The Journal of Risk Finance

An empirical analysis of the behavioral influences and information sources affecting the cyber insurance decisions of German SMEs

213

Alina Salzberger
Friedrich-Alexander-Universität Erlangen-Nürnberg, Nuremberg, Germany

Received 27 May 2024
Revised 2 October 2024
Accepted 19 November 2024

Abstract

Purpose – The cyber insurance market in Germany shows a notable gap: while many large corporations are already demanding cyber insurance, small and medium-sized enterprises (SMEs) are still reluctant, despite its benefits. This study aims to analyze the behavioral and informational factors that influence cyber insurance decision-making and uncover the determinants that may inhibit demand among German SMEs.

Design/methodology/approach – Using the data from a questionnaire survey of 1,248 German SME executives, the influence of behavioral and informational factors on cyber insurance demand is assessed utilizing logistic regression.

Findings – The results reveal that the estimated financial impact and anxiety about a potential cyberattack significantly increase the likelihood of SMEs purchasing cyber insurance. Conversely, the perceived probability of future cyberattacks and prior experience do not significantly influence insurance decisions, probably due to challenges in probability estimation. In addition, confidence in the organization's cyber risk management has a positive but insignificant influence on cyber insurance demand. External cybersecurity specialists positively impact cyber insurance demand, while internal cyber risk assessment has no significant influence, highlighting the challenges SMEs face in cyber risk assessment. Independent Internet research negatively impacts the purchase of cyber insurance, probably due to information overload.

Originality/value – This study significantly contributes to the literature on corporate (cyber) insurance purchasing by primarily focusing on behavioral influences on SMEs' insurance decision-making. It is also the first empirical analysis of the key information sources used by SMEs in their insurance decision-making, thereby providing various academic and practical implications.

Keywords Cyber insurance, SMEs, Cyber risk perception, Behavioral influences, Information sources

Paper type Research paper

1. Introduction

As cyberattacks increasingly target German companies, with a 12% rise in affected enterprises from 2022 to 2023, based on a survey of 900 companies by Hiscox (2023), effective cyber risk management and the implementation of business cyber insurance are crucial to protect an organization from potential losses due to cyberattacks. While previous literature has identified several motives for small and medium-sized enterprises (SMEs) to purchase insurance, some of them are particularly relevant to cyber risks. For instance, as SMEs face various challenges in their cyber risk management (Hoppe *et al.*, 2021), they could especially benefit from the additional support services provided by cyber insurers. Furthermore, given the great loss potential involved in cyberattacks, the personal risk aversion of SME owners should drive cyber insurance demand (Mayers and Smith, 1982) since owners of smaller and closely held

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

The Journal of Risk Finance
Vol. 26 No. 2, 2025
pp. 213-240
Emerald Publishing Limited
e-ISSN: 2331-2947
p-ISSN: 1526-5943
DOI 10.1108/JRF-05-2024-0151

enterprises often bear organizational risk through their private wealth (Ehling, 2013; Hiebl, 2013). Despite the increasing threat, however, the demand for cyber insurance among SMEs remains low (Gothaer, 2024).

Although significant growth opportunities for cyber insurance within the SME sector are predicted, for example by Deloitte (2022), research on the insurance decision-making processes of SMEs remains limited. Furthermore, while existing literature acknowledges that the risk attitude of SME owners influences insurance decisions, there is a lack of knowledge on other behavioral factors that might also impact the insurance decisions of SMEs. The closest studies to the current paper are those of Hoppe *et al.* (2017) and de Smidt and Botzen (2018). Hoppe *et al.* (2017) empirically analyze the demand for business interruption insurance among German SMEs and find that behavioral factors such as risk aversion and insurance expertise influence SMEs' demand for insurance. De Smidt and Botzen (2018) note that prior experience, the threshold level of concern, the degree of worry and trust in organizational cyber risk management have a significant influence on cyber risk perception among managers of large Dutch organizations. While previous literature has confirmed some of the findings of de Smidt and Botzen (2018) regarding behavioral influences on cyber risk perception among German SMEs (Salzberger, 2024), no paper has focused specifically on SMEs' cyber insurance purchasing decisions to date.

This study aims to fill the existing gap by evaluating behavioral factors such as risk perception, prior experience and emotions like confidence and anxiety in the context of SMEs' cyber insurance decisions. By focusing on these factors, the analysis sheds light on the impact of behavioral factors in the business insurance contexts and offers new insights into the purchasing behavior of SMEs. Additionally, given the European Insurance and Occupational Pensions Authority's (EIOPA, 2022) emphasis on providing appropriate information on insurance access for SMEs, this paper also examines the sources of information that SMEs rely on when making cyber insurance decisions, including internal cyber risk assessment, external assistance and Internet research, which, to the best knowledge of the author, have also not been analyzed previously.

The analysis is based on data from an online questionnaire with 1,248 completed datasets from German SME executives regarding their SME cyber insurance decision-making processes and relevant information sources. The results reveal that cyber insurance demand increases with firm size and that subjective cyber risk perception in terms of estimated financial impact and perceived anxiety significantly influence cyber insurance demand. While external assistance in cyber insurance decisions positively affect the cyber insurance demand, independent Internet research decreases the likelihood that an organization will seek cyber insurance. This may highlight the need for assistance in the cyber insurance decision for SMEs and an information overload regarding this topic on the Internet. Hence, such insights could enable cyber insurers to develop more targeted marketing and distribution strategies that are potentially personalized and offline and that focus on the financial impact of successful cyberattacks and the associated negative emotions, thereby achieving higher penetration rates for cyber insurance in the SME sector (Stiefel and Jeske, 2022).

The paper is structured as follows. Section 2 provides the theoretical background on SMEs, corporate insurance motives and the cyber insurance demand. The examined cyber insurance determinants and information sources will be explained and hypotheses will be developed. In Section 3, the research method, the survey design and the data collection approach are presented. Section 4 comprises the results and a discussion of the outcomes. Section 5 summarizes the findings.

2. Theoretical background and hypothesis development

2.1 SMEs, cyber risks and the cyber insurance demand

SMEs represent 99.3% of all businesses in Germany (Institut für Mittelstandsforschung [IfM] Bonn, 2021) and 99.8% of all businesses in Europe (Di Bella *et al.*, 2023), thereby encompassing

sole proprietors, high-technology startups and niche market leaders (Hoppe *et al.*, 2021). In 2022, German SMEs generated 27.3% of the country's total turnover, amounting to 2.664 billion euros (IfM Bonn, 2023). Despite the significant proportion of SMEs among all businesses, the definition of SMEs varies globally, likely due to the high heterogeneity that SMEs exhibit (Hoppe *et al.*, 2021). However, most definitions include an upper limit on the number of employees for classification (Heidt *et al.*, 2019). The definition provided by the European Commission (2003), which is frequently applied in European SME studies (Hoppe *et al.*, 2021), sets this upper limit at 250 employees (European Commission, 2003). As additional classification criteria, the European Commission (2003) uses annual turnover (up to 50 million euros) and balance sheet total (up to 43 million euros) to distinguish between micro-, small and medium-sized enterprises [1]. Besides the advantages of high innovativeness (Hillebrand and Henseler-Unger, 2018) and adaptability to changes in their environment (Aragón-Sánchez and Sánchez-Marín, 2005), SMEs also face several challenges, such as structural barriers from limited management and technical skills (European Union, 2020) and resource constraints, including difficulties in obtaining financing and attracting skilled employees (Hoppe *et al.*, 2021). These constraints and a short-term temporal focus often lead executives in SMEs to prioritize core business processes over secondary ones like information technology (IT) security or cyber risk management, thereby allocating crucial IT security budgets elsewhere (Deloitte, 2020; Heidt *et al.*, 2019; Hoppe *et al.*, 2021). This is particularly concerning given the growing threat of cyber risk for SMEs (HDI, 2023).

In the literature, cyber risk is defined in various ways (e.g. Cebula and Young, 2010; Eling and Schnell, 2016). Zängerle and Schiereck (2023) have attempted to establish a uniform understanding by systematically evaluating over 140 text passages, revealing different subject-specific approaches to its definition. Given the focus on the cyber insurance sector, this paper adopts the one provided by Eling *et al.* (2016, p. 12), who define cyber risk as "any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services." Cyber risk, which still constitutes an emerging risk (de Smidt and Botzen, 2018), can stem from criminal activities (e.g. cyberattacks) or non-criminal causes (e.g. human failure) (Hoppe *et al.*, 2021). It can manifest as high-probability/low-impact as well as low-probability/high-impact risk. This paper specifically addresses cyber risk resulting from cyberattacks, which can take place in great variety, with great opacity and across borders (de Smidt and Botzen, 2018), while leading to both direct (e.g. business interruptions) and indirect (e.g. reputational damages) costs for the affected enterprise as well as third parties (Zängerle and Schiereck, 2023).

The number of cyberattacks against organizations is steadily increasing and is expected to also further rise in future due to the emergence of new key technologies (e.g. artificial intelligence or the metaverse) and the growing professionalism of attackers (Finlex, 2023; MunichRe, 2023). The Association of the German Information and Telecommunications Industry (Bitkom, 2023) estimates that German companies suffered losses of over 148 billion euros due to cyberattacks in 2023, though the actual figure may be even higher since many cyberattacks remain undetected (HDI, 2023) or unreported due to bureaucratic hurdles or concerns about reputational damages (Bitkom, 2023; de Smidt and Botzen, 2018). However, it is not only large organizations that are increasingly targeted, but SMEs as well. According to HDI's (2023) annual cyber study, there has been an observable shift in the relationship between company size and the frequency of attacks. While larger companies were more frequently targeted in 2022, smaller companies are now more often affected by cyberattacks than mid-sized organizations. Among the 702 German SMEs surveyed by HDI, 39% of small enterprises, 36% of medium-sized enterprises and 25% of micro-enterprises reported that they were affected by cyberattacks in 2023. The average financial loss for SMEs following a successful cyberattack amounted to 66,812 euros (HDI, 2023).

Although various cyber risk management tools to protect the organization from potential cyberattacks exist, SMEs face significant challenges in effectively managing cyber risk. Hoppe *et al.* (2021), who analyzed 37 industry surveys on SME cyber risk management, observe for

example a lack of appropriate cyber risk awareness. While SMEs are generally aware of cyber threats, they frequently underestimate their own cyber risk exposure (e.g. HDI, 2023) which can be attributed, according to Salzberger (2024), to the optimistic bias (Weinstein, 1980). Additionally, SMEs often lack expertise in cyber risk management, largely due to a lack of internal IT experts and budget constraints regarding external assistance (Hoppe *et al.*, 2021).

Even when SMEs are aware of cyber risks, they often fail to implement necessary cyber risk management measures, leading to insufficient incident response preparation (HDI, 2023; Hoppe *et al.*, 2021). However, even with extensive IT security measures, organizations may not be fully protected from losses due to cyberattacks. To manage the remaining risk exposure, SMEs could transfer these risks to an insurer through cyber insurance (Gordon *et al.*, 2003; Kosub, 2015). Cyber insurance allows companies to contractually outsource uncertain losses from cyberattacks by paying a fixed and hence predictable insurance premium (Gordon *et al.*, 2003; Mukhopadhyay *et al.*, 2013). Customers can choose between a packaged or a stand-alone cyber product, with this paper focusing on the latter as it covers cyber risks more explicitly (Eling and Zhu, 2018). Cyber insurance covers both first-party (e.g. incurred costs for data recovery or business interruption) and third-party losses (e.g. liability claims by third parties due to a data protection breach). However, its primary value lies in the accompanying assistance services (e.g. 24/7 claims hotline, data and system recovery by specialists or external security audits) that are offered by cyber insurers (Camillo, 2017; HDI, 2023). These services can significantly enhance an organization's overall cyber risk management. For instance, the HDI (2023) cyber study has found that 37% of insured companies have an incident response plan in place, compared to only 16% of uninsured ones.

The global demand for cyber insurance is steadily increasing and is estimated to reach a maximum of 33.3 billion USD by 2027 (MunichRe, 2023). In Germany, the Federal Financial Supervisory Authority (BaFin, 2024) reports that gross premiums written for stand-alone cyber policies rose to 700 million euros in 2022, a 144% increase since 2020. Despite a growing interest in cyber insurance among SMEs [2], BaFin's analysis in 2023 of 178 primary cyber insurers shows that large corporations remain the primary customers of cyber insurance, representing 81% of the total market share, while SMEs only account for 18% of premium income (BaFin, 2024). Similarly, the Gothaer SME survey of 2024 notes that only 25% of 1,022 surveyed German SMEs have obtained cyber insurance (Gothaer, 2024). Given the various insurance motives for organizations (see Section 2.2), the low cyber insurance demand of SMEs seems counterintuitive. Despite the challenges of providing appropriate cyber solutions for the highly diverse SME sector, a recent McKinsey study (Binder *et al.*, 2022) highlights significant market growth potentials for insurers due to uninsured small and micro-enterprises in Germany. Similarly, a Deloitte (2022) publication states that 16% of surveyed SMEs across multiple countries plan to include cyber insurance in their insurance portfolio within the next three years. In order to leverage these market potentials, it is essential to identify the key factors that drive cyber insurance demand.

2.2 Corporate insurance purchasing

There is extensive literature investigating the potential motives for corporate insurance demand that focuses in particular on financial advantages, organizational characteristics and the reduction of agency problems. While these studies provide valuable insights into the insurance demand of large corporations (e.g. Aunon-Nerin and Ehling, 2008; Core, 1997; Davidson *et al.*, 1992; Hoyt and Khang, 2000; Main, 1983; Regan and Hur, 2007; Yamori, 1999), the specific insurance demand of smaller and closely held enterprises has scarcely been investigated due to the limited data availability (Yamori, 1999). Table 1 summarizes the key findings related to the most relevant insurance motives for large corporations and SMEs. As shown in the table, significant differences exist between the insurance motives of smaller enterprises and those of larger organizations, despite the limited focus on SMEs in the literature so far.

Table 1. Relevant insurance motives regarding financial benefits, agency problems and organizational characteristics for large enterprises vs SMEs

	Findings for large organizations	Findings for SMEs
Financial aspects	• Insurance can reduce the *transaction costs of bankruptcy* (e.g. [1], [3], [4], [9]) • Purchasing insurance depends on the *financial situation* (e.g. the capitalization, debt capacity, cost of distress, cash availability, capital market access) of the enterprise (e.g. [5], [6], [8], [9], [12]) • Insurance is purchased to achieve *earnings stability* (e.g. [7]) • Insurance is purchased to reduce taxable income and expected tax liabilities (e.g. [1],[4], [9]) – other results found by [7] and [10]. The German tax system offers limited opportunities to reduce the tax burden through insurance [8]	• *Expected bankruptcy costs* are less than proportional to firm size, making insurance more valuable for smaller firms (e.g. [1], [5], [9]) – opposing results found by [16]: SMEs with a higher probability of bankruptcy purchase less insurance, probably because riskier SMEs cannot afford to buy insurance • *Price-sensitive* SMEs purchase less business interruption insurance [17] • Smaller firms purchase insurance to *protect equity* [8] • Tax incentives have been shown to be a motive for purchasing insurance among Japanese SMEs [16]
Agency problems/ information asymmetries	*Between bondholders and shareholders* Differing interests between debtholders and shareholders can lead to an underinvestment problem. By requiring insurance, debtholders limit a firm's risk to a certain level while reducing the agency costs of monitoring the behavior of the equity holders and increasing firm value (e.g. [2], [3], [4], [12]) – other results found by [7] *Between management and shareholders* Insurers have a comparative advantage in monitoring risk-reducing decisions made by management for shareholders [1], with the degree of risk aversion of managers depending on the extent to which compensation is linked to performance (e.g. [4], [6], [13]) *Relationship with others* • Insurance is motivated by competition and can facilitate cooperation and coordination (e.g. [14]) • Insurance can act as a signal of firm quality – greater levels of coverage signal higher expected cash flows (e.g. [7], [15])	*Between bondholders and shareholders* • Insurance could be used to strengthen the existing relationship: insurance demand within private firms is motivated by increasing the organization's debt capacity [18] due to the high importance of bank borrowings (which are the main sources of financing) for SMEs. Those facing financial constraints due to weak relationships with their banks tend to have a higher insurance demand [16] • Insurance is often purchased by SMEs at the request of banks [16] *Between management and shareholders* In SMEs, a separation between ownership and management is often not possible (e.g. [8],[16]). Therefore, the risk management motives of owners and managers are much more aligned [18]: the owners of closely held organizations have greater control over management behavior than those of widely held organizations [8]

(*continued*)

Table 1. Continued

	Findings for large organizations	Findings for SMEs
Organizational aspects	*Ownership structure* Corporations purchase less insurance than closely held firms with concentrated ownership (e.g. [1], [6], [8], [11]) – other results found by [9] and [10] *Organizational size* Smaller enterprises purchase more insurance than larger organizations (e.g. [1], [4], [8], [9], [10], [11]) – other results found by [6] *Industry* • Regulated firms purchase more insurance than unregulated firms (e.g. [1], [6], [9], [10]) – other results by [4] • Firms from industries where higher operating revenues are associated with a higher insurance risk purchase insurance (e.g. [15]) *Other characteristics* • Organizations with greater *growth opportunities* purchase more directors' and officers' (D&O) insurance to improve management decision-making and avoid underinvestment (e.g. [6]) • Firms with greater *internal risk diversification* (e.g. technological) require less insurance (e.g. [8]) • Insurance is purchased due to *comparative advantages* in risk bearing and the *real service efficiencies of the insurer* (e.g. [1], [4], [7], [8], [9])	*Ownership structure* For SMEs a negative relation between ownership concentration and insurance demand and a positive one between the number of family owners and insurance demand has been identified [18] – other results found by [16]: the importance of financial benefits as an insurance motive varies with the ownership structure *Organizational size* Smaller SMEs purchase less insurance than larger ones (e.g. [16], [17]) *Industry* Organizations in trading and manufacturing industries purchase more business interruption insurance [17] *Other characteristics* *Growth potential* is not significantly related to insurance demand in SMEs, probably because SMEs with growth expectations do not have sufficient financial resources to purchase insurance [16]

Note(s): [1] Mayers and Smith (1982), [2] Mayers and Smith (1987), [3] MacMinn (1987), [4] Hoyt and Khang (2000), [5] Aunon-Nerin and Ehling (2008), [6] Core (1997), [7] Main (1983), [8] Krummaker (2019), [9] Regan and Hur (2007), [10] Yamori (1999), [11] Krummaker and Graf von der Schulenburg (2008), [12] Davidson *et al*. (1992), [13] Han (1996), [14] Ashby and Diacon (1998), [15] Grace and Rebello (1993), [16] Asai (2019), [17] Hoppe *et al*. (2017), [18] Ehling (2013)
Source(s): Authors own creation

One of the most critical differences highlighted in the literature regarding insurance motives for SMEs and large corporations is risk aversion. Risk aversion does not apply as an insurance motive for large organizations, since shareholders can diversify risk through capital markets, leading to a negative net present value when purchasing insurance at actuarially unfair rates (Mayers and Smith, 1982; Regan and Hur, 2007). However, risk aversion constitutes an important insurance motive for owners of smaller enterprises (Greenwald and Stiglitz, 1990; Mayers and Smith, 1982). Owners of smaller enterprises are generally more sensitive to risk changes as a single risk event can lead to catastrophic losses, as well as business closure and liability involving private assets (Ehling, 2013; Hiebl, 2013).

To the best of the author's knowledge, only three papers have empirically examined the insurance demand of SMEs. Ehling (2013) analyzes the insurance demand of Norwegian

SMEs, using over 1,855 firm-year observations from an international insurance broker on property insurance purchases. Asai (2019) assesses the insurance demand of 767 Japanese SMEs in the manufacturing industry. Finally, Hoppe *et al.* (2017) evaluate the business interruption insurance decisions of 1,732 German SMEs. Among these, only Ehling (2013) and Hoppe *et al.* (2017) incorporate behavioral factors such as risk aversion within their analysis. While Ehling (2013) cannot confirm that risk aversion has a major impact on SME's insurance decision-making, Hoppe *et al.* (2017) find that both risk aversion and insurance know-how have a significant positive influence on the decision to purchase business interruption insurance.

Aside from risk aversion, which is the most important insurance motive for individuals (Krummaker, 2019), other behavioral factors, such as biases (e.g. overconfidence bias), heuristics (e.g. the availability heuristic) and risk perception have been extensively studied in the context of individual insurance decisions (e.g. Bregu, 2022; Kellens *et al.*, 2013; Siegrist and Gutscher, 2008). However, these factors have not been adequately explored in the context of insurance decision-making for SMEs, although Mayers and Smith (1982) suggest that smaller and/or closely held firms may have the same insurance motives as individuals, and Heidt *et al.* (2019) concludes that individual leadership attitudes and values may have a strong influence on IT security investments. Previous research indicates that behavioral influences, particularly biases and heuristics, are especially prevalent in the decision-making process of SMEs in the organizational context (Capolupo *et al.*, 2024). They are also more significant for entrepreneurs in smaller organizations than for managers in larger companies. This may be due to a higher level of uncertainty in decision-making, stemming from limited data availability, as well as a higher decision complexity, resulting from the absence of structured decision-making processes (Busenitz and Barney, 1997). Thus, the unconscious use of heuristics to "reduce the complex tasks of assessing probabilities and predicting values to simpler judgmental operations" (Tversky and Kahneman, 1974, p. 1124) could be a valid strategy for overcoming decision-making constraints.

However, the use of heuristics can also lead to persistent biases which can negatively impact risk assessment, for example, through misleading experiences or emotions (Slovic, 1987). As executives in smaller enterprises might be subject to behavioral factors in their insurance decision-making, cognitive biases may explain the relatively low demand for cyber insurance among SMEs despite the clear benefits outlined in Table 1. Additionally, while Hoppe *et al.* (2017) investigate the influence of different distribution channels on SMEs' insurance decisions, revealing that SMEs with business interruption insurance demonstrate significantly higher "trust in the insurance distribution" (p. 576), "agent affinity" (p. 576) or "broker affinity" (p. 576) than those without business interruption insurance, a gap in understanding the sources of information influencing SMEs' cyber insurance decisions remains. This study seeks to fill these gaps by evaluating additional behavioral influences, such as subjective risk perception, prior experience, confidence and anxiety, as well as by identifying the most relevant information sources for SMEs when considering cyber insurance.

2.3 Hypothesis development

2.3.1 Organizational size. Most of the previous literature suggests that smaller enterprises should purchase more insurance than larger organizations (see Table 1 in Section 2.2). This expectation is often explained by the bankruptcy cost hypothesis, according to which smaller enterprises have to face higher expected bankruptcy costs, making insurance more valuable for them (Aunon-Nerin and Ehling, 2008; Hoyt and Khang, 2000; Mayers and Smith, 1982). In the context of cyber insurance, the service efficiencies and comparative advantages of insurers in processing claims and other administrative services further support this expectation (Hoyt and Khang, 2000; Main, 1983; Mayers and Smith, 1982, 1990). While larger organizations typically have dedicated security teams, adequate IT budgets and sophisticated internal risk management processes (Huaman *et al.*, 2021; Krummaker, 2019), SMEs are facing significant

challenges in cyber risk management (see Section 2.1) and could therefore particularly benefit from the services offered by cyber insurers (Talesh, 2018). However, contrary to these theoretical expectations, recent industry surveys and market data reveal that cyber insurance demand actually increases with enterprise size (see Section 2.1). This unexpected relationship has also been observed in other insurance contexts, such as business interruption insurance for SMEs (Hoppe *et al.*, 2017) and corporate terrorism insurance (Thomann *et al.*, 2012). Considering these findings and current market observations leads to formulating the following hypothesis H1:

H1. Smaller enterprises purchase significantly less cyber insurance than larger organizations.

2.3.2 Cyber risk perception. Both Hoppe *et al.* (2017) and Thomann *et al.* (2012), who observe a counterintuitive relationship between insurance demand and enterprise size, suggest that behavioral factors, such as subjective risk perception (Thomann *et al.*, 2012), may influence organizational insurance decisions. According to the expected utility theory, which may also apply to organizational insurance decisions (Thomann *et al.*, 2012), cyber insurance should be purchased if it provides a higher expected utility than remaining uninsured (Kshetri, 2018). However, making insurance decisions typically requires information about the probability of risk occurrence and the expected loss, which might not be always available for SME executives, given the current challenges in obtaining relevant information regarding cyberattack probability and expected losses (Kshetri, 2018) and SMEs' limited cyber risk assessment capabilities (Hoppe *et al.*, 2021). Hence, as supposed by Slovic (1987), executives might "rely on intuitive risk judgments" (Slovic, 1987, p. 280) instead of purely objective estimations within their cyber insurance decision-making process. Consequently, subjective risk perception might strongly influence decisions related to risk protection (Barberis, 2013; de Smidt and Botzen, 2018) and insurance (Slovic *et al.*, 1977). Despite its importance, subjective risk perception, most frequently measured by the determinants of "perceived impact" and "perceived probability" (Kellens *et al.*, 2013), has received limited attention in previous research on SMEs' insurance decisions.

For large organizations, previous literature on insurance demand has found a positive relation between the expected distress cost and the degree of corporate property insurance coverage (Aunon-Nerin and Ehling, 2008). In the cyber context, based on their survey with 172 managers of large organizations in the Netherlands, de Smidt and Botzen (2018) observe a low cyber insurance demand, accompanied by an underestimation of the expected cost of a successful cyberattack. Although de Smidt and Botzen (2018) hypothesize a link between low cyber insurance demand and the underestimation of financial impacts, they do not further analyze this relationship. As the annual cyber study from HDI (2023) shows that only 23% out of 702 asked German SMEs perceive a high to rather high risk of financial losses from potential cyberattacks, an underestimation of financial impact might also be observable in the SME sector. Building on this observation and the assumption of de Smidt and Botzen (2018), hypothesis H2a is:

H2a. SME executives with a higher degree of cyber risk perception in terms of the estimated financial impact of a cyberattack are more likely to purchase cyber insurance.

Thomann *et al.* (2012) posit that managers also buy terrorism insurance based on their personal assessment of the probability of risk occurrence. Similarly, Huaman *et al.* (2021), analyzing cyber risk perception measured by the perceived likelihood of successful cyberattacks among 5,000 German SMEs, find that smaller enterprises (fewer than 50 employees) perceive a lower likelihood of becoming a victim of cyberattacks compared to larger organizations (more than 500 employees). Given that the observed relationship between probability estimates and cyber insurance demand is positive for increasing organizational size, a positive relation between probability estimates for cyberattacks and insurance demand might also exist, as suggested by Thomann *et al.* (2012). Therefore, H2b is stated as follows:

H2b. SME executives with a higher degree of cyber risk perception in terms of the perceived probability of cyberattack occurrence are more likely to purchase cyber insurance.

2.3.3 Prior experience. According to Tversky and Kahneman (1973, 1974), risk perceptions can be influenced by the availability heuristic, which suggests that prior experience with risk events can significantly drive the ease of imagining (similar) risk events occurring in the future (de Smidt and Botzen, 2018; Tversky and Kahneman, 1974), thereby increasing risk perceptions and motivating the purchase of insurance. The influence of prior experience on insurance demand has already been shown, for example, by Thomann *et al.* (2012) with respect to terrorism insurance, as they observe that the terrorist activity level of the prior 12 months strongly influences corporate decisions about that type of insurance.

For cyber risk, Salzberger (2024) has already observed that personal experience with cyberattacks has a positive influence on the perception of cyber risk in regard to the probability estimates of future cyberattacks for SME owners and managers. Asai (2019) does not find that prior experience of natural disasters has an influence on SMEs' demand for property liability insurance, based on an ordinary least squares analysis of data from 767 Japanese SMEs. However, a positive influence on cyber insurance demand is assumed, as a survey by Advisen and Partner Re (2020) reveals that media coverage and experience of cyber-related losses are the two most important factors driving the demand for cyber insurance, according to the 260 cyber insurance brokers and 190 cyber underwriters surveyed. Hence, following this leads to hypothesis H3:

H3. SME executives with personal experience of successful cyberattacks are more likely to purchase cyber insurance.

2.3.4 Perceived confidence. In addition to availability, the overconfidence bias may influence the cyber insurance decisions of SMEs. Overconfidence refers to an individual's tendency to overestimate their own skills, predictive abilities and knowledge (Russo and Schoemaker, 2018) which, as a result, might lead to intuitive and impulsive management decisions with little understanding of which tasks would require further assistance or expertise (Chira *et al.*, 2008). Although the influence of overconfidence on insurance demand has already been shown in various settings, its direction remains unclear. While Bregu (2022) has found in a within-subject experiment involving 128 subjects that individuals purchase significantly less insurance when overestimating their abilities to predict potential losses, Hoppe *et al.* (2017) observe that German SMEs that rated their insurance competencies higher were significantly more likely to purchase business interruption insurance.

In the context of cyber risk, Salzberger (2024) observes that German SMEs generally rate their internal knowledge and competencies highly, despite most of them lacking essential cyber risk management measures. In support of these observations, Hoppe *et al.* (2021) find within their meta-study about SMEs' cyber risk management that SMEs are generally overconfident about their cyber risk preparedness, resulting in a substantial gap between perceived and actual readiness for potential cyberattacks. Hence, the overestimation of existing cyber risk preparedness might lead to the erroneous assumption that no further protection against losses from cyberattacks through cyber insurance is needed, resulting in a low cyber insurance demand among German SMEs. Following this assumption leads to hypothesis H4:

H4. SME executives with a higher level of confidence in the organization's cyber risk management measures are less likely to purchase cyber insurance.

2.3.5 Perceived anxiety. According to the "risk as feelings" model from Loewenstein *et al.* (2001), emotions such as "worry, fear, dread, or anxiety" (Loewenstein *et al.*, 2001, p. 270) can significantly influence risk perception and decision-making under conditions of risk and uncertainty. The model suggests that individuals may perceive risk through an emotional lens,

relying more on their instincts and institutions rather than on logic, reason or scientific principles to assess risk. In particular, when judging the likelihood and severity of an event, people tend to act based on feelings that are generated by the "vividness" (Loewenstein *et al.*, 2001, p. 275) of the personal experience or the perceived danger of the event. Therefore, if cyberattacks are perceived as highly threatening, the heightened perception of cyber risk should motivate the demand for cyber insurance. Brighetti *et al.* (2014) have already found that emotions influence the individual insurance decision, though the effects vary depending on the different emotions and insurance types analyzed.

In the cyber domain, de Smidt and Botzen (2018) observe that worry has a significant positive influence on the perceived probability and impact of future cyberattacks for managers of large organizations. However, according to Cheung-Blunden and Ju (2016) and Lawson *et al.* (2016), feelings of anxiety can also negatively impact information perception and processing. While a certain level of anxiety might encourage protective cybersecurity behavior, excessive anxiety has been shown to result in impaired memory processes within risk evaluation (e.g. Derakshan and Eysenck, 2009). Consequently, it remains unclear whether negative emotions about cyberattacks effectively motivate the implementation of protection measures or whether anxiety leads to inefficient and biased information processing without meaningful behavioral changes (Renaud and Dupuis, 2019; Renaud and Ophoff, 2021). Although Kshetri (2020) suggests that insurers promote cyber insurance by leveraging fear and anxiety, whether the level of perceived anxiety actually influences the cyber insurance purchasing behavior of SMEs has not yet been analyzed. Therefore, hypothesis H5 is posited as follows:

H5. SME executives with a higher level of anxiety regarding future cyberattacks are more likely to purchase cyber insurance.

2.3.6 Information sources. Hoppe *et al.* (2017) is the only empirical analysis that also focuses on the influence of relevant distribution channels on SMEs' insurance decisions. They show that German SMEs that frequently review their insurance needs and have high insurance expertise are more likely to demand business interruption insurance. Similarly, the Global Cyber Risk Perception Survey by Marsh and Microsoft (2019), which included 1,500 business leaders from organizations of different countries and sizes, found that organizations conducting quantitative internal risk assessments are more likely to purchase cyber insurance. However, Krummaker (2019) assumes that the professionalism of the internal insurance decision-making process decreases along with decreasing enterprise size. The various challenges in cyber risk management for SMEs (see Section 2.1), combined with the complexity and variety of insurance products available to SMEs (EIOPA, 2022), could lead to a biased cyber risk assessment and the conclusion that insurance is not needed. Nonetheless, it is assumed that SMEs conducting internal cyber risk assessments are generally more aware of their cyber risk exposure than those without such evaluations and thus are more likely to purchase insurance. Hypothesis H6a is therefore:

H6a. SME executives are more likely to purchase cyber insurance when they analyze their cyber risk exposure through internal cyber risk assessment measures.

Following the previous argument, EIOPA (2022) notes that SMEs may need assistance in their insurance decision-making. While Hoppe *et al.* (2017) have found that German SMEs with business interruption insurance heavily rely on the recommendations of their insurance broker, Vero (2021) reports a decline in broker engagement, with more than 25% of the 1,500 Australian SMEs surveyed only having minimal contact with their insurance broker in 2021, up from approximately 9% in 2012. Similarly, the share of SMEs actively collaborating with their brokers also decreased from approximately 35% in 2012 to 22% in 2021. Reflecting this trend, the annual HDI (2023) cyber study shows that SMEs rely heavily on external "IT service providers" and "IT consulting" for cybersecurity, with 45% of the 702 asked SME executives reporting that their installed prevention measures are based on recommendations from these

external experts. Consequently, the role of independent cybersecurity experts may become increasingly important in the decision to purchase cyber insurance among SMEs. Therefore, H6b is proposed as follows:

H6b. SME executives are more likely to purchase cyber insurance when they receive assistance from external cybersecurity experts in their cyber risk management and insurance decisions.

In the past, SMEs often tended to "set and forget" (Vero, 2021, p. 8) their insurance, while in the past decade, they have sought to become more involved in insurance, with 60% of the 1,500 participating SMEs in the Vero survey indicating that they personally research their insurance needs online. Similarly, a global KPMG (2021) survey with 75,000 participating SMEs shows that the availability of clear and simple information about insurance online and the ability to buy insurance online are two of the most important features when purchasing business interruption insurance, after price. Regarding cybersecurity, according to the HDI (2023) cyber study, the Internet is the fourth most important source of information for German SMEs on IT and cyber security, while in the UK online research ranks first among the most relevant sources of information for advice or guidance on cybersecurity issues (Renaud and Ophoff, 2021). Assuming that online information provided by cyber insurers is well suited for SMEs, online research on cyber insurance should positively influence SMEs' demand for cyber insurance. Therefore, H6c is proposed as follows:

H6c. SME executives are more likely to purchase cyber insurance when they independently research cyber insurance products online.

3. Research method, survey design and data sampling

3.1 Research method and survey design

To analyze the determinants of *CyberIns* assumed in hypotheses H1 to H6c, a logistic regression analysis is employed, following the approach of Hoppe *et al.* (2017), Gatzert and Schubert (2022) and Lechner and Gatzert (2018), who examine the determinants of business interruption insurance for German SMEs and organizational cyber risk management and enterprise risk management, respectively. Following Gatzert and Schubert (2022) and Lechner and Gatzert (2018), it is assumed that

$$CyberIns = f\left(Size, Cost, Prob, Experience, Confidence, Anxiety, Intern, Extern, Internet\right)$$

The binary dependent variable, *CyberIns*, takes a value of 1 if an enterprise demands cyber insurance and 0 otherwise. By applying the logarithmized quotient of the probability that an enterprise demands cyber insurance and the converse probability, one can calculate the odds ratio. The coefficients β_1 to β_{11} denote the estimated regression parameters for the respective determinants. Size dummies were included which reflect the respective enterprise sizes of micro-, small, medium-sized and large enterprises.

$$\begin{aligned} ln\left(\frac{p\left(CyberIns=1\right)}{1-p\left(CyberIns=1\right)}\right) &= \beta_{1-3}\,Size + \beta_4 Cost + \beta_5\,Prob + \beta_6\,Experience \\ &\quad + \beta_7\,Confidence + \beta_8\,Anxiety + \beta_9 Intern + \beta_{10} Extern \\ &\quad + \beta_{11}\,Internet + \varepsilon. \end{aligned}$$

Due to the limited availability of data on SME cyber insurance decision-making, a large standardized online questionnaire was developed which was mainly derived from the one used by de Smidt and Botzen (2018) for analyzing the cyber insurance demand and cyber risk perception of managers from large Dutch organizations. The current study focuses on the

cyber insurance demand of German SMEs, as well as the behavioral influences in their insurance decision-making process and the most relevant information sources affecting their decision. Consequently, questions about the current demand for cyber insurance, previous experience of cyberattacks, perceived confidence in cyber risk management, anxiety regarding future cyberattacks and information sources related to the cyber insurance decision-making process are of particular interest for this analysis. The relevant questions included in this analysis can be found in the Supplementary material.

First, and in contrast to the questionnaire of de Smidt and Botzen (2018), the respondents were informed about the most common types of cyberattacks against German SMEs between 2020 and 2022 (i.e. malware, phishing, [distributed] denial-of-service [(D)DoS] and ransomware attacks [3]) to ensure a common understanding of the different types of cyberattacks surveyed in the questionnaire. Following the approach of de Smidt and Botzen (2018), risk perception was measured using the variables of "perceived probability" and "perceived impact." Therefore, the participants were asked first about their perceived probability of being the target of a successful cyberattack of each cyberattack type (*Prob_Malware*, *Prob_Phishing*, *Prob_DoS*, *Prob_Ransomware*), measured on a scale from 0% to 100% [4]. A cyberattack was defined as successful if it results in financial damage to the targeted organization. The mean of the four provided probability estimates was calculated to generate the overall *Prob* variable included in the logistic regression model. The same procedure was applied to ask for the estimated cost of successful cyberattacks. The respondents rated their expected financial impact of successful malware (*Cost_Malware*), phishing (*Cost_Phishing*), (D)DoS (*Cost_DoS*) and ransomware (*Cost_Ransomware*) attacks on a six-point scale (1 = less than €25,000 to 6 = more than €500,000 [5]), and the overall mean *Cost* variable was calculated. The *Prob* and *Cost* variables, therefore, constitute the cyber risk perception variables relevant to hypotheses H2a and H2b.

In a procedure similar to that employed by de Smidt and Botzen (2018), the respondents were next asked to rate their confidence in the cyber risk management measures implemented in their organizations on a six-point Likert scale. In particular, they were asked about the sufficiency and appropriateness of the installed cyber risk *Prevention* and *Reaction* measures for potential cyberattacks [6]. The mean score of both questions was calculated to obtain the *Confidence* variable for analyzing hypothesis H4. Following the approach of Elhai *et al.* (2017), the level of anxiety concerning potential cyberattacks was assessed through seven anxiety-related items measured on a seven-point Likert scale [7]. The mean score of these seven items was computed to form the *Anxiety* variable, which was used to analyze hypothesis H5. In line with the question utilized by de Smidt and Botzen (2018), to evaluate the influence of previous *Experience*, respondents were asked if they had been affected by a cyberattack in the past in various contexts (i.e. within their own enterprise or in previous work situations, private surroundings or personally). Since previous literature has emphasized that the experienced risk event must be perceived as salient to influence risk perception and insurance demand (Gennaioli and Shleifer, 2010; de Smidt and Botzen, 2018), the respondents were also asked if the cyberattack resulted in financial damages. Therefore, the experience variable in the logistic regression model is set to 1 for all the respondents who experienced a financially damaging cyberattack and to 0 for all others.

Next, and again in line with de Smidt and Botzen (2018), the respondents were asked about their cyber insurance status (*CyberIns*). The SME executives could choose from the response options "have cyber insurance," "plan to purchase cyber insurance," "have not purchased and do not plan to purchase cyber insurance" and "have not discussed the issue within the organization" [8]. Respondents who chose the last response option were removed from the dataset, as *CyberIns* is the dependent variable of the logistic regression, with the binary values indicating whether the organization has decided for or against purchasing cyber insurance. As outlined in hypotheses H6a to H6c and in line with recent findings from industry studies

regarding SMEs' information sources, respondents were asked whether they based their cyber insurance decision on an internal risk assessment (*Intern*), advice from an external cybersecurity specialist (*Extern*), or information obtained from the *Internet*. Respondents could rate their agreement with each information source on a seven-point Likert scale (1 = do not agree at all to 7 = completely agree) for the analysis of hypotheses H6a to H6c.

Finally, questions were included about the enterprise (i.e. the number of employees, the annual sales, the balance sheet total and industry) and the respondent (i.e. company function, age and gender), along with a question to assess the respondent's answering accuracy (rated on a seven-point Likert scale).

3.2 Data sampling

Parts of the online survey that focused on the influence of behavioral factors on SME cyber risk perception have been previously evaluated. Therefore, a detailed description of the data collection and pretesting processes can be found in Salzberger (2024).

To reach the relevant target group of German SMEs, a comprehensive database accessible through the university network was employed. The selection criteria were based on the definition of SMEs used by the European Commission (2003), which includes enterprises with a maximum of 249 employees, an annual turnover of up to 50 million euros, and a balance sheet total of up to 43 million euros. The filtering resulted in 430,439 enterprises with accessible email addresses, although for most organizations only general firm email addresses were available. Following the approach of Hiebl *et al.* (2019), and to ensure that the survey reached the appropriate decision-makers regarding cyber insurance, the intended recipients were defined as owners, members of the managing board or responsible managers from the IT or risk management departments. To verify the respondents' role, a question that asked for the company function(s) of the respondents was integrated into the questionnaire. Given the expected low response rate typical in organizational surveys, as noted by de Smidt and Botzen (2018), it was decided to contact all available organizations (convenience sampling), in line with the method utilized in Hiebl *et al.* (2019). Furthermore, it was technically ensured that every organization could answer the online questionnaire only once.

Of the 430,439 companies that were contacted to participate in the online survey, 5,638 confirmed they had received the email invitation, as evidenced by opening the link to the online questionnaire. A total of 1,828 enterprises completed the questionnaire. Of these, 463 datasets were excluded because the respondent indicated that their enterprise had not yet decided whether to buy cyber insurance and the outcome of this decision was necessary for conducting the logistic regression. In addition, 68 datasets were removed as the responding person was not the owner, a member of the managing board or an executive from the IT or risk management departments, ensuring the accuracy and relevance of the information provided regarding cyber insurance decisions. Furthermore, 16 datasets from companies in the public sector or associations and 33 datasets with a low answering accuracy of the respondents (scores of 3 and below on the seven-point Likert scale) were excluded. As a result, a total of 1,248 datasets are analyzed in this paper for the first time in regard to cyber insurance demand. Following the methodology of Hiebl *et al.* (2019) and utilizing the delivery-confirmed emails as denominator (N = 5,638), a response rate of 22.13% was achieved. Using the total number of firms contacted (N = 430,439) resulted in a response rate of 0.3%.

As in Salzberger (2024), a test for non-response bias was conducted in line with Armstrong and Overton (1977) by using an extrapolation method for time trends. A *t*-test was employed to compare the responses of the first third and the last third of respondents for the relevant variables of *Prob*, *Cost*, *Anxiety*, *Confidence*, *Intern*, *Extern* and *Internet* (following the approaches of Gupta and Hammond, 2005; Ulrich *et al.*, 2022). No significant differences were found in the responses between the two subgroups [9], indicating that the following analysis is unlikely to be affected by non-response bias. The analysis was conducted utilizing Microsoft Excel, SPSS and Stata.

4. Results and discussion

4.1 Summary statistics and univariate differences

4.1.1 Sample characteristics. The final sample (N = 1,248) consists of 293 (23.5%) micro-enterprises and 571 (45.8%) small, 272 (21.8%) medium-sized and 112 (9.0%) large enterprises, based on the classification used by the European Commission (2003). In terms of industry distribution, 14.8% of the responding enterprises operate in the manufacturing industry (N = 185), followed by 14.3% from the information and communication sector (N = 178), while 9.4% operate in other economic sectors (N = 117). A complete list containing the classification of the business sectors according to the German Federal Bureau of Statistics is provided in Table B1 in the Supplementary material. Of the total 1,248 respondents, 840 (67.3%) are members of the management board, 540 (43.3%) are responsible for IT and 174 respondents (13.9%) work in the risk management department (see Table B2 in the Supplementary material). The sample includes 84.3% (N = 1,052) male and 12.8% female (N = 160) respondents (with 2.9% of respondents not providing gender information). The average age of the respondents is 49.35 years (N = 1,133).

4.1.2 Cyber insurance demand and information sources. After excluding the initial 427 datasets from enterprises that have not yet decided whether to purchase cyber insurance, the survey results show that 44.7% (558 of N = 1,248) of the responding enterprises have not obtained or do not plan to buy cyber insurance. Meanwhile, 38.0% (474 of N = 1,248) already have cyber insurance, while 17.3% (216 of N = 1,248) plan to sign a cyber insurance contract in the future. Regarding information sources, internal cyber risk assessments (*Intern*) and *Internet* research on cyber insurance were conducted more extensively by companies that actively sought cyber insurance compared to those who decided not to. Additionally, companies with cyber insurance relied more heavily on the assistance of an external cyber security expert (*Extern*) than those without cyber insurance (see Table B3 in the Supplementary material).

4.1.3 Behavioral influences. Cyber risk perception was measured using variables for the perceived probability and estimated financial impact of malware, phishing, (D)DoS and ransomware attacks. On average, the respondents estimated a 38.62% probability of their firm suffering a successful cyberattack within the next year. The mean estimated cost of a successful cyberattack was 2.37, indicating an estimated cost of €25,000 to €100,000 per attack (see Table B4 in the Supplementary material for detailed descriptive values for each cyberattack type).

Perceived anxiety was assessed using seven anxiety-related items concerning future cyberattacks. The mean *Anxiety* score was 2.52 (Cronbach's alpha = 0.883; standard deviation [SD] = 1.25; N = 1,248), measured on a seven-point Likert scale, indicating a generally low level of anxiety among German executives regarding future cyberattacks (see Table B5 in the Supplementary material for detailed descriptive values of the items and the aggregated variable). *Confidence* in organizational cyber risk management was measured utilizing the two variables of *Prevention* and *Reaction*, both assessed on a six-point Likert scale. The aggregated mean *Confidence* was 4.32 (Cronbach's alpha = 0.850, SD = 1.13; N = 1,248), indicating a generally high degree of confidence in the implemented cyber risk management measures within the sample (see Table B6 in the Supplementary material for more details). Additionally, 72.1% (900 of N = 1,248) reported having experienced a cyberattack, either in their own organization, in their previous work, personally or in their personal lives. Among those with prior *Experience*, most respondents (46.6% of N = 900) successfully defended against the cyberattack. For analysis, the variable of *Experience* categorized the respondents into the two groups of enterprises that were successfully attacked (N = 318) and those that were not targeted or for whom the cyberattack did not result in financial damage (N = 930) (see Table B7 in the Supplementary material).

Table 2 summarizes the descriptive statistics for the variable *CyberIns* and the analyzed determinants.

Table 2. Summary statistics

	Mean	SD	Min	Median	Max
CyberIns	0.5529	0.49739	0.00	1.0000	1.00
Size	2.1627	0.88649	1.00	2.0000	4.00
Cost	2.3754	1.29886	1.00	2.0000	6.00
Prob	0.3862	0.27915	0.00	0.3250	1.00
Experience	0.2548	0.43593	0.00	0.0000	1.00
Confidence	4.3221	1.13592	1.00	4.5000	6.00
Anxiety	2.5209	1.25401	1.00	2.2857	7.00
Intern	5.2644	1.94362	1.00	6.0000	7.00
Intern_transformed	0.5734	0.33926	0.014	0.5000	1.00
Extern	2.2772	2.03105	1.00	1.0000	7.00
Internet	2.6955	1.91023	1.00	2.0000	7.00

Source(s): Authors own creation

4.1.4 Univariate differences. Table 3 shows the univariate statistics of the subsamples of enterprises that either already have or plan to purchase cyber insurance ($N = 690$) and those that have already decided against cyber insurance ($N = 558$). Regarding *Size*, organizations in the *CyberIns* group are significantly larger compared to those in the No-*CyberIns* group. Furthermore, enterprises with *CyberIns* exhibit a significantly higher risk perception in both the mean *Cost* estimate and the mean *Prob* estimate of potential cyberattacks, compared to those without *CyberIns*. In addition, the degree of perceived *Anxiety* concerning future cyberattacks is significantly higher in the *CyberIns* group than in the No-*CyberIns* group. The level of *Confidence* in cyber risk prevention and reaction measures does not differ significantly between the two groups. The difference in prior *Experience* of a successful cyberattack is significant only at the 5% level.

Regarding the information sources, although organizations with *CyberIns* exhibit a higher level of internal cyber risk assessment (*Intern*), the difference between the two groups is only significant at the 5% level. However, enterprises with *CyberIns* rely significantly more on an

Table 3. Univariate differences across groups with ($N = 690$) and without *CyberIns* ($N = 558$)

	CyberIns group ($N = 690$)		No-CyberIns group ($N = 558$)		Differences		Effect size Cohen's	
	Mean	Median	Mean	Median	In means	In medians	|d|	|r|
Size	2.3797	2.000	1.8943	2.000	0.4854***	0.000***	0.569	0.2716
Cost	2.7127	2.500	1.9583	1.500	0.7543***	1.000***	0.606	0.3187
Prob	0.4245	0.400	0.3388	0.2625	0.0857***	0.1474***	0.311	0.1664
Experience	0.2797	0.000	0.2240	0.000	0.0557*	0.000*	0.128	0.0635
Confidence	4.3051	4.500	4.3432	4.500	−0.0381	0.000	0.034	0.0173
Anxiety	2.7409	2.429	2.2488	2.000	0.4921***	0.2486***	0.400	0.2069
Intern	5.3652	6.000	5.1398	6.000	0.2254*	0.000	0.116	0.0263
Intern_transformed	0.5782	0.500	0.5675	0.500	0.0107	0.000	0.032	0.0263
Extern	2.5406	1.000	1.9516	1.000	0.5890***	0.000***	0.293	0.1621
Internet	2.0275	1.000	3.5215	4.000	−1.4940***	−3.000***	0.849	0.3800

Note(s): Differences in means are based on a *t*-test. Differences in medians are based on a non-parametric Mann–Whitney *U*-test. ***denotes statistical significance at the 1% level, *denotes statistical significance at the 5% level. Small effect size from |d| = 0.2 (respectively |r| = 0.1), medium effect size from |d| = 0.5 (respectively |r| = 0.3) and large effect from |d| = 0.8 (respectively |r| = 0.5) (Cohen, 1992)
Source: Authors own creation

external cybersecurity specialist for their decision-making (*Extern*), while enterprises without *CyberIns* depend on their decision not to purchase cyber insurance significantly more on independent *Internet* research.

4.2 Pearson and Spearman's rank correlation coefficients

Table B8 in the Supplementary material presents the Pearson and Spearman's rank correlation coefficients between *CyberIns* and the analyzed determinants. A statistically significant positive relation is identified between *CyberIns* and the determinants *Size*, *Cost*, *Prob*, *Anxiety* and *Extern*. Conversely, a statistically significant negative relation is found between *CyberIns* and *Internet* research. A positive correlation at the 5% significance level is identified between *CyberIns* and *Experience*, while no significant relation is noted for *Confidence* and *Intern*. Since absolute correlation coefficients above a threshold value of 0.8 are not observed (Mason and Perreault, 1991) and the calculated variance inflation factors all fall below the threshold of 10 (Marquardt, 1970), multicollinearity should not pose a problem in the following logistic regression analysis.

4.3 Empirical results of the logistic regression regarding the determinants of cyber insurance demand

The results of the logistic regression are shown in Table 4. The first column presents the respective hypothesis, the second the independent variable, the third the expected relationship

Table 4. Results of the logistic regression regarding the determinants of *CyberIns* ($N = 1{,}248$)

Hypothesis	Variable	Predicted relationship	Parameter estimate (β)	Standard error	Wald	*p*-value	Odds ratio exp (β)
1	*Size*	–			28.433	0.000***	
	Size (1)		−1.295	0.315	16.920	0.000***	0.274
	Size (2)		−1.026	0.293	12.236	0.000***	0.358
	Size (3)		−0.434	0.312	1.928	0.165	0.648
2a	*Cost*	+	0.339	0.061	31.138	0.000***	1.403
2b	*Prob*	+	0.407	0.262	2.418	0.120	1.502
3	*Experience*	+	0.182	0.156	1.356	0.244	1.199
4	*Confidence*	+	0.091	0.064	2.018	0.155	1.096
5	*Anxiety*	+	0.265	0.062	18.506	0.000***	1.303
6a	*Intern_transformed*	+	0.075	0.207	0.130	0.718	1.077
6b	*Extern*	+	0.153	0.036	18.485	0.000***	1.165
6c	*Internet*	+	−0.481	0.039	153.429	0.000***	0.618
	Intercept		−0.016	0.459	0.001	0.972	0.984
Model fit							
R^2 Nagelkerke		0.354					

Note(s): (1) In line with the proposed procedure of Tabachnick and Fidell (2014) and to comply with the conditions of the logistic regression, the linearity of the logit was examined for metric variables by evaluating the interaction between the determinants and the ln transformation of the respective determinant. Due to a violation of the linearity assumption by *Intern*, the variable was transformed into $Intern\_transformed = \frac{1}{(Max_{(Intern)}+1-Intern}$; to normalize the strong left-skewed distribution, a reciprocal transformation was used, thereby adding "$Max_{(Intern)}+1$" to ensure that the transformation was defined over all values of *Intern* (Field, 2018); (2) The logistic regression was repeated without the *Intern_transformed* variable. Both the values for Nagelkerke's R^2 and AUC as well as the results concerning the significances and relations of the determinants with *CyberIns* remained unchanged; (3) The reference category for the categorial variable of *Size* was large enterprises, whereby *Size (1)* indicates micro-enterprises, *Size (2)* small enterprises and *Size (3)* medium-sized enterprises; *** indicate the 1% statistical significance level

Source(s): Authors own creation

and the fourth the parameter estimate (β). The standard error, the Chi-square value of the Wald test, the p-value and the odds ratios exp(β) are also presented.

The overall fit of the logistic regression model is shown by a Nagelkerke's pseudo R^2 of 0.354 and a high value for the area under the receiver operating characteristic (ROC) curve (area under the curve [AUC] = 0.804) [10].

The results of the logistic regression show that organizational *Size* (Wald[3] = 28.433, $p < 0.001$), the *Cost* estimate of future cyberattacks (Wald[1] = 31.138, $p < 0.001$), perceived *Anxiety* of potential cyberattacks (Wald[1] = 18.506, $p < 0.001$), the assistance of *Extern* cybersecurity experts (Wald[1] = 18.485, $p < 0.001$) and independent *Internet* research on cyber insurance (Wald[1] = 153.429, $p < 0.001$) all significantly influence whether a German enterprise demands cyber insurance or not (significance of the model: $\chi^2[11] = 383.710$; $p = 0.000$).

In line with the predefined hypotheses, the results of the logistic regression confirm a significant positive relationship between the *Size* of an organization and the demand for cyber insurance (H1), i.e. smaller enterprises purchase significantly less cyber insurance than large ones. A significant difference in cyber insurance demand is observed when comparing micro-enterprises to large enterprises, with the probability of purchasing cyber insurance decreasing by 72.6% for micro-enterprises compared to large enterprises ($p < 0.001$; exp[β] = 0.274). Similarly, a significant difference is identified between small and large enterprises, with the probability of purchasing cyber insurance decreasing by 64.2% for small enterprises compared to large enterprises ($p < 0.001$; exp[β] = 0.358). Both size variables indicate a substantial effect on cyber insurance demand (Chen *et al.*, 2010). However, no significant difference is observable in the demand for cyber insurance between medium-sized and large enterprises ($p = 0.165$).

Consistent with H2a, the estimate of the financial impact of future cyberattacks (*Cost*) has a significant positive influence on the demand for cyber insurance, i.e. executives who estimate a higher financial impact from potential cyberattacks are more likely to purchase cyber insurance (H2a). Specifically, a one-unit increase in perceived financial impact (measured on a six-point scale) increases the likelihood of purchasing cyber insurance by 40.3% ($p < 0.001$; exp[β] = 1.403). However, for the second component of cyber risk perception, the perceived probability of future cyberattacks (*Prob*), no statistically significant relationship ($p = 0.120$) could be found (H2b). In line with the assumption of de Smidt and Botzen (2018), only the cost estimate of future cyberattacks seems to be relevant in the decision-making process regarding cyber insurance, while the perceived probability is not. De Smidt and Botzen (2018) attribute this to the challenges executives might face in estimating probabilities due to the high uncertainty and complexity of cyber risks. Since their study focuses on executives of large enterprises with more advanced cyber risk management processes, such an observation is particularly reasonable for the executives of SMEs with corresponding deficiencies in cyber risk management and assessment abilities.

As hypothesized in H5, executives who exhibit a higher level of anxiety about future cyberattacks (*Anxiety*) are more likely to purchase cyber insurance. Specifically, a one-unit increase in the perceived anxiety regarding future cyberattacks (measured on a seven-point Likert scale) increases the likelihood of an organization purchasing cyber insurance by 30.3% ($p < 0.001$; exp[β] = 1.303), indicating a small but significant effect (Chen *et al.*, 2010). In contrast, the determinants of previous *Experience* with successful cyberattacks (H3) and *Confidence* in cyberattack preparedness (H4) have no significant influence on the demand for cyber insurance ($p = 0.244$ and $p = 0.155$ respectively). The rejection of H3 could be linked to that of H2b. According to Tversky and Kahneman's (1974) availability heuristic, prior experience primarily influences probability and likelihood estimates, but not cost estimates. Since the perceived probability of cyberattacks (H2b) was found to be insignificant, this might explain why prior experience (H3) also lacks significance. The annual cyber study by HDI (2023) supports this finding, showing that SMEs' cost estimates for successful cyberattacks vary only slightly between those with experience (84,202 euros) and those without (85,244 euros). A significant correlation is also only observed in the current paper for *Experience* and

the *Prob* variable, but not for the *Cost* variable (see correlation analysis Table B8 in the Supplementary material). Regarding H4, in line with the findings of Hoppe *et al.* (2017) on SMEs' demand for business interruption insurance, a positive relation between *Confidence* in cyber risk management and insurance demand is identified which argues against an overconfidence bias regarding cyber risk preparedness, suggesting that cyber insurance appears to be part of an appropriate cyber risk management system. However, the relationship was not statistically significant, as also evidenced by the non-significant correlation between the two variables (see Table B8 in the Supplementary material).

The influence of internal cyber risk assessment (*Intern*) on the demand for cyber insurance was found to be insignificant ($p = 0.718$), leading to the rejection of H6a. This finding aligns with Krummaker (2019), who noted a decreasing professionalism in risk management processes with decreasing enterprise size. Consequently, the cyber risk management processes carried out in SMEs may not be sufficiently sophisticated to provide a realistic assessment of their current cyber risk exposure. As a result, internal cyber risk assessment fails to increase the awareness of cyber risks, thereby not motivating the demand for insurance. In contrast, the assistance of external cybersecurity experts (*Extern*) has a significant positive influence on the demand for cyber insurance, which confirms H6b. External and professional assistance in cyber risk assessment and the corresponding insurance decision likely results in a more accurate and alarming evaluation of an organization's cyber risk exposure, which in turn increases the likelihood of purchasing cyber insurance. Specifically, a one-unit increase in the *Extern* variable (measured on a seven-point Likert scale) increases the likelihood of purchasing cyber insurance by 16.5% ($p < 0.001$; $\exp[\beta] = 1.165$).

Contrary to H6c, independent *Internet* research on cyber insurance has a significant negative effect on the demand for cyber insurance. A one-unit increase in the *Internet* variable (measured on a seven-point Likert scale) decreases the likelihood of purchasing cyber insurance by 38.2% ($p < 0.001$; $\exp[\beta] = 0.618$). This could be attributed to an information overload that SMEs may encounter online. In line with this, Meier and Burda (2020) explain the lack of concrete cybersecurity measures in SMEs by the overwhelming nature of the topic of information security. This is also confirmed by the study of Renaud and Ophoff (2021), in which 56% of the 361 UK SMEs surveyed stated that online cybersecurity information was "beyond my needs" (p. 34). Hillebrand and Henseler-Unger (2018) report similar findings for German SMEs in expert interviews back in 2018, suggesting that the SME-suitable presentation of cyber products online is likely to be a long-term problem.

4.4 Robustness tests regarding the determinants of CyberIns

In accordance with Lechner and Gatzert (2018), and to assess the impact of potential outliers, an additional analysis was conducted excluding 19 outlying observations with standardized residuals greater than 2 in absolute value (Backhaus *et al.*, 2021). The results of the logistic regression with the adjusted sample are shown in Table B9 in the Supplementary material. The additional analysis demonstrates an even higher level of goodness of fit (Nagelkerke's pseudo $R^2 = 0.412$; AUC = 0.826), and the relationships between *CyberIns* and the determinants of *Size*, *Cost*, *Anxiety*, *Extern* and *Internet* remain highly significant (overall significance of the model: $\chi^2[11] = 452.123$; $p = 0.000$). Therefore, the logistic regression results from Section 4.3 should not be distorted by potential outliers.

Another common issue in empirical research is endogeneity caused by omitted variables, where the independent variables correlate with the error term, potentially compromising the robustness of statistical inference and the reliability of estimation results (Bendig and Hoke, 2024; Frank, 2000). To initially assess endogeneity, Pearson correlations between the analyzed determinants and the residual of the logistic regression were calculated. The results indicate significant correlations only for the determinants of *Cost* and *Internet*, although the correlation values of 0.0672 and −0.0988 suggest a weak relationship between these determinants and the residuals. To further address potential confounding variables and evaluate the robustness of the

results, the robustness of inference to replacement was analyzed, as proposed by Bendig and Hoke (2024) and Xu *et al.* (2019). This method calculates the percentage of bias necessary to invalidate the inference for the determinants included in the logistic regression, based on the average marginal effects in a nonlinear model. The analysis revealed that for *Size* 55.42% (692 out of $N = 1{,}248$), for *Cost* 66.35% (828 out of $N = 1{,}248$), for *Anxiety* 55.54% (693 out of $N = 1{,}248$), for *Extern* 55.49% (693 out of $N = 1{,}248$) and for *Internet* 88.02% (1,098 out of $N = 1{,}248$) of cases would need to be replaced with cases for where the effect is zero to invalidate the inference. Given that more than 50% of cases for each determinant would need to be replaced, it is "unlikely that a confounding variable will significantly influence the estimates" (Bendig and Hoke, 2024, p. 154).

Furthermore, various sensitivity analyses have been performed. Following Gatzert and Schubert (2022), who conducted an additional logistic regression with robust standard errors, a bootstrapping approach with 2,000 samples and bias-corrected and accelerated 95% confidence intervals (Efron, 1987) was applied. This approach, using approximated robust standard errors, confirms the significant influence of the variables of *Size*, *Cost*, *Anxiety*, *Extern* and *Internet* on *CyberIns* demand.

In addition, a stepwise logistic regression approach was conducted, as in Hoppe *et al.* (2017). This involved gradually including blocks of determinants related to cyber insurance demand (e.g. first incorporating behavioral factors, followed by informational factors and enterprise size). This allows for assessing the robustness of the results and the impact of each block on the overall model. As can be seen in Table B10 in the Supplementary material, the inclusion of behavioral factors (i.e. *Cost*, *Prob*, *Experience*, *Confidence* and *Anxiety*) results in a Nagelkerke's pseudo R^2 value of 0.145. This value increases to 0.331 with the additional informational factors analyzed (i.e. *Intern*, *Extern*, *Internet*). Incorporating *Size* as an additional independent variable further increases the Nagelkerke's pseudo R^2 slightly to 0.354.

Furthermore, while Gatzert and Schubert (2022) conduct robustness checks for different industries (i.e. the banking and insurance industry), this study performs them across different enterprise sizes. To examine the impact of behavioral and informational factors on cyber insurance demand for different enterprise sizes, logistic regression analyses were conducted separately for each of the four firm sizes. The results of these analyses are presented in Table B11 in the Supplementary material. The results reveal that the influence of behavioral factors on the cyber insurance decision diminishes as firm size increases. Specifically, subjectively estimated *Cost* and the perceived level of *Anxiety* regarding future cyberattacks significantly affect the decision only in micro-enterprises and small firms. Additionally, the assistance of external cybersecurity experts (*Extern*) impacts the cyber insurance decision-making only in micro-, small and large enterprises. The significant effect observed for large firms may be attributed to the increasing complexity of cyber risk management in large enterprises, which may require external assistance. Conversely, the negative impact of *Internet* research on cyber insurance decision-making is significant across all firm sizes, indicating that information overload from online cyber security information may be a common issue faced by all firms.

As an additional sensitivity analysis, the logistic regression was extended to include industry variables as further determinants of cyber insurance demand, although this is not the focus of the current paper. Specifically, due to enhanced regulatory requirements relating to cyber security, critical entities are expected to have greater cyber risk awareness and consequently a higher demand for cyber insurance [e.g. the Critical Entities Resilience (CER) Directive from the European Parliament, Council of the European Union, 2022]. Following the definition of the CER Directive, organizations from the energy, transport, banking, financial market infrastructure, health, drinking and wastewater, digital infrastructure, public administration, space and food production, processing and distribution sectors are included in the critical entities variable (*CrEn*). Two critical infrastructure sectors, the finance and insurance industry (*FinIns*) and the information and communication industry (*InfCom*), are considered separately. This is due to their high volume of sensitive data (Gatzert and Schubert,

2022) and data-centric business model, which may further incentivize securing against cyberattack losses through insurance. The results are provided in Table B12 in the Supplementary material. Critical entities (*CrEn*) and organizations from the finance and insurance industry (*FinIns*) show a significantly higher likelihood of demanding insurance (significant at the 5% level). However, the determinants of *Size*, *Cost*, *Anxiety*, *Extern* and *Internet* remain highly significant at the 1% level.

5. Conclusion

As discussed, various motives drive organizations to purchase insurance, with most literature observing that smaller enterprises tend to obtain more insurance than large corporations. For cyber risks in particular, SMEs should benefit from the various assistance services provided by cyber insurers due to their significant challenges in cyber risk management. Considering the increasing threat of cyberattacks, it seems counterintuitive that larger enterprises currently demand more cyber insurance than SMEs. Given that the literature suggests SMEs to purchase insurance for similar reasons as individuals, a significant gap has been recognized in analyzing behavioral influences other than risk aversion on insurance demand. These aspects have already been evaluated in the individual's insurance context. Moreover, these behavioral factors may help explain the discrepancy between the actual cyber threat landscape and the cyber insurance demand among SMEs. Moreover, as EIOPA has recently emphasized the importance of information about insurance access for SMEs (EIOPA, 2022), this study also analyzed the influence of different information sources on SMEs' insurance decisions.

The results confirm observations from current industry studies that the demand for cyber insurance significantly increases with company size. Furthermore, the perception of the financial impact of future cyberattacks significantly drives the demand for cyber insurance, such that SMEs that anticipate a higher financial impact are more likely to purchase cyber insurance. However, the probability estimation of potential cyberattacks has no significant influence on SMEs' cyber insurance decisions, probably due to the inherent difficulties in accurately estimating the likelihood of such events. Additionally, SME executives with a higher level of anxiety about future cyberattacks are more likely to seek cyber insurance, while prior experience with cyber incidents and confidence in their organizational cyber risk management do not have a significant impact on their cyber insurance decisions. Information from internal cyber risk assessments does not considerably influence demand, whereas the assistance of external cybersecurity experts in the decision-making process significantly drives the likelihood of purchasing cyber insurance. These results may confirm the challenges SMEs are facing within internal cyber risk assessment while emphasizing the positive influence of external advice that SMEs may need in their cyber insurance decisions. In addition, SMEs that rely on independent Internet research are less likely to purchase cyber insurance, probably due to information overload regarding the cybersecurity topic on the Internet.

These findings make significant contributions to the academic as well as the practical literature. Academically, this study provides crucial insights into the cyber insurance decisions of SMEs by exploring behavioral factors such as risk perception and anxiety as significant influences. Additionally, it is one of the first to empirically assess the relevant information sources used by SMEs in their cyber insurance decision-making process. In practical terms, the findings offer valuable knowledge for cyber insurers. Considering the importance of perceived financial impact and anxiety about future cyberattacks, as well as the high confidence in one's own cyber risk management measures, insurers should focus on making risks and potential consequences more vivid and tangible while emphasizing the limitations of the internal cyber risk management strategies implemented (de Smidt and Botzen, 2018). Furthermore, as many SMEs are currently underinsured, focusing on the relevant influencing factors within the cyber insurance decision and providing well-suited and customized cyber insurance solutions for the highly heterogeneous SME segment could unlock substantial growth opportunities for

insurers (Binder *et al.*, 2022). Moreover, by finding effective ways to communicate the benefits of cyber insurance to SMEs, insures could help these businesses avoid information overload and gain access to comprehensive cyber risk management services (Talesh, 2018). Given the critical economic role of SMEs (Sukumar *et al.*, 2023), enhancing their protection against cyber risk could also be of particular interest to the government, contributing to the overall stability and prosperity of the SME sector in Germany (EIOPA, 2023).

Although the current analysis provides valuable insights, it also has some limitations. Since the questionnaire was sent via email to the respective SMEs, a self-selection bias may exist (Heidt *et al.*, 2019). Furthermore, as only one executive from each SME participated in the survey, it cannot be ruled out that individual attitudes or motivations influenced the responses provided (von Skarczinski *et al.*, 2022). However, since the top management typically makes cyber risk management decisions in SMEs, the subjective assessments of executives are relevant in explaining willingness to purchase cyber insurance (Meier and Burda, 2020). Moreover, the response rate within the current analysis is relatively low compared to other online surveys, although low response rates are common for surveys that focus on the organizational context (de Smidt and Botzen, 2018). The study relies on cross-sectional data, while longitudinal data could also provide meaningful insights into the determinants of cyber insurance decision-making in SMEs. Although follow-up questionnaires often face limited participation in the organizational context, as shown by Dreißigacker *et al.* (2021), future research could benefit from this approach. Finally, while the paper focuses on behavioral influences, other factors like budget constraints or insurance costs (de Smidt and Botzen, 2018) could be explored in subsequent works, as they were not the focus of this evaluation.

Notes

[1]. Micro-enterprises: up to nine employees and up to 2 million euros in annual turnover or balance sheet total, small enterprises: up to 49 employees and up to 10 million euros in annual turnover or balance sheet total, and medium-sized enterprises: up to 249 employees and up to 50 million euros in annual turnover or 43 million euros in balance sheet total (European Commission, 2003).

[2]. An increase in the demand for cyber insurance among SMEs is shown, for example, in the annual SME study by the cyber insurer Gothaer (2024), which surveyed approximately 1,000 German SMEs. In this study, 25% of the SMEs reported having purchased cyber insurance in 2024, representing an increase of 5% compared to 2023 (20%) and 9% compared to 2021 (16%).

[3]. A study by Dreißigacker *et al.* (2021) has identified the most relevant types of cyberattacks affecting German companies in 2020, including malware, phishing and ransomware attacks. Similarly, research by Bitkom (2022) shows comparable trends for 2021 and 2022, although (D)DoS attacks were more common than ransomware attacks in those years. Therefore, probability and cost estimates were asked for malware, phishing, ransomware and (D)DoS attacks.

[4]. While de Smidt and Botzen (2018) ask about the probability that a successful cyberattack targets the own organization as an open question, in this questionnaire the respondents could choose their perceived probability by moving a slider between 0% and 100% to clearly define the uniformity of the answers in terms of format and margins.

[5]. For estimating the financial impact of a successful cyberattack, the survey question of de Smidt and Botzen (2018) was followed but amended by using a six-point Likert scale with adopted cost ranges (1 = less than €25,000, 2 = between €25,000 and €50,000, 3 = between €50,000 and €100,000, 4 = between €100,000 and €250,000, 5 = between €250,000 and €500,000 and 6 = more than €500,000) reflecting current market observations from the cyber insurer HDI regarding cyber losses for SMEs in Germany at the time of the study (HDI, 2022). Adjustments were necessary as de Smidt and Botzen (2018) focus on large enterprises, where the cost ranges correspond to higher expected damages.

[6]. While de Smidt and Botzen (2018) asked about the managers' degree of trust in their organization's ability to successfully prevent, mitigate and deal with successful cyberattacks within a single question, SME executives were asked about their agreement regarding the installation of appropriate prevention measures against cyberattacks and their preparedness to respond to cyberattacks in two

separate questions. Furthermore, to enhance uniformity within the questionnaire, the degree of confidence was measured on a six-point Likert scale (1 = do not agree at all to 6 = completely agree), rather than on a four-point scale as in de Smidt and Botzen (2018).

[7]. While de Smidt and Botzen (2018) only asked the surveyed managers to indicate their degree of worry of a successful cyberattack against the own enterprise on a five-point Likert scale, a more sophisticated approach was used in this paper. Following Elhai *et al.* (2017), who have analyzed the degree of anxiety related to electronic data hacking by utilizing an adapted version of the Generalized Anxiety Disorder-7 scale (GAD-7) from Spitzer *et al.* (2006), a modified GAD-7 version relating to cyberattacks in an organizational context (and not only to data hacking in a personal context) was employed. Furthermore, to increase consistency within the questionnaire, the four-point scale from Elhai *et al.* (2017) was expanded to a seven-point Likert scale, where respondents had to rate their agreement (1 = do not agree at all to 7 = completely agree) with the following items: when thinking about the possibility of a successful cyberattack against the own enterprise, (1) I feel nervous and anxious, (2) I feel like I can't stop or control my worries, (3) I worry a lot about my enterprise's cybersecurity, (4) I am afraid that a cyberattack could also affect my enterprise, (5) I quickly feel angry, annoyed or irritated, (6) I find it difficult to sit calmly and (7) I find it difficult to relax.

[8]. The question regarding cyber insurance demand was adopted from the questionnaire of de Smidt and Botzen (2018). However, they did not provide an option for respondents to indicate that their organization had not yet discussed whether cyber insurance should be purchased. Instead, they only provided the option of not having cyber insurance. There might, however, be a difference between actively deciding against cyber insurance and not having it because it has not yet arisen as a topic within the organization.

[9]. Only for the *Internet* variable was a significant difference observed, such that the first third of respondents rated their use of the Internet as a source of information for the cyber insurance decision significantly higher than the last third. However, it is not surprising that the respondents who use the Internet more frequently are also among the first third of those in the online survey.

[10]. The AUC can have a maximum value of 1. The closer the AUC value is to 1, the better the predictive power (Backhaus *et al.*, 2021).

References

Advisen and Partner Re (2020), "Cyber insurance – the market's view", available at: https://www.partnerre.com/wp-content/uploads/2020/09/Cyber-Insurance-The-Markets-View-2020.pdf (accessed 8 April 2024).

Aragón-Sánchez, A. and Sánchez-Marín, G. (2005), "Strategic orientation, management characteristics, and performance: a study of Spanish SMEs", *Journal of Small Business Management*, Vol. 43 No. 3, pp. 287-308, doi: 10.1111/j.1540-627X.2005.00138.x.

Armstrong, J.S. and Overton, T.S. (1977), "Estimating nonresponse bias in mail surveys", *Journal of Marketing Research - Special Issue: Recent Developments in Survey Research*, Vol. 14 No. 3, pp. 396-402, doi: 10.2307/3150783.

Asai, Y. (2019), "Why do small and medium enterprises (SMEs) demand property liability insurance?", *Journal of Banking and Finance*, Vol. 106, pp. 298-304, doi: 10.1016/j.jbankfin.2019.07.012.

Ashby, S.G. and Diacon, S.R. (1998), "The corporate demand for insurance: a strategic perspective", *The Geneva Papers on Risk and Insurance - Issues and Practice*, Vol. 23 No. 86, pp. 34-51, doi: 10.1057/gpp.1998.3.

Aunon-Nerin, D. and Ehling, P. (2008), "Why firms purchase property insurance", *Journal of Financial Economics*, Vol. 90 No. 3, pp. 298-312, doi: 10.1016/j.jfineco.2008.01.003.

Backhaus, K., Erichson, B., Gensler, S., Weiber, R. and Weiber, T. (2021), *Multivariate Analysemethoden*, 16th ed., Springer Gabler, Wiesbaden.

BaFin (2024), "Cyber insurance: strong demand – but what about the risks?", available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2024/fa_bj_2402_Cyberversicherung_en.html (accessed 8 April 2024).

Barberis, N. (2013), "The psychology of tail events: progress and challenges", *American Economic Review: Papers and Proceedings*, Vol. 103 No. 3, pp. 611-616, doi: 10.1257/aer.103.3.611.

Bending, D. and Hoke, J. (2024), "Probing for omitted variable bias: the role of the impact threshold of a confounding variable in complementing instrumental variable estimations", *Industrial Marketing Management*, Vol. 122, pp. 145-159, doi: 10.1016/j.indmarman.2024.08.009.

Binder, S., Horsch, P., Lorenz, J.-T. and Schollmeier, F. (2022), "Small and medium-size commercial insurance: the big opportunity", available at: https://www.mckinsey.com/industries/financial-services/our-insights/small-and-medium-size-commercial-insurance-the-big-opportunity (accessed 8 April 2024).

Bitkom (2022), "Wirtschaftsschutz 2022", available at: https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf (accessed 31 May 2023).

Bitkom (2023), "Wirtschaftsschutz 2023", available at: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf (accessed 8 April 2024).

Bregu, K. (2022), "The effect of overconfidence on insurance demand", *The Geneva Risk and Insurance Review*, Vol. 47 No. 2, pp. 298-326, doi: 10.1057/s10713-021-00064-5.

Brighetti, G., Lucarelli, C. and Marinelli, N. (2014), "Do emotions affect insurance demand?", *Review of Behavioral Finance*, Vol. 6 No. 2, pp. 136-154, doi: 10.1108/RBF-04-2014-0027.

Busenitz, L.W. and Barney, J.B. (1997), "Differences between entrepreneurs and managers in large organizations: biases and heuristics in strategic decision-making", *Journal of Business Venturing*, Vol. 12 No. 1, pp. 9-30, doi: 10.1016/S0883-9026(96)00003-1.

Camillo, M. (2017), "Cyber risk and the changing role of insurance", *Journal of Cyber Policy*, Vol. 2 No. 1, pp. 53-63, doi: 10.1080/23738871.2017.1296878.

Capolupo, N., Virglerova, Z., Rosa, A. and Palmucci, D.N. (2024), "The relationship between biases and entrepreneurial decision-making. Evidence from Italian and Czech SMEs", *International Entrepreneurship and Management Journal*, Vol. 20 No. 4, pp. 3323-3348, doi: 10.1007/s11365-024-00983-5.

Cebula, J.J. and Young, L.R. (2010), "A taxonomy of operational cyber security risks", available at: https://insights.sei.cmu.edu/documents/2198/2010_004_001_15200.pdf (accessed 8 April 2024).

Chen, H., Cohen, P. and Chen, S. (2010), "How big is a big odds ratio? Interpreting the magnitudes of odds rations in epidemiological studies", *Communications in Statistics - Simulation and Computation*, Vol. 39 No. 4, pp. 860-864, doi: 10.1080/03610911003650383.

Cheung-Blunden, V. and Ju, J. (2016), "Anxiety as a barrier to information processing in the event of a cyberattack", *Political Psychology*, Vol. 37 No. 3, pp. 387-400, doi: 10.1111/pops.12264.

Chira, I., Adams, M. and Thornton, B. (2008), "Behavioral bias within the decision making process", *Journal of Business and Economics Research*, Vol. 6 No. 8, pp. 11-20, doi: 10.19030/jber.v6i8.2456.

Cohen, J. (1992), "A power primer", *Psychological Bulletin*, Vol. 112 No. 1, pp. 155-159, doi: 10.1037//0033-2909.112.1.155.

Core, J.E. (1997), "On the corporate demand for directors' and officers' insurance", *The Journal of Risk and Insurance*, Vol. 64 No. 1, pp. 63-87, doi: 10.2307/253912.

Davidson, W.N., Cross, M.L. and Thornton, J.H. (1992), "Corporate demand for insurance: some empirical and theoretical results", *Journal of Financial Services Research*, Vol. 6 No. 1, pp. 61-71, doi: 10.1007/BF01046118.

de Smidt, G. and Botzen, W. (2018), "Perceptions of corporate cyber risks and insurance decision-making", *The Geneva Papers on Risk and Insurance: Issues and Practice*, Vol. 43 No. 2, pp. 239-274, doi: 10.1057/s41288-018-0082-7.

Deloitte (2022), "The future of small business insurance – what do customers want?", available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-small-business-survey-report.pdf (accessed 8 April 2024).

Deloitte (2020), "Cyber Security im Mittelstand", available at: https://www.deloitte.com/content/dam/assets-zone2/de/de/docs/services/financial-advisory/2024/DP_Erfolgsfaktorenstudie_Cyber_Security_im_Mittelstand.pdf (accessed 8 April 2024).

Derakshan, N. and Eysenck, M.W. (2009), "Anxiety, processing efficiency, and cognitive performance", *European Psychologist*, Vol. 14 No. 2, pp. 168-176, doi: 10.1027/1016-9040.14.2.168.

Di Bella, L., Katsinis, A. and Lagüera-González, J. (2023), *Annual Report on European SMEs 2022/2023: SME Performance Review 2022/2023*, Publications Office of the European Union, available at: https://data.europa.eu/doi/10.2826/69827 (accessed 8 April 2024).

Dreißigacker, A., von Skarczinski, B. and Wollinger, G.R. (2021), *Cyberangriffe gegen Unternehmen in Deutschland – Ergebnisse einer Folgebefragung 2020*, Research Report No. 162, Criminological Research Institute of Lower Saxony e.V., available at: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_162.pdf (accessed 29 April 2022).

Efron, B. (1987), "Better bootstrap confidence intervals", *Journal of the American Statistical Association*, Vol. 82 No. 397, pp. 171-185, doi: 10.2307/2289144.

Ehling, P. (2013), "Corporate insurance and managers' and owners' risk aversion", *SSRN Electronic Journal*, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1343915 (accessed 26 March 2024).

EIOPA (2022), "SMEs access to insurance – the information gap and a way forward", available at: https://www.eiopa.europa.eu/system/files/2022-07/smes-access-to-insurance-irsg-position-paper.pdf (accessed 8 April 2024).

EIOPA (2023), "EIOPA launches survey on access to cyber insurance by SMEs", available at: https://www.eiopa.europa.eu/eiopa-launches-survey-access-cyber-insurance-smes-2023-09-20_en (accessed 8 April 2024).

Elhai, J.D., Levine, J.C. and Hall, B.J. (2017), "Anxiety about electronic data hacking – predictors and relations with digital privacy protection behavior", *Internet Research*, Vol. 27 No. 3, pp. 631-649, doi: 10.1108/IntR-03-2016-0070.

Eling, M. and Schnell, W. (2016), "What do we know about cyber risk and cyber risk insurance?", *The Journal of Risk Finance*, Vol. 17 No. 5, pp. 474-491, doi: 10.1108/JRF-09-2016-0122.

Eling, M. and Zhu, J. (2018), "Which insurers write cyber insurance? Evidence from the U.S. property and casualty insurance industry", *Journal of Insurance Issues*, Vol. 41 No. 1, pp. 22-56.

Eling, M., Schnell, W. and Sommerrock, F. (2016), "Ten key questions on cyber risk and cyber risk insurance", available at: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf (accessed 8 April 2024).

European Commission (2003), "Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises", *Official Journal of the European Union, L*, Vol. 124, pp. 36-41, 2003/361/EC.

European Parliament, Council of the European Union (2022), "Directive (EU) 2022/2557 of the European Parliament and of the council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC", *Official Journal of the European Union, L*, Vol. 333, pp. 164-198, PE/51/2022/REV/1.

European Union (2020), "User guide to the SME definition", available at: https://ec.europa.eu/docsroom/documents/42921 (accessed 15 April 2024).

Field, A. (2018), *Discovering Statistics Using IBM SPSS Statistics*, 5th ed., SAGE, Los Angeles.

Finlex (2023), "Finlex D&O and cyber market report 2023", available at: https://finlex.io/wp-content/uploads/2023/10/Finlex_DO-Cyber-Market-Report_2023.pdf (accessed 8 April 2024).

Frank, K.A. (2000), "Impact of a confounding variable on a regression coefficient", *Sociological Methods and Research*, Vol. 29 No. 2, pp. 147-194, doi: 10.1177/0049124100029002001.

Gatzert, N. and Schubert, M. (2022), "Cyber risk management in the US banking and insurance industry: a textual and empirical analysis of determinants and value", *Journal of Risk and Insurance*, Vol. 89 No. 3, pp. 725-763, doi: 10.1111/jori.12381.

Gennaioli, N. and Shleifer, A. (2010), "What comes to mind", *Quarterly Journal of Economics*, Vol. 125 No. 4, pp. 1399-1433, doi: 10.1162/qjec.2010.125.4.1399.

Gordon, L.A., Loeb, M.P. and Sohail, T. (2003), "A framework for using insurance for cyber-risk management", *Communications of the ACM*, Vol. 46 No. 3, pp. 81-85, doi: 10.1145/636772.636774.

Gothaer (2024), "Gothaer KMU-Studie zeigt: der Mittelstand investiert verstärkt in Cybersicherheit", available at: https://presse.gothaer.de/pressreleases/gothaer-kmu-studie-zeigt-der-mittelstand-investiert-verstaerkt-in-cybersicherheit-3314733 (accessed 16 April 2024).

Grace, M.F. and Rebello, M.J. (1993), "Financing and the demand for corporate insurance", *The Geneva Papers on Risk and Insurance Theory*, Vol. 18 No. 2, pp. 147-172, doi: 10.1007/BF01111467.

Greenwald, B.C. and Stiglitz, J.E. (1990), *Asymmetric Information and the New Theory of the Firm: Financial Constraints and Risk Behavior*, NBER Working Paper Series Working Paper [No. 3359], National Bureau of Economic Research, Cambridge, MA, doi: 10.3386/w3359.

Gupta, A. and Hammond, R. (2005), "Information systems security issues and decisions for small businesses – an empirical examination", *Information Management and Computer Security*, Vol. 13 No. 4, pp. 297-310, doi: 10.1108/09685220510614425.

Han, L.-M. (1996), "Managerial compensation and corporate demand for insurance", *The Journal of Risk and Insurance*, Vol. 63 No. 3, pp. 381-404, doi: 10.2307/253618.

HDI (2022), "Cyberangriffe und Schäden bei KMU – Ergebniss der HDI Cyber-Studie", available at: https://www.hdi.de/konzern/presse/cyberangriffe-und-schaeden-bei-kmu/ (accessed 29 April 2022).

HDI (2023), "HDI Cyberstudie 2023", available at: https://www.hdi-brandportal.com/share/hej29x7V (accessed 8 April 2024).

Heidt, M., Gerlach, J.P. and Buxmann, P. (2019), "Investigating the security divide between SME and large companies: how SME characteristics influence organizational IT security investments", *Information Systems Frontiers*, Vol. 21 No. 6, pp. 1285-1305, doi: 10.1007/s10796-019-09959-1.

Hiebl, M.R.W. (2013), "Risk aversion in family firms: what do we really know?", *The Journal of Risk Finance*, Vol. 14 No. 1, pp. 49-70, doi: 10.1108/15265941311288103.

Hiebl, M.R.W., Duller, C. and Neubauer, H. (2019), "Enterprise risk management in family firms: evidence from Austria and Germany", *The Journal of Risk Finance*, Vol. 20 No. 1, pp. 39-58, doi: 10.1108/JRF-01-2018-0003.

Hillebrand, A. and Henseler-Unger, I. (2018), "Aktuelle Lage der IT-Sicherheit in KMU: Wie kann man die Umsetzungslücke schließen?", *Datenschutz und Datensicherheit*, Vol. 42 No. 11, pp. 686-690, doi: 10.1007/s11623-018-1025-y.

Hiscox (2023), "Cyber Readiness Report 2023 – die wichtigsten Erkenntnisse", available at: https://hiscoxdedrupal.prod.acquia-sites.com/sites/default/files/documents/hiscox-cyber-readiness-report-2023-wichtigste-erkenntnisse.pdf (accessed 8 April 2024).

Hoppe, F., Gatzert, N. and Gruner, P. (2017), "Betriebsunterbrechungsversicherung bei kleinen und mittleren Unternehmen: Eine Empirische Analyse von Einflussfaktoren auf die Versicherungsentscheidung", *Zeitschrift für die gesamte Versicherungswissenschaft*, Vol. 106 No. 5, pp. 555-590, doi: 10.1007/s12297-017-0391-0.

Hoppe, F., Gatzert, N. and Gruner, P. (2021), "Cyber risk management in SMEs: insights from industry surveys", *The Journal of Risk Finance*, Vol. 22 Nos 3/4, pp. 240-260, doi: 10.1108/JRF-02-2020-0024.

Hoyt, R.E. and Khang, H. (2000), "On the demand for corporate property insurance", *The Journal of Risk and Insurance*, Vol. 67 No. 1, pp. 91-107, doi: 10.2307/253678.

Huaman, N., von Skarczinski, B., Wermke, D., Stransky, C., Acar, Y., Dreißigacker, A. and Fahl, S. (2021), "A large-scale interview study on information security in and attacks against Small and Medium-sized Enterprises", *paper presented at the 30th USENIX Security Symposium (USENIX Security '21)*, Vancouver, BC, 11 August – 13 August, available at: https://publications.cispa.saarland/3437/ (accessed 19 March 2024).

IfM Bonn (2021), "Mittelstand im Einzelnen – Unternehmensbestand", available at: https://www.ifm-bonn.org/statistiken/mittelstand-im-einzelnen/unternehmensbestand (accessed 15 March 2024).

IfM Bonn (2023), "Mittelstand im Einzelnen – Umsätze", available at: https://www.ifm-bonn.org/statistiken/mittelstand-im-einzelnen/umsaetze (accessed 16 August 2024).

Kellens, W., Terpestra, T. and De Maeyer, P. (2013), "Perceptions and communication of flood risks: a systematic review of empirical research", *Risk Analysis*, Vol. 33 No. 1, pp. 24-49, doi: 10.1111/j.1539-6924.2012.01844.x.

Kosub, T. (2015), "Components and challenges of integrated cyber risk management", *Zeitschrift für die gesamte Versicherungswissenschaft*, Vol. 104 No. 5, pp. 615-634, doi: 10.1007/s12297-015-0316-8.

KPMG (2021), "Future of small and medium business commercial insurance", available at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2021/02/future-of-small-and-medium-business-commercial-insurance.pdf (accessed 8 April 2024).

Krummaker, S. (2019), "Firm's demand for insurance: an explorative approach", *Risk Management and Insurance Review*, Vol. 22 No. 3, pp. 279-301, doi: 10.1111/rmir.12128.

Krummaker, S. and Graf von der Schulenburg, J.-M. (2008), "Die Versicherungsnachfrage von Unternehmen: Eine Empirische Untersuchung der Sachversicherungsnachfrage deutscher Unternehmen", *Zeitschrift für die gesamte Versicherungswissenschaft*, Vol. 97 No. 1, pp. 79-97, doi: 10.1007/s12297-008-0004-z.

Kshetri, N. (2018), "The economics of cyber-insurance", *IEEE IT Professional*, Vol. 20 No. 6, pp. 9-14, doi: 10.1109/MITP.2018.2874210.

Kshetri, N. (2020), "The evolution of cyber-insurance industry and market: an institutional analysis", *Telecommunications Policy*, Vol. 44 No. 8, 102007, doi: 10.1016/j.telpol.2020.102007.

Lawson, S.T., Yeo, S.K., Yu, H. and Greene, E. (2016), "The cyber-doom effect: the impact of fear appeals in the US cyber security debate", in Pissanidis, N., Rõigas, H. and Veenendaal, M. (Eds), *NATO CCD COE Publications*, Tallinn, pp. 65-80, doi: doi: 10.1109/CYCON.2016.7529427.

Lechner, P. and Gatzert, N. (2018), "Determinants and value of enterprise risk management: empirical evidence from Germany", *The European Journal of Finance*, Vol. 24 No. 10, pp. 867-887, doi: 10.1080/1351847X.2017.1347100.

Loewenstein, G.F., Weber, E.U., Hsee, C.K. and Welch, N. (2001), "Risk as feelings", *Psychological Bulletin*, Vol. 127 No. 2, pp. 267-286, doi: 10.1037/0033-2909.127.2.267.

MacMinn, R.D. (1987), "Insurance and corporate risk management", *The Journal of Risk and Insurance*, Vol. 54 No. 4, pp. 658-677, doi: 10.2307/253115.

Main, B.G.M. (1983), "Why large corporations purchase property/liability insurance", *California Management Review*, Vol. 25 No. 2, pp. 84-95, doi: 10.2307/41165008.

Marquardt, D.W. (1970), "Generalized inverses, ridge regression, biased linear estimation, and nonlinear estimation", *Technometrics*, Vol. 12 No. 3, pp. 591-612, doi: 10.2307/1267205.

Marsh and Microsoft (2019), "2019 Global cyber risk perception survey", available at: https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf?ranMID=43674&ranEAID=je6NUbpObpQ&ranSiteID=je6NUbpObpQ-hKju6aLwhLlzLY3qiyYJCA&epi=je6NUbpObpQ-hKju6aLwhLlzLY3qiyYJCA&irgwc=1 (accessed 8 April 2024).

Mason, C.H. and Perreault, W.D. (1991), "Collinearity, power, and interpretation of multiple regression analysis", *Journal of Marketing Research*, Vol. 28 No. 3, pp. 268-280, doi: 10.1177/002224379102800302.

Mayers, D. and Smith, C.W. (1982), "On the corporate demand for insurance", *Journal of Business*, Vol. 55 No. 2, pp. 281-296, doi: 10.1086/296165.

Mayers, D. and Smith, C.W. (1987), "Corporate insurance and the underinvestment problem", *The Journal of Risk and Insurance*, Vol. 54 No. 1, pp. 45-54, doi: 10.2307/252881.

Mayers, D. and Smith, C.W. (1990), "On the corporate demand for insurance: evidence from the reinsurance market", *Journal of Business*, Vol. 63 No. 1, pp. 19-40, doi: 10.1086/296481.

Meier, D.A. and Burda, D. (2020), "Cybersicherheit als Führungsaufgabe in Schweizer KMU", in Schellinger, J., Tokarski, K.O. and Kissling-Näf, I. (Eds), *Digitale Transformation und Unternehmensführung*, Springer Gabler, Wiesbaden, pp. 83-104.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S.K. (2013), "Cyber-risk decision models: to insure IT or not?", *Decision Support Systems*, Vol. 56 No. 1, pp. 11-26, doi: 10.1016/j.dss.2013.04.004.

MunichRe (2023), "Cyber insurance: risks and trends 2023", available at: https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html (accessed 8 April 2024).

Regan, L. and Hur, Y. (2007), "On the corporate demand for insurance: the case of Korean nonfinancial firms", *The Journal of Risk and Insurance*, Vol. 74 No. 4, pp. 829-850, doi: 10.1111/j.1539-6975.2007.00236.x.

Renaud, K. and Dupuis, M. (2019), "Cyber security fear appeals: unexpectedly complicated", in *New Security Paradigms Workshop (2019)*, ACM, available at: https://faculty.washington.edu/marcjd/articles/fear-appeals.pdf (accessed 8 April 2024), doi: 10.1145/3368860.3368864.

Renaud, K. and Ophoff, J. (2021), "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 1 No. 1, pp. 24-46, doi: 10.1108/OCJ-03-2021-0004.

Russo, J.E. and Schoemaker, P.J.H. (2018), "Overconfidence", in Augier, M. and Teece, D.J. (Eds), *The Palgrave Encyclopedia of Strategic Management*, Palgrave Macmillan UK, London, pp.1234-1246.

Salzberger, A. (2024), "Cyber risk awareness of German SMEs: an empirical study on the influence of biases and heuristics", *Zeitschrift für die gesamte Versicherungswissenschaft*, Vol. 113 No. 1, pp. 55-104, doi: 10.3790/zverswiss.2024.1430701.

Siegrist, M. and Gutscher, H. (2008), "Natural hazards and motivation for mitigation behavior: people cannot predict the affect evoked by a severe flood", *Risk Analysis*, Vol. 28 No. 3, pp. 771-778, doi: 10.1111/j.1539-6924.2008.01049.x.

Slovic, P. (1987), "Perception of risk", *Science*, Vol. 236 No. 4799, pp. 280-285, doi: 10.1126/science.3563507.

Slovic, P., Fischhoff, B., Lichtenstein, S., Corrigan, B. and Combs, B. (1977), "Preference for insuring against probable small losses: insurance implications", *The Journal of Risk and Insurance*, Vol. 44 No. 2, pp. 237-258, doi: 10.2307/252136.

Spitzer, R.L., Kroenke, K., Williams, J.B.W. and Löwe, B. (2006), "A brief measure for assessing generalized anxiety disorder: the GAD-7", *Archives of Internal Medicine*, Vol. 166 No. 10, pp. 1092-1097, doi: 10.1001/archinte.166.10.1092.

Stiefel, S. and Jeske, K.J. (2022), "Einflussfaktoren auf den Abschluss einer Versicherung – eine Analyse des Zusammenhangs zwischen Persönlichkeitseigenschaften und dem individuellen Risikomanagement", *Zeitschrift für die gesamte Versicherungswissenschaft*, Vol. 111 No. 4, pp. 433-463, doi: 10.1007/s12297-022-00538-z.

Sukumar, A., Mahdiraji, H.A. and Jafari-Sadeghi, V. (2023), "Cyber risk assessment in small and medium-sized enterprises: a multilevel decision-making approach for small e-tailors", *Risk Analysis*, Vol. 43 No. 10, pp. 2082-2098, doi: 10.1111/risa.14092.

Tabachnick, B.G. and Fidell, L.S. (2014), *Using Multivariate Statistics*, 6th ed., Pearson, Harlow.

Talesh, S.A. (2018), "Data breach, privacy, and cyber insurance: how insurance companies act as 'compliance managers' for businesses", *Law and Social Inquiry*, Vol. 43 No. 2, pp. 417-440, doi: 10.1111/lsi.12303.

Thomann, C., Pascalau, R. and Graf von der Schulenburg, J.-M. (2012), "Corporate management of highly dynamic risks: evidence from the demand for terrorism insurance in Germany", *The Geneva Risk and Insurance Review*, Vol. 37 No. 1, pp. 57-82, doi: 10.1057/grir.2011.3.

Tversky, A. and Kahneman, D. (1973), "Availability: a heuristic for judging frequency and probability", *Cognitive Psychology*, Vol. 5 No. 2, pp. 207-232, doi: 10.1016/0010-0285(73)90033-9.

Tversky, A. and Kahneman, D. (1974), "Judgement under uncertainty: heuristics and biases", *Science*, Vol. 185 No. 4157, pp. 1124-1131, doi: 10.1126/science.185.4157.1124.

Ulrich, P.S., Timmermann, A. and Frank, V. (2022), "Organizational aspects of cybersecurity in German family firms – do opportunities or risks predominate?", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 2 No. 1, pp. 21-40, doi: 10.1108/OCJ-03-2021-0010.

Vero (2021), "2021 SME insurance index", available at: https://www.vero.com.au/broker/news-insights/sme-insurance-index/tenth-sme-ins-index-report.html (accessed 8 April 2024).

von Skarczinski, B.S., Dreißigacker, A. and Teuteberg, F. (2022), "Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 2 No. 2, pp. 79-112, doi: 10.1108/OCJ-08-2021-0020.

Weinstein, N.D. (1980), "Unrealistic optimism about future life events", *Journal of Personality and Social Psychology*, Vol. 39 No. 5, pp. 806-820, doi: 10.1037/0022-3514.39.5.806.

Xu, R., Frank, K.A., Maroulis, S.J. and Rosenberg, J.M. (2019), "confound: command to quantify robustness of causal inferences", *STATA Journal*, Vol. 19 No. 3, pp. 523-550, doi: 10.1177/1536867X19874223.

Yamori, N. (1999), "An empirical investigation of the Japanese corporate demand for insurance", *The Journal of Risk and Insurance*, Vol. 66 No. 2, pp. 239-252, doi: 10.2307/253611.

Zängerle, D. and Schiereck, D. (2023), "Cyberrisiken – Vom Begriffswirrwarr zu einem einheitlichen Begriffsverständnis", *HMD. Praxis der Wirtschaftsinformatik*, Vol. 60 No. 1, pp. 214-229, doi: 10.1365/s40702-022-00888-3.

Supplementary material
The supplementary material for this article can be found online.

Corresponding author
Alina Salzberger can be contacted at: alina.salzberger@fau.de