decision-making. Our data showed that ecosystem collaboration such as insurers providing tools via MSPs is mutually beneficial. SMEs get better advice, insurers get better-informed clients (likely leading to fewer disputes and better risk profiles), and MSPs can differentiate their service.

Policymakers and industry bodies should take note of the clear evidence that SMEs as a group are underprepared and that market mechanisms alone are not swiftly correcting this given the persistently low uptake rates. Our results support the arguments of Woods and Simpson (2017) and others that some policy intervention might be warranted. For instance, government endorsed cyber insurance frameworks or accreditation could address trust issues. If an SME sees that a policy meets a government or Chamber of Commerce standard, they may feel more secure in its legitimacy. Additionally, subsidies or tax incentives for cybersecurity spending (including insurance premiums) could nudge behaviour, as several participants suggested. While our study alone cannot perform a cost-benefit analysis of such incentives, it aligns with economic arguments that externalities from cyber incidents (e.g., affecting customers, partners, and the economy) justify some public investment in promoting resilience. A positive externality of higher cyber insurance adoption is that insurers, through their underwriting, can enforce better security practices (since they require them for coverage) – a point consistent with the notion of advantageous selection mentioned in recent research (Branley-Bell et al., 2022; Adriko and Nurse, 2024b). Thus, encouraging insurance uptake indirectly improves overall security postures among SMEs, which has public good aspects by reducing overall cybercrime impact.

Our work also draws attention to an area often overlooked i.e. the emotional and psychological dimension of SME decision-making. Many interventions we discuss (education, incentives, simplification) will only succeed if they resonate with SME owners' psyche. For example, framing matters since telling an SME "You are at high risk of X" might cause denial or fatalism, whereas showing them "many businesses like yours have bounced back from attacks thanks to insurance" can instil a sense of agency and optimism. The language of empowerment needs to be carefully calibrated. Essentially, SMEs should be treated as capable agents who, with the right information and tools, can make prudent decisions for their business. Our findings demonstrate that SMEs are neither ignorant nor irrational but rather, they are optimising within their perceived constraints and knowledge. Thus, any solution must expand their perceived opportunity space (e.g., by lowering cost or complexity) or shift their perceptions (e.g., by making the threat more immediate or the solution more trusted).

5.6. Limitations and future research

While this study provides valuable insights into SME perceptions and decision-making on cyber insurance, several limitations must be acknowledged. The qualitative methodology applied in this study is based on a small sample of semi-structured interviews. This may restrict the generalisability of the findings across different industries, regions, and regulatory contexts. Furthermore, reliance on self-reported data may introduce biases such as selective recall or exaggeration which may potentially affect the accuracy of insights. However, qualitative research remains invaluable for capturing nuanced perspectives, exploring complex decision-making processes, and generating rich, in-depth insights that may not emerge through quantitative methods alone. Future research could benefit from complementing qualitative approaches with quantitative methods, incorporating larger sample sizes, and strengthening these findings with objective data such as case studies or industry reports to enhance reliability. Additionally, while we included a range of stakeholders, the perspectives of SME employees (non-decision-makers) and customers of SMEs were outside our scope; their views could add another layer to understanding the ecosystem effects of SME cyber decisions.

The study exclusively and intentionally focuses on SMEs which limits its applicability to larger enterprises, which may face distinct challenges and decision-making dynamics. Additionally, due to the rapidly evolving cyber threat landscape or insurance market, the time-bound nature of data collection (May 2024 – May 2025) means that the findings may not fully reflect the current cyber landscape and insurance market. While our study acknowledges the rapidly evolving nature of the cyber threat landscape and the cyber insurance market, recent developments and studies related to SMEs suggest that our findings remain pertinent. For example, El-Hajji and Mirza (2024), a study published in October 2024 highlights that SMEs face increasing cybersecurity challenges as they handle more sensitive data, making them attractive targets for cyberattacks. This research emphasises the need for effective risk assessment frameworks for SMEs, which aligns with our findings (El-Hajji and Mirza, 2024). Additionally, a June 2024 report also noted the global decrease in cyber insurance premiums as businesses improve their security measures, reflecting the adaptability of the market in response to the evolving cyber threat environment (Techdirect, 2024). These developments suggest that the challenges and dynamics identified in our research continue to be relevant, reinforcing the validity of our work in the current market context. Another area for future inquiry is quantitatively testing the effectiveness of the recommended interventions for example, piloting a simplified policy or a decision support framework in a controlled study to measure impact on adoption and outcomes. Longitudinal studies following SMEs through the decision process would also be valuable to validate and enrich our findings.

The sampling approach, which combined purposive and snowball techniques, may have introduced bias, potentially overrepresenting informed participants while underrepresenting less-engaged SMEs. Geographic constraints further limit the generalisability of the findings, as cultural, economic, and regulatory variations across regions could significantly influence SME cybersecurity practices and attitudes toward insurance. Future studies should adopt broader international sampling strategies to capture diverse perspectives and regional differences. Finally, this research primarily explores perceptions and decision-making processes, leaving measurable outcomes, such as the actual impact of cyber insurance on SME resilience and recovery, relatively unexplored. Future research should investigate these outcomes to provide a more comprehensive understanding of cyber insurance effectiveness. Examining how insurance contributes to mitigating financial and operational risks post-incident would offer valuable insights for both SMEs and policymakers.

Finally, another limitation of this study is the small number of SME participants, due to the well-known challenges in accessing this group such as limited time, awareness, and competing priorities. To address this, we included insurers, brokers, third-party providers, and academics who regularly engage with SMEs and offered informed, practice-based perspectives. While this may limit the depth of SME-specific insights, the broader stakeholder input ensured a more comprehensive view of the SME cyber insurance landscape, supporting the study's aim to understand the wider decision-making ecosystem. Additionally, we observed thematic saturation across interviews with recurring patterns in challenges, decision criteria, and stakeholder influence suggesting that the sample was sufficient to support the research aims (Guest et al., 2006).

6. Conclusion

This research examined the perceptions, challenges, and decision-making dynamics of SMEs with respect to cyber insurance and explored strategies to improve their engagement with cyber risk management. Through 38 interviews spanning SME owners/managers, insurers, brokers, service providers, and academics, we gained a holistic view of the landscape. Our findings reaffirm that SMEs face substantial barriers including limited awareness, financial constraints, complexity of insurance products, and a trust deficit; which contribute to low cyber insurance uptake. However, looking beyond these hurdles, we delved into why they persist, uncovering that SME decision-making is heavily influenced by behavioural factors such as optimistic risk perception and cognitive overload from complexity. These insights help explain the discrepancy between the high level of cyber risk exposure and the low adoption of insurance in the SME sector.

Importantly, our study moves past a purely diagnostic contribution and into a prescriptive one. By integrating perspectives from all stakeholders, we identified tangible measures to address the current shortcomings. Strengthening the theoretical foundation with concepts like Expected Utility Theory and Prospect Theory allowed us to pinpoint where SMEs diverge from “rational” decision models. We advocate for a multi-faceted approach; educating SMEs in relatable ways to make cyber risks and insurance value more concrete, simplifying insurance offerings and purchasing processes to reduce friction, aligning incentives (through discounts or modular coverage) to SMEs' financial realities, and leveraging partnerships and technology (brokers, MSPs, automated tools) to embed cyber risk management into SMEs' routine decision-making. Underlying all these is the need to treat SME stakeholders as collaborative partners in risk management, not simply as disempowered end-users. Instead, we focus on neutrality and agency, recognising SMEs' capacity to make prudent decisions when given appropriate support and information.

This study contributes to the academic discourse by filling a gap at the intersection of cybersecurity, risk management, and small business management. It corroborates and extends prior empirical work, bringing new depth to our understanding of SME behaviour. Practically, the insights serve insurers, brokers, and policymakers in refining their strategies to increase cyber resilience among SMEs. For insurers and brokers, the message is clear: simplification, transparency, and value-added engagement are not just customer-friendly but necessary to unlock a hesitant market. For policymakers and industry bodies, there is justification to facilitate knowledge-sharing, perhaps through public-private initiatives, and to consider incentives or frameworks that encourage better risk management practices and decision making.

In closing, the imperative for bolstering SME cyber resilience cannot be understated. Cyber threats will continue to grow in sophistication, and SMEs, with their constrained resources, will remain in the cross-hairs. Cyber insurance, as part of a broader risk management strategy, holds promise to cushion the blow of attacks and even incentivise better security practices. However, realising that promise requires closing the gap between perception and action, between availability and adoption. Our research shines a light on that gap and offers a roadmap for bridging it. Ultimately, enabling SMEs to make informed, risk-aligned decisions; whether it be to invest in a security upgrade or to purchase a cyber insurance policy strengthens not only the individual businesses but the wider economic fabric in which they operate.

CRediT authorship contribution statement

Rodney Adriko: Writing – review & editing, Writing – original draft, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Jason R.C. Nurse:** Writing – review & editing, Supervision, Project administration, Formal analysis, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: One of the authors is an editor of the Computers & Security Journal (Elsevier) Given his/her/their role as Editor, he had no involvement in the peer review of this article and had no access to information regarding its peer review. Full responsibility for the editorial process for this article was delegated to another journal editor. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendices

Appendix A. Participant information

#	Category	Industry	Years of Experience	Organisational Roles
P1	Third Party Service Provider	Government	10 yrs	Executive Leadership
P2	Researcher	Academia	8 yrs	Academic
P3	Researcher	Academia	12 yrs	Academic
P4	Researcher	Academia	10 yrs	Academic
P5	Researcher	Academia	9 yrs	Academic
P6	Third Party Service Provider	Government	15 yrs	Executive Leadership
P7	Researcher	Academia	7 yrs	Academic
P8	Third Party Service Provider	Cyber Security	11 yrs	Cyber Security Leadership
P9	Insurer	Insurance	14 yrs	Cyber Advisory / Consultancy
P10	Insurer	Insurance	18 yrs	Director-Level Management
P11	Third Party Service Provider	Government	12 yrs	Executive Leadership
P12	Insurer	Insurance	9 yrs	Director-Level Management
P13	Third Party Service Provider	Cyber security	16 yrs	Executive Leadership
P14	Insurer	Insurance	6 yrs	International Relations / Engagement
P15	Insurer	Insurance	14 yrs	Cyber Risk & Threat Intelligence
P16	Insurer	Insurance	12 yrs	Cyber Professional Services
P17	SME	Government	12 yrs	Director-Level Management
P18	Insurer	Insurance	19 yrs	Operational Leadership
P19	SME	Not for Profit	8 yrs	Board Governance
P20	SME	Professional Services	15 yrs	Director-Level Management
P21	SME	Not for Profit	9 yrs	Finance Executive
P22	SME	Professional Services	13 yrs	Executive Leadership
P23	Researcher	Academia	17 yrs	Academic
P24	SME	Professional Services	11 yrs	Training & Education Leadership
P25	Third Party Service Provider	Government	15 yrs	Executive Leadership
P26	SME	Professional Services	14 yrs	Director-Level Management
P27	Third Party Service Provider	Professional Services	12 yrs	Executive Leadership
P28	SME	Manufacturing	9 yrs	Finance Executive
P29	Third Party Service Provider	Cyber security	20 yrs	Technology Executive
P30	SME	Cyber security	11 yrs	Commercial / Account Management
P31	SME	Not for Profit	8 yrs	Technology Executive
P32	SME	Financial Services	20 yrs	Executive Leadership
P33	Third Party Service Provider	Cyber security	15 yrs	Partner / Vendor Management
P34	Third Party Service Provider	Government	6 yrs	Cyber Innovation Leadership
P35	SME	Construction	10 yrs	Cyber Security Leadership
P36	SME	Cyber security	8 yrs	Commercial / Account Management
P37	SME	Wholesale and Retail Trade	4 yrs	Director-Level Management
P38	Researcher	Government	7 yrs	Director-Level Management

Appendix B. Codebook

	Description
(R01) How SMEs make insurance decisions	
Theme	**Codes**
Influence of External Factors	Attacks on competitors
	Broker and insurer support
	Compliance with third party requirements and legislation
	Media coverage of attacks
	Personal relationships with insurance brokers
Internal Business Considerations	Competing financial priorities
	Cybersecurity is not a priority
	Monetary Impact Analysis
Product and Service Specific Factors	Cyber insurance bundled with another product
Risk Perception and Management	Fear of effects of attack
	Risk Assessment
	SME Owner's perception of risk and insurance
(R02) SME perception and understanding of cyber insurance	
Theme	**Codes**
Barriers to Cyber Insurance Adoption	Cyber insurance is expensive
	Cyber insurance is hard to buy and obtain
	Knowledge gap on cyber insurance
	No time to work on security and insurance
Perceived Value and Necessity of Cyber Insurance	Cyber insurance can replace security
	Cyber insurance is a luxury and unnecessary
	Cyber insurance is not valuable
	Cyber insurance is valuable to our Risk Management effort

(*continued on next page*)

(*continued*)

	Description
Risk Perception and Responsibility	Cyber insurance is covered in other insurance offerings
	Offloading responsibility to outsourced third party (IT service provider and cloud service providers)
	Our internal security controls are adequate
	Too small to be targeted
Trust and Efficacy of Insurance Providers	Cyber insurance is a silver bullet to cyber risk management
	Insurers do not pay claims
(RO3) Solutions to enable SMEs to make well-informed decisions regarding cyber insurance	
Theme	**Codes**
Collaborations and Partnerships	Collaboration between insurers, policyholders, and Academia
	Developing and enhancing Cyber Resilience Centres or business communities
	Government Support and involvement in cyber initiatives
	Insurance partnerships with MSPs and big technology vendors
	Insurers and insureds working together as a partnership
	Software vendors incorporating Security by Design in software
Education and Awareness	Awareness Ambassadors within SMEs
	Creating cyber awareness that relates to real and personal life experiences
	Cyber-attack simulations for SME business owners
	Cyber insurance advertisements on TV and Radio
	Enhancing cybersecurity awareness to SMEs
	Increasing customer awareness through online portals and hubs
	Increasing knowledge and awareness of insurance brokers
	Insurer and insurance brokers increasing guidance to SMEs
	Introducing Cyber Hygiene Campaigns
	National media covering cyber insurance
	Newsletters highlighting security warnings
	Simulating organisational behavioural change on cybersecurity
Incentives and Financial Support	Incentivising customers to only buy from certified secure online stores
	Monetary Relief and Incentives for Security Control Implementation
	Tax breaks for SMEs to purchase cyber insurance
Policy and Regulatory Measures	Bundling cyber insurance within security standard certifications
	Enforcing insurance through supply chain requirements
	Mandating Cyber Insurance
	Mandating Minimum Standards for SMEs
Simplification and Accessibility	Automation of cyber risk assessment by insurers
	Creating and designing simplified insurance policies
	Cyber Breach reports tailored to SMEs
	Cyber insurance bundled with other insurance lines
	Designing cyber policies tailored to SME needs
	Simple cybersecurity standards that SMEs can achieve
Technology and Innovation	Building Innovation and knowledge hubs to empower SMEs
	Data Driven methodology in Cyber Insurance
	Developing Risk Calculator to estimate cyber risk
	Effective Risk Analysis
	Facilitating accurate risk quantification
	Insurance Premium Calculator
	Use of Enterprise Risk Management Tools

Appendix C. Interview Protocol for SMEs

Introduction

1. Can you provide a brief overview of your SME, including its industry, size, country of operation, and primary operations?
2. Can you please describe your role within the SME? (e.g., job title, responsibilities)
3. What are the main cybersecurity responsibilities you handle within the organisation?
4. How would you define your level of knowledge in relation to cyber risks and cybersecurity? (On a scale of 1–10)

Perceptions and Understanding of Cybersecurity and Cyber Insurance

1. What are your thoughts on cyber insurance and its relevance to, or use to support, SMEs cybersecurity initiatives?
2. Do you think that cyber insurance can support, influence, or lead to a better security posture (or security practices) at an SME? If so, how? If not, why not?
3. Have you noticed any improvement in your cyber posture because of obtaining insurance or through support by insurers? If so, how?

Consideration of Cyber Insurance

8. Have you or your organisation considered cyber insurance as part of your risk management strategy? If yes, has your company purchased one or more insurance products to manage/mitigate your cyber risk? Who is responsible for procuring cyber insurance in your organisation?
If not,

- Has your company considered to buy any traditional insurance policy in the last two years?
- Has your company cancelled any traditional insurance policies in the last two years because of budgetary constraints/significant premium increases?
- Will your company consider buying any traditional above insurance policy in the future?
  a. What factors influenced your organisation's decision-making process regarding cyber insurance? Or what factors do you think would influence an SME's decision-making process regarding cyber insurance?

9. What solutions and strategies, including approaches and tools, do you think can be used to empower SMEs to make well-informed decisions regarding cyber insurance, ensuring alignment with their broader cybersecurity initiatives?
10. When purchasing cyber insurance were you clearly informed about any embedded exclusions and the limitations of the coverage? Were you presented with a list of examples of events that are excluded from the coverage?
11. How satisfied are you with the offered cyber insurance coverage with respect to your risk exposure? Have you issued a claim with your insurer and have any claims been declined by the insurer?
12. What aspects of insurance related to security (in the policies) do you utilise the most (e.g., pre-breach security services, post breach ones, or specific aspects. etc.)

Challenges and Needs

13. What do you see as a major challenge in your cyber insurance policy? Are there any challenges that you face with your insurers?
14. How do you think your SME can be best supported by insurers, government and other stakeholders to get the most out of cyber insurance for your business resilience?

Conclusion

15. Are there any specific areas where you feel additional support or resources are needed to enhance your cybersecurity practices?
16. Would you be willing to engage with the researchers on follow-up discussions?

Appendix D. Interview Protocol for insurers

Introduction

1. Can you please describe your role within the insurance company?
2. How long has your company been offering cyber insurance products?
3. Does your cyber insurance offering target businesses of all sizes, or particular business sizes?
4. What types of insurance products does your company offer, specifically targeting SMEs and to what extent was the contract tailored to SMEs?
5. What are the most common coverage options included in cyber insurance policies for SMEs?
6. What are the main considerations when designing cyber insurance policies for SMEs?

Perceptions and understanding of SMEs Regarding Cyber Insurance

1. From your experience, how do SMEs typically perceive cyber insurance and its importance?
2. What are some common misconceptions or challenges SMEs face when considering cyber insurance?
3. What steps and strategies have you taken to support SMEs during the initial orientation and selection process of buying cyber insurance?
4. From your experience, can cyber insurance influence or enhance security posture of SMEs? If so, how so? Is there special value of insurance to SMEs over larger organisations?
5. Basing on your experience and engagement with several SMEs, what is the main reason that SMEs purchase insurance policies?
6. What aspects of insurance related to security (in the policies) do SMEs use the most (e.g., pre-breach security services, post breach ones, or specific aspects. etc.)
7. Does your cyber insurance offering require or recommend a particular standard or good practice for assessing the risk of a potential SME? a. If yes, please identify and describe in a few words. b. If no, please name any standards or good practices you might have under consideration.
8. Have any of your customers experienced an improvement in their cyber posture because of obtaining insurance? If so, how have you supported them in enhancing their cyber resilience?

Solutions and Strategies for Empowering SMEs

1. What solutions and strategies, including approaches and tools, do you think can be used to empower SMEs to make well-informed decisions regarding cyber insurance, ensuring alignment with their broader cybersecurity initiatives?
2. How do you think insurers can best support SMEs to get the most out of cyber insurance as a risk management measure for business resilience?
3. Are there any challenges that you face when engaging with your SME cyber insurance customers that use insurance in managing their cybersecurity risk?

Conclusion

1. Is there anything else you would like to share or emphasize regarding your company's approach to cyber insurance for SMEs?
2. Would you be willing to engage with the researchers on follow-up discussions?

Appendix E. . Interview Protocol for Third-Party Service Providers Offering Security Services to SMEs

Introduction

1. Can you please describe the services your company offers to SMEs in terms of cybersecurity?
2. What services do you provide to insurers aimed at improving the policyholder's security posture?
3. What are the main cybersecurity challenges you observe among SMEs you work with?
4. How does your company assess and understand the specific needs and challenges faced by SMEs in terms of cybersecurity?

Perceptions and understanding of SMEs Regarding Cyber Insurance

1. Do you work with clients who have cyber insurance as part of their risk management effort? If yes, how do they typically perceive cyber insurance and its importance? If no, how do SMEs generally perceive cyber insurance?
2. What are some common misconceptions or challenges SMEs face when considering cyber insurance?
3. What steps and strategies have you taken to support SMEs and insurers during the initial orientation and selection process of buying cyber insurance?
4. From your interactions with SMEs, how do you perceive their understanding of cyber insurance and its relevance to cybersecurity?
5. From your experience working with SMEs, can cyber insurance influence or enhance security posture of SMEs? If so, how so? Is there special value of insurance to SMEs over larger organisations?
6. Basing on your experience and engagement with several SMEs, what is the main reason that SMEs purchase insurance policies?
7. Do you support insurers to provide continuous updates of the policyholders' cybersecurity posture? If so, how, and how often do you perform these tests?
8. What aspects of your services related to security do SMEs use the most (e.g., pre-breach security services, post breach ones, or specific aspects. etc.)
9. Have any of your clients experienced an improvement in their cyber posture because of obtaining insurance? If so, how have you supported them in enhancing their cyber resilience?

Solutions and Strategies for Empowering SMEs

1. What solutions and strategies, including approaches and tools, do you think can be used to empower SMEs to make well-informed decisions regarding cyber insurance, ensuring alignment with their broader cybersecurity initiatives?
2. How do you think insurers and MSSPs can best support SMEs to get the most out of cyber insurance as a risk management measure for business resilience?
3. Are there any challenges that you face when engaging with your clients that use insurance in managing their cybersecurity risk?

Conclusion

17. Would you be willing to engage with the researchers on follow-up discussions?

Appendix F. . Interview Protocol for Researchers with Similar Work in Empowering SMEs

1. Can you please provide an overview of your research experience and expertise around cybersecurity, cyber insurance, and SMEs? What specific aspects of research in this area have you focused on?
2. Have you conducted any previous studies or research projects related to empowering SMEs in making informed decisions regarding cyber insurance?
   - *If so, what were the main objectives and findings of these studies?*
   - *If not, in your view, how do SMEs typically approach the decision-making process regarding cyber insurance, according to your findings?*

Perceptions and Understanding of Cybersecurity and Cyber Insurance

1. From your experience, how do SMEs typically perceive cyber insurance and its importance?
2. Based on your research, what are some common misconceptions and misunderstandings of SMEs concerning cybersecurity and cyber insurance?
3. From your experience, can cyber insurance influence or enhance security posture of SMEs? If so, how so? Is there special value of insurance to SMEs over larger organisations?

Empowerment Strategies

1. Have you explored any solutions or strategies in your research to empower SMEs to make well-informed decisions regarding cyber insurance?
   - *If so, which ones?*
   - *If not, which solutions do you think would benefit SMEs in decision making?*
2. From research conducted by other researchers other than yourself, can you identify examples of approaches or tools that have shown promise in aligning cyber insurance decisions with broader cybersecurity initiatives for SMEs?
3. In your own opinion, how would you evaluate or assess the effectiveness of the proposed approaches in research?
4. Have you identified any challenges or limitations in implementing these approaches, and how do you think they can be addressed?
5. How do you think insurers can best support SMEs to get the most out of cyber insurance as a risk management measure for business resilience?

Future Directions and Collaboration Opportunities

1. What do you see as the future directions for research in empowering SMEs in cybersecurity and cyber insurance?
2. Are there any specific areas where further collaboration or partnerships could be beneficial in advancing cybersecurity research and practical solutions for SMEs?

Conclusion

1. Is there anything else you would like to share or emphasise regarding the research on cybersecurity and cyber insurance for SMEs?
2. Would you be willing to engage with the researchers on follow-up discussions?

Data availability

No data was used for the research described in the article.

References

ENISA (2023) Cyber Insurance: Fitting the Needs of Operators of Essential Services?, ENISA. https://www.enisa.europa.eu/news/cyber-insurance-fitting-the-needs-of-operators-of-essential-services.

Acora. (2024). Cyberattacks soar in Q2 2024: what SMEs need to know. https://acora.one/news/article/cyberattacks-soar-in-q2-2024-what-smes-need-to-know.

Adriko, R., Nurse, J.R.C., 2024a. Cybersecurity, cyber insurance, and small-to-medium-sized enterprises: a systematic review. Inf. Comput. Secur. 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. Digit. Threats 5 (3). https://doi.org/10.1145/3676283.

Affinity, 2024. The Growing Need for Cyber Insurance Products in SMEs. WTW. https://www.wtwco.com/en-gb/insights/2024/04/the-growing-need-for-cyber-insurance-products-in-smes.

Agarwal, P. (2021). Is cyber liability insurance an answer against growing cyber threats?

Ahmad, A., Bosua, R., Scheepers, R., 2014. Protecting organizational competitive advantage: a knowledge leakage perspective. Comput. Secur. 42, 27–39. https://doi.org/10.1016/j.cose.2014.01.001.

Allan, K. (2023). The rapidly evolving threat landscape of 2024. https://cybermagazine.com/articles/the-rapidly-evolving-threat-landscape-of-2024.

Alshaikh, M., 2020. Developing cybersecurity culture to influence employee behavior: a practice perspective. Comput. Secur. 98, 102003. https://doi.org/10.1016/j.cose.2020.102003.

Analysys Mason, 2022. SMEs' Lack of Cyber-Security Expertise Gives Providers and Operators a Strong Opportunity to Upsell Services. Analysys Mason. https://www.analysysmason.com/research/content/articles/sme-cyber-security-rdmz0-ren04/.

Anscombe, T. (2024a). Black Hat USA 2024: how cyber insurance is shaping cybersecurity strategies. https://www.welivesecurity.com/en/business-security/black-hat-usa-2024-cyber-insurance-shaping-cybersecurity-strategies/.

Anscombe, T. (2024b). Why tech-savvy leadership is key to cyber insurance readiness. https://www.welivesecurity.com/en/business-security/why-tech-savvy-leadership-key-cyber-insurance-readiness/.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., Schlitzer, M.F., 2021. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decis. Support Syst. 147, 113580. https://doi.org/10.1016/j.dss.2021.113580.

Arntzen, T.Ø.A., 2022. An effect analysis of ISO/IEC 27001 certification on technical security of norwegian grid operators. In: Proceedings of the IEEE International Conference on Big Data (Big Data), pp. 2620–2629. https://doi.org/10.1109/BigData55660.2022.10020529.

Arroyabe, M.F., Arranz, C.F.A., De Arroyabe, I.F., de Arroyabe, J.C.F., 2024. Revealing the realities of cybercrime in small and medium enterprises: understanding fear and taxonomic perspectives. Comput. Secur. 141, 103826. https://doi.org/10.1016/j.cose.2024.103826.

Brady, S. (2023), "Increasing cyber security incidents transform cyber insurance", available at: www.leasinglife.com/features/cyber-insurers-price-out-smes/(accessed 30 November 2024).

Bada, M., Sasse, A.M., Nurse, J.R.C., 2015. Cyber security awareness campaigns: why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society.

Biener, C., Eling, M., Wirfs, J., 2015. Insurability of Cyber Risk: An Empirical Analysis. Geneva Pap. Risk. Insur. Issues Pract. 40, 131–158. https://doi.org/10.1057/gpp.2014.19.

Branley-Bell, D., Coventry, L., Briggs, P., 2022. Cyber Insurance from the stakeholder's perspective: a qualitative analysis of barriers and facilitators to adoption. In: Proceedings of the 2022 European Symposium on Usable Security, pp. 151–159. https://doi.org/10.1145/3549015.3554206.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101. https://doi.org/10.1191/1478088706qp063oa.

Bryce, C., 2018. Security governance as a service on the cloud. In: Proceedings of the IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), pp. 30–35.

Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., Nurse, J.R.C., 2023. How cyber insurance influences the ransomware payment decision: theory and evidence. The Geneva Papers on Risk and Insurance - Issues and Practice 48 (2), 300–331. https://doi.org/10.1057/s41288-023-00288-8.

Chiaradonna, S., Lanchier, N., 2022. Exact Insurance Premiums for Cyber Risk of Small and Medium-Sized Enterprises. Math. Model. Nat. Phenom. 17, 40.

Chidukwani, A., Zander, S., Koutsakis, P., 2022. A Survey On The Cyber Security of small-to-medium businesses: challenges, research focus and recommendations. IEEE Access 10, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899.

Coker, J., 2024. Half of SMEs Unprepared for Cyber-Threats. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/smes-unprepared-cyber-threats/.

Collins, A., 2023. Why SMEs Must Have Cyber Insurance. Insurance Thought Leadership. https://www.insurancethoughtleadership.com/cyber/why-smes-must-have-cyber-insurance.

Cowbell, 2020. Cowbell Cyber Finds Small-to-Medium-Sized Enterprises (SMEs) More Likely to Adopt Cyber Insurance. Cowbell Cyber. https://cowbell.insure/news-events/pr/cowbell-cyber-finds-small-to-medium-sized-enterprises-smes-more-likely-to-adopt-cyber-insurance/.

Cowbell, 2023. Lack of Cyber Education Leaves Businesses Exposed, With Inadequate Risk Prevention Efforts Making 3 in 4 SMEs a Target. Cowbell Cyber. https://cowbell.insure/news-events/pr/lack-of-cyber-education-uk-survey/.

CRAG, 2024. Integrating Cyber Insurance Into Your Risk Management Strategy. CRAG. https://www.crag443.com/post/integrating-cyber-insurance-into-your-risk-management-strategy.

Curtis, H. (2024). Cyber insurance procurement process labelled 'a disaster'–insurance post. https://www.postonline.co.uk/commercial/7955448/cyber-insurance-procurement-process-labelled-a-disaster.

Dacorogna, M., Kratz, M., 2023. Managing cyber risk, a science in the making. Scand. Actuar. J. 2023 (10), 1000–1021. https://doi.org/10.1080/03461238.2023.2191869.

Databarracks. (2024). Data health check 2024. https://datahealthcheck.databarracks.com/2024/.

de Smidt, G., Botzen, W., 2018. Perceptions of corporate cyber risks and insurance decision-making. In: The Geneva Papers on Risk and Insurance - Issues and Practice, 43. Springer, pp. 239–274. https://doi.org/10.1057/s41288-018-0082-7.

Delinea, 2023. 2023 State of Cyber Insurance Report, Trends and Insights. December 30. Delinea. https://delinea.com/resources/cyber-insurance-report-2023.

Denning, N. (2022). Mind the gap: a lack of cyber security skills is leaving SMEs exposed–policy monitor. https://policymonitor.co.uk/2022/12/08/mind-the-gap-a-lack-of-cyber-security-skills-is-leaving-smes-exposed/.

Dinkova, M., El-Dardiry, R., Overvest, B., 2024. Should firms invest more in cybersecurity? Small Bus. Econ. 63 (1), 21–50. https://doi.org/10.1007/s11187-023-00803-0.

Dunn, W.N., 2018. Rediscovering pragmatism and the policy sciences. Eur. Policy Anal. 4, 13–22. https://doi.org/10.1002/epa2.1038.

Efeoghene, F., 2024. Cyber Insurance for SMEs: Affordable Protection Or Unnecessary Expense? Datafloq. https://datafloq.com/read/cyber-insurance-smes/.

El-Hajj, M., Mirza, Z.A., 2024. Protecting small and medium enterprises: a specialized cybersecurity risk assessment framework and tool. Electronics 13 (19). https://doi.org/10.3390/electronics13193910.

Eling, M., Schnell, W., 2016. What do we know about cyber risk and cyber risk insurance? J. Risk Financ. 17 (5), 474–491. https://doi.org/10.1108/JRF-09-2016-0122.

Eskins, G., & McCabe, M. (2024). Closing the cyber protection gap. https://www.marshmclennan.com/insights/publications/2024/september/closing-the-cyber-protection-gap.html.

Franke, U., 2017. The cyber insurance market in Sweden. Comput. Secur. 68, 130–144. https://doi.org/10.1016/j.cose.2017.04.010.

Franke, U., Turell, J., Johansson, I., 2021. The cost of incidents in essential services–data from Swedish NIS reporting. In: Percia David, D., Mermoud, A., Maillart, T. (Eds.), Critical Information Infrastructures Security. Springer International Publishing, pp. 116–129. https://doi.org/10.1007/978-3-030-93200-8_7.

FSB. (2024). Cracking the case: uncovering the cost of small business crime. https://www.fsb.org.uk/resource-report/cracking-the-case-uncovering-the-cost-of-small-business-crime.html.

Gilbert, S., 2017. Can a cyber insurance policy keep businesses ahead of information-security risk? J. Data Prot. Priv. 1 (3), 321–328.

GlobalDataFinancialServices, 2024. Insurers Should Look to Target the Cyber Insurance Gap Among SMEs. Life Insurance International. https://www.lifeinsuranceinternati onal.com/analyst-comment/insurers-should-look-to-target-the-cyber-insurance-gap-among-smes/.

Gohil, J., 2023. Why Cyber Insurance is a Must-Have For SMEs. Cowbell Cyber. https://cowbell.insure/blog/cyber-insurance-for-smes/.

GOV.UK, 2023. Cyber Security Breaches Survey 2023. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023.

GOV.UK, 2024a. Cyber Security Breaches Survey 2024. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024.

GOV.UK, 2024b. Improving UK Cyber Resilience: AI, Software, and Skills. GOV.UK. https://www.gov.uk/government/speeches/improving-uk-cyber-resilience-ai-software-and-skills.

GOV.UK, 2025. Cyber Security Breaches Survey 2025. GOV.UK. Retrieved June 2, 2025, from. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025.

Guest, G., Bunce, A., Johnson, L., 2006. How many interviews are enough? An experiment with data saturation and variability. Field Methods 18 (1), 59–82. https://doi.org/10.1177/1525822X05279903. Original work published 2006.

Guthrie, K.H., 2024. Doing qualitative research in a digital world: by Trena M. Paulus and Jessica N. Lester, SAGE Publications, Inc., 2021, 376 pages, 9781544321585 Paperback. Int. J. Qual. Stud. Educ. 37 (1), 314–315. https://doi.org/10.1080/09518398.2021.2003901.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., Levallet, N., 2023. Evaluating the adoption of cybersecurity and its influence on organizational performance. SN Bus. Econ. 3 (5), 97. https://doi.org/10.1007/s43546-023-00477-6.

Hiscox. (2024). Hiscox Cyber Readiness Report 2023, Hiscox Group. https://www.hiscoxgroup.com/cyber-readiness.

Herath, H.S., Herath, T.C., 2021. Cyber Insurance: Models and Challenges. In: *Encyclopedia of Cryptography, Security and Privacy*. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–4.

Hoppe, F., Gatzert, N., Gruner, P., 2021. Cyber risk management in SMEs: insights from industry surveys. J. Risk Financ. 22 (3/4), 240–260.

Hornetsecurity, 2024. Urgent Training Gap Exposed: A Quarter of Organisations Unprepared for Cyber-Attacks. Hornetsecurity–Next-Gen Microsoft 365 Security. https://www.hornetsecurity.com/en/blog/company-security-awareness-survey-2024/.

Horowitz, M. (2024). Introduction to the 2023 cybersecurity report by Maya Horowitz. https://go.checkpoint.com/2023-mid-year-security-report/.

Howden. (2024a). Cyber insurance entering a new phase of development as non-US territories set to capture 54% of growth up to 2030, according to new Howden report. https://www.howdengroupholdings.com/news/cyber-insurance-entering-a-new-phase-of-development-as-non-us-territories-set-to-capture-54-of-growth-up-to-2030.

Howden. (2024b). Howden's 2024 cyber insurance report. Retrieved August 28, 2024, from https://www.howdengroupholdings.com/reports/2024-cyber-report.

Huang, K., Wang, X., Wei, W., Madnick, S., 2023. The Devastating Business Impacts of a Cyber Breach. Harvard Business Review. https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.

IASME, 2024. Cyber Liability Insurance. Cyber Essentials. https://iasme.co.uk/cyber-essentials/cyber-liability-insurance/.

IFAC, 2023. Cybersecurity Is Critical for all Organizations–Large and Small. IFAC. https://www.ifac.org/knowledge-gateway/discussion/cybersecurity-critical-all-organizations-large-and-small.

Joshi, C., Slapničar, S., Yang, J., Ko, R.K.L., 2025. Contrasting the optimal resource allocation to cybersecurity controls and cyber insurance using prospect theory versus expected utility theory. Comput. Secur. 154, 104450. https://doi.org/10.1016/j.cose.2025.104450.

Jones, R. (2024). The state of active insurance: 2024 cyber claims report. https://www.coalitioninc.com/en-gb/blog/undefined/blog/2024-cyber-claims-report.

Kapani, C., 2024. SMEs Spending Thousands on Outsourced Cyber Security Costs. Insurance Times. https://www.insurancetimes.co.uk/news/smes-spending-thousands-on-outsourced-cyber-security-costs/1452553.article.

Kibiswa, N., 2019. Directed qualitative content analysis (DQlCA): a tool for conflict analysis. Qual. Rep. 24 (8), 2059–2079. https://doi.org/10.46743/2160-3715/2019.3778.

MacColl, J., Nurse, J.R.C., & Sullivan, J. (2021). Cyber insurance and the cyber security challenge [Reports and papers]. RUSI Occasional Paper; Royal United Services Institute for Defence and Security Studies (RUSI). https://kar.kent.ac.uk/89041/.

Maggiani, V., 2024. SMEs Remain Unprepared as Cyber Threats Escalate. UK Construction Online. https://www.ukconstructionmedia.co.uk/features/smes-remain-unprepared-as-cyber-threats-escalate/.

March, J.G., Shapira, Z., 1987. Managerial perspectives on risk and risk taking. Manag. Sci. 33 (11), 1404–1418. https://doi.org/10.1287/mnsc.33.11.1404.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A., 2017. Cyber-insurance survey. Comput. Sci. Rev. 24, 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001.

Mott, G., Turner, S., Nurse, J.R.C., MacColl, J., Sullivan, J., Cartwright, A., Cartwright, E., 2023. Between a rock and a hard(ening) place: cyber insurance in the ransomware era. Comput. Secur. 128, 103162. https://doi.org/10.1016/j.cose.2023.103162.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S.K., 2013. Cyber-risk decision models. Decis. Support Syst. 56 (C), 11–26.

Munich Re, 2024. Global Cyber Risk and Insurance Survey 2024. Munich Re. https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey.html.

NCSC. (2024). Cyber insurance industry unites to bear down on ransom payments https://www.ncsc.gov.uk/news/cyber-insurance-industry-unites-reduce-ransom-harm.

NEBRC, 2024. 12 Cyber Security Trends SMEs Should be Aware of in 2024 and Beyond. North East Business Resilience Centre. https://www.nebrcentre.co.uk/12-cyber-security-trends-smes-should-be-aware-of-in-2024-and-beyond/.

Oğüt, H., Raghunathan, S., Menon, N., 2011. Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Anal. Off. Publ. Soc. Risk Anal. 31, 497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x.

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.

Olney, M. (2023). SMEs in the crosshairs: why do hackers target small-to-medium sized enterprises? https://insights.integrity360.com/smes-in-the-crosshairs-why-do-hackers-target-small-to-medium-sized-enterprises.

Orange. (2024). Cy-Xplorer–The #1 cyber extortion report. https://www.orangecyberdefense.com/be/resourses/cy-xplorer-2024.

Osborn, E., Simpson, A., 2018. Risk and the small-scale cyber security decision making dialogue–a UK case study. Comput. J. 61 (4), 472–495. https://doi.org/10.1093/comjnl/bxx093.

Patterson, C.M., Nurse, J.R.C., Franqueira, V.N.L., 2024. "I don't think we're there yet": the practices and challenges of organisational learning from cyber security incidents. Comput. Secur. 139, 103699. https://doi.org/10.1016/j.cose.2023.103699.

Paulus, T.M., Lester, J.N., 2022. Doing qualitative research in a digital world: by Trena M. Paulus and Jessica N. Lester, SAGE Publications, Inc., 2021, 376 pages, 9781544321585 Paperback. Int. J. Qual. Stud. Educ. 37 (1), 314–315. https://doi.org/10.1080/09518398.2021.2003901.

Rafferty, I., 2024. UK Insurance Market Over Cyber 'Hurdle'. Insurance Times. https://www.insurancetimes.co.uk/analysis/uk-insurance-market-over-cyber-hurdle/1447570.article.

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

Romanosky, S., Ablon, L., Kuehn, A., Jones, T.M., 2019. Content analysis of cyber insurance policies: how do carriers price cyber risk? J. Cybersecur. 5 (1). Publisher.

Sharp. (2023). SMEs are the prime target for cyber attackscyber-attacks. https://www.sharp.co.uk/news-and-events/blog/smes-are-the-prime-target-for-cyber-attacks.

Slovic, P., 1987. Perception of risk. Science 236 (4799), 280–285. https://doi.org/10.1126/science.3563507.

Tam, T., Rao, A., Hall, J., 2021. The good, the bad and the missing: a narrative review of cyber-security implications for Australian small businesses. Comput. Secur. 109, 102385. https://doi.org/10.1016/j.cose.2021.102385.

Techdirect, 2024. TECHDIRECT, Cybersecurity Strategies for Small and Medium Enterprises (SMEs). TECHDIRECT. https://techdirect.net/blog/cybersecurity-strategies-for-small-and-medium-enterprises-smes.

Valli, C., Martinus, I., Stanley, J., & Kirby, M. (2021). CyberCheck.me: a review of a small to medium enterprise cyber security awareness program (pp. 233–242). 10.1007/978-3-030-71017-0_17.

van de Weijer, S., Leukfeldt, R., Moneva, A., 2024. Cybercrime during the COVID-19 pandemic: prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. Comput. Secur. 139, 103693. https://doi.org/10.1016/j.cose.2023.103693.

van der Kleij, R., Schraagen, J.M., Cadet, B., Young, H., 2022. Developing decision support for cybersecurity threat and incident managers. Comput. Secur. 113, 102535. https://doi.org/10.1016/j.cose.2021.102535.

Verizon, 2024a. DBIR Report 2024–Summary of Findings. Verizon Business. https://www.verizon.com/business/en-gb/resources/reports/dbir/2024/summary-of-findings/.

Verizon, 2024b. The Truth Behind 4 Cybersecurity Myths for Small Businesses. Verizon Business. https://www.verizon.com/business/en-gb/resources/infographics/four-small-business-cybersecurity-myths/.

Waelchli, S., Walter, Y., 2025. Reducing the risk of social engineering attacks using SOAR measures in a real world environment: a case study. Comput. Secur. 148, 104137. https://doi.org/10.1016/j.cose.2024.104137.

Wang, S.S., 2019. Integrated framework for information security investment and cyber insurance. Pac.-Basin Financ. J. 57, 101173. https://doi.org/10.1016/j.pacfin.2019.101173.

WEF, 2024. The Rise of AI Threats and Cybersecurity: Predictions for 2024. World Economic Forum. https://www.weforum.org/agenda/2024/02/what-does-2024-have-in-store-for-the-world-of-cybersecurity/.

Wilson, M., McDonald, S., 2024. One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses. Inf. Secur. J. Glob. Perspect. 0 (0), 1–35. https://doi.org/10.1080/19393555.2024.2357310.

Wood, A., 2024. UK SMEs Alarmingly Underprepared for Cyber Threats, Cowbell Reveals. Startups Magazine. https://startupsmagazine.co.uk/index.php/article-uk-smes-alarmingly-underprepared-cyber-threats-cowbell-reveals.

Woods, D.W., Simpson, A., 2017. Policy measures and cyber insurance: a framework. J. Cyber Policy 2, 1–18. https://doi.org/10.1080/23738871.2017.1360927.

World Bank, 2022. World Bank SME Finance: Development News, Research, Data [Text/HTML]. World Bank. https://www.worldbank.org/en/topic/smefinance.

Yanow, D., 2000. Conducting Interpretive Policy Analysis. SAGE Publications, Inc. https://doi.org/10.4135/9781412983747

Zanke, A., Weber, T., Dornheim, P., Engel, M., 2024. Assessing information security culture: a mixed-methods approach to navigating challenges in international corporate IT departments. Comput. Secur. 144, 103938. https://doi.org/10.1016/j.cose.2024.103938.