Zeitschrift für die gesamte Versicherungswissenschaft, 113 (2024), 55 – 104
https://doi.org/10.3790/zverswiss.2024.1430701

Cyber Risk Awareness of German SMEs: An Empirical Study on the Influence of Biases and Heuristics

Alina Salzberger

Abstract

The number of successful cyberattacks against small and medium-sized enterprises (SMEs) is increasing steadily, while various studies already showed that especially SMEs often lack an appropriate awareness concerning their own cyber risk exposure. Therefore, the aim of this paper is to analyze the cyber risk perception of German SMEs and investigate the influence of biases and heuristics on German SMEs' cyber risk awareness. This is done based on a questionnaire survey among 1,540 owners and managers of German SMEs with up to 250 employees. The results show that perceived probabilities for cyberattacks against the own enterprise are significantly lower rated than for comparable organizations, which indicates the influence of an optimistic bias with respect to risk estimates. Additionally, perceived cyber risk also varies significantly depending on direct and indirect experience as well as the stated degree of confidence in one's own cyber risk management capabilities, indicating the presence of the availability heuristic and the overconfidence bias in cyber risk perceptions.

Zusammenfassung

Die Zahl erfolgreicher Cyberangriffe auf kleine und mittlere Unternehmen (KMU) steigt stetig an, während verschiedene Studien bereits gezeigt haben, dass insbesondere in KMU oft ein angemessenes Bewusstsein für die eigene Cyberrisikoexposition fehlt. Ziel dieser Arbeit ist es daher, die Cyber-Risikowahrnehmung deutscher KMU zu analysieren und den Einfluss von Verzerrungen und Heuristiken auf das Cyber-Risikobewusstsein deutscher KMU anhand einer Fragebogenerhebung mit 1.540 Inhabern und Führungskräften deutscher KMU mit bis zu 250 Mitarbeitern zu untersuchen. Die Ergebnisse zeigen, dass die wahrgenommene Wahrscheinlichkeit für Cyberangriffe auf das eigene Unternehmen signifikant niedriger eingeschätzt wird als für vergleichbare Unternehmen, was auf den Einfluss einer optimistischen Verzerrung in Bezug auf die Risikoeinschätzung hinweist. Darüber hinaus variiert das wahrgenommene Cyber-Risiko auch

Alina Salzberger
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)School of Business, Economics and Society
Lange Gasse 20, 90403 Nürnberg, Germany
alina.salzberger@fau.de.

Duncker & Humblot · Berlin

signifikant in Abhängigkeit von direkter und indirekter Erfahrung sowie dem angegebenen Grad des Vertrauens in die eigenen Cyber-Risikomanagement Fähigkeiten, was auf die Verfügbarkeitsheuristik und eine Verzerrung durch Selbstüberschätzung in der Cyber-Risikowahrnehmung hinweist.

Keywords: Cyber risk perception, cyber risk awareness, SMEs, Biases, Heuristics, Behavioral Influences

1. Introduction

The threat of successful cyberattacks against organizations is increasing steadily (Hiscox 2021 and 2022). Therefore, it is not surprising that in almost every risk report about the most important business risks in 2022 and 2023 cyber risks are listed in the Top 5 (e. g., Allianz Global Corporate & Specialty SE 2022 and 2023; Hiscox 2022). Despite the general increase of cyberthreats to organizations of all sizes, numerous studies also detected that especially the owners and responsible managers in small and medium-sized enterprises (SMEs)[1] in Germany often exhibit an inappropriate cyber risk perception (e. g., GDV 2021 and 2022a).

Besides other reasons for the low cyber risk perception of German SMEs, some authors assume the influence of biases and heuristics on cyber risk awareness (e. g., Hoppe et al. 2021). It is for this reason that behavioral influences on cyber risk awareness of German SMEs will be analyzed within this paper. This will be done based on a questionnaire survey among 1,540 German SME owners and managers, to investigate the influence of the availability heuristic, the overconfidence bias and the optimistic bias as these are most often supposed types of biases and heuristics in cyber risk perception according to the cyber literature.

To the best knowledge of the author, to date, no quantitative-empirical study exists that specifically focuses on the influence of biases and heuristics on the cyber risk perception of German SMEs. Closest to the present paper is the work of de Smidt and Botzen (2018) who already investigated organizational cyber

[1] To provide a basis for comparing the results on this topic within the European Union, the definition of the European Commission is followed. Accordingly, the term SME includes all enterprises that employ less than 250 persons and have an annual turnover less than 50 million Euros or an annual balance sheet total below 43 million Euros (European Union 2020, Article 2 of the annex to Recommendation 2003/361/EC). Thereby, the term SME can again be subdivided in the groups of micro- (up to 9 employees and up to 2 million Euros annual turnover or balance sheet total), small- (up to 49 employees and up to 10 million Euros annual turnover or balance sheet total), and medium-sized enterprises (up to 249 employees and up to 50 million Euros annual turnover or 43 million Euros balance sheet total).

risk perception (and cyber insurance demand) by the usage of a questionnaire for large organizations in the Netherlands. Thereby, a significant influence of the availability heuristic, the threshold level of concern, the degree of worry, and confidence in organizational risk management on cyber risk perception has been observed. Additionally, they observe a "not in my organization effect" (de Smidt and Botzen 2018, p. 255) which refers to the existence of an optimistic bias in cyber risk perceptions. However, there exist several differences between the current work and the paper from de Smidt and Botzen (2018). Firstly, de Smidt and Botzen (2018) analyze the cyber risk perception for large enterprises in the Netherlands while the current paper focuses on German SMEs. Furthermore, while de Smidt and Botzen (2018) submitted their questionnaire to professionals within the risk management and insurance department of large organizations, owners and managing directors of SMEs are asked in the present study, who are often responsible for (cyber) risk management decisions (Henschel 2003; Welter et al. 2015) but who might be also laypersons within this field. Finally, while de Smidt and Botzen (2018) focus on the influence of the availability heuristic and emotional factors, the current paper will extend the analysis by focusing on the availability heuristic, the optimistic bias and overconfidence, which are of great relevance with respect to probability perceptions for future cyberattacks.

Aside from de Smidt and Botzen (2018), also other authors assume the influence of biases and heuristics in the cyber risk context: For example, Hoppe et al. (2021) investigate within their review of 37 industry surveys the current cyber risk management status of SMEs. Among others, based on these studies, they find overconfident perceptions for actual cyber risk preparedness which could refer to an overconfidence bias. Moreover, Kamiya et al. (2021) formulated a model to analyze changes in cyber risk management and firm reputation after a successful cyberattack by the usage of data from 224 attacked firms of all sizes in the US. They find that organizations increase their investment in risk management after a successful cyberattack which could be explained, according to the authors, by the availability heuristic. Additionally, Rhee et al. (2012) already observed the existence of an optimistic bias in information security perception such that perceived likelihood for information security breaches within the own organization was rated as lower than for business partners. These results were achieved by the usage of a questionnaire among 204 MIS (Management Information System) executives from enterprises of all sizes in the US.

The present paper thus intends to close a gap in the existing literature by conducting a survey among German SMEs to study the influence of biases and heuristics on cyber risk awareness. The results generally confirm a low cyber risk perception of German SME owners and managers as already suggested by previous literature. While more realistic estimates were observable when asked re-

garding the cyber risk for a comparable organization, a low cyber risk perception was observed with respect to the own enterprise, indicating the influence of the optimistic bias. Additionally, also an influence of experience (direct and indirect), hence the availability heuristic, as well as the perceived degree of confidence in the organizational cyber risk preparedness seems to affect cyber risk perception in terms of perceived probability of future cyberattacks.

The paper is structured as follows. Section 2 reviews the literature on cyber risk awareness of SME owners and managers. The examined biases and heuristics will be explained and hypotheses will be developed. In Section 3, the research method, the data collection approach, and the survey design are presented. Section 4 comprises the results and discussion of the survey. Section 5 summarizes the findings.

2. Theoretical Background and Hypotheses Development

2.1 Theoretical Background on SMEs, Cyber Risks and Cyber Risk Perception

Not only in Germany, but also in Europe as a whole, SMEs constitute more than 99 % of all existing enterprises and realize more than 50 % of the European value creation (Institut für Mittelstandsforschung Bonn (IfM Bonn) 2022). Apart from their economic importance, SMEs face numerous challenges in today's business environment, as for example the scarcity of specialized employees, or the growing importance of digitization and thus an increasing risk of cybercrime (Icks and Kranzusch 2022). In the literature, the term cyber risk is defined in multiple ways. Following the suggestion of Hoppe et al. (2021), cyber risk will in the following be defined as the "risk emerging from the use of IT that compromises the confidentiality, availability or integrity of data or services" based on Eling and Schnell (2016, p. 483), as this definition includes all possible forms of cyberthreats and also those that are especially relevant for SMEs (Hoppe et al. 2021). Accordingly, the Criminological Research Institute of Lower Saxony (Kriminologisches Forschungsinstitut Niedersachsen; hereinafter referred to as Dreißigacker et al. 2021) discovered in their research report with 687 participating companies that German SMEs are most targeted by cyberattacks that affect the availability of data and services such as malware (including spyware), ransomware, phishing, and (D)DoS attacks (Dreißigacker et al. 2021).

Thereby, the threat of cyber risk events for German SMEs has not stopped its upward trend in the previous years. For instance, a survey by PwC with 400 organizations from the German midsize-sector revealed that the percentage of attacked SMEs almost doubled from 10 % in 2015 to 19 % in 2016 (Engemann et al. 2017) while the latest Cyber Readiness Report from Hiscox (2022) shows that 38.8 % of 546 surveyed German enterprises with up to 250 employees were

targeted by a cyberattack. Alongside the rising frequency of cyberattacks against SMEs, also the losses SMEs have to bear in case of an attack increased in the previous years. Hiscox detects in the Cyber Readiness Report from 2021 over all analyzed countries that, compared to larger firms, SMEs face higher losses relative to business size with median costs of $8,000 for enterprises with less than ten employees for each cyber incident (Hiscox 2021). Thereby, the German industry ranks among the most affected within the European Union with median costs per cyberattack of $21,000 in 2021 (Hiscox 2022) and total losses in the year 2020 amounting to $47.9 million from cyberattacks (Hiscox 2021). It is evident that not only the probability, but also the financial impacts of cyberattacks steadily increase for German SMEs.

To address their cyber risk exposure, organizations need to implement an effective cyber risk management process that should include the fundamental steps of context establishment, risk assessment and risk treatment (see, e. g., ISO 31000 2018) whereby the probability of cyberattack occurrence or the expected losses of cyber incidents could either be reduced (e. g., by investing in IT security tools) or existent cyber risk exposures could be transferred to a third party (e. g., by entering into a cyber insurance contract) (Hoppe et al. 2021). However, to establish a suitable cyber risk management process, an appropriate cyber risk perception constitutes an important prerequisite (Gatzert and Schubert 2022), which is often lacking in German SMEs.

As an example, Hoppe et al. (2021) observe based on their review of various industry studies that cyber risk awareness, cyber risk culture and cyber risk management seem to be often inappropriately established in SMEs such that IT security strategies are often lacking and demand for corporate cyber insurance in Germany is only slowly increasing (Hoppe et al. 2021). Similar findings are also reported by Ulrich et al. (2022) from their quantitative study with 184 German family-firms. They find, analogously to Hoppe et al. (2021), that German family businesses often lack appropriate cyber risk awareness. Additionally, Dreißigacker et al. (2021) provide a two time-based survey with computer assisted telephone interviews in 2019 (with 5,000 total responses) and a follow-up web-based survey in 2020 (with 687 total responses) concerning cyberattacks against German enterprises. They observe that cyber risk perception in German enterprises is generally low although an increase from 2019 to 2020 is noticeable. However, especially larger firms with more than 500 employees perceive the threat of targeted cyberattacks as higher than smaller or medium-sized enterprises (Dreißigacker et al. 2021). While there are already various studies addressing the challenges and deficiencies in (cyber) risk awareness, (cyber) risk management and the consequent (cyber) risk culture of SMEs (e. g., Falkner and Hiebl 2015; Gupta and Hammond 2005; Kuusisto and Ilvonen 2003; Santos-Olmo et al. 2016; Valli et al. 2014), none of them analyzed behavioral influences on cyber risk perception empirically so far.

In general, risk perception can be defined in various ways. Bubeck et al. (2012) define perceived risk as the combined measurement of perceived probability and estimated impact for certain events and also Kellens et al. (2013) observe within their meta-study about empirical research on flooding risk perception that the perceived impact and perceived probability of risk occurrence is used most frequently in non-theoretical risk perception analyses[2]. Besides differentiating between estimations for probability and consequences of risk events, individuals often unconsciously differentiate between a personal-level risk and a societal-level risk judgement (Tyler and Cook 1984). This differentiation is especially observable for probability estimations of negative events and often leads to the biased opinion that the own probability for the occurrence of a negative event is lower than for comparable others, also known as an optimistic bias (Weinstein 1989). In general, there exist multiple biases that can lead to predictable and systematic under-or overestimations of risks. They result out of heuristics, so-called mental shortcuts of intuitive thinking (Kahneman 2013) that individuals use unconsciously to "reduce the complex tasks of assessing probabilities and predicting values to simpler judgmental operations" (Tversky and Kahneman 1974, p. 1124). Correspondingly, cyber risk perception and estimations of German SMEs could be influenced by biases and heuristics, as assessing cyber risks is complex due to various types of cyber risk events that can occur either as high-probability/low-impact risks but also as low-probability/high-impact risks. Additionally, cyber risks are dynamic, intangible, and complexly interlinked across organizations and country-borders (Ashby et al. 2018; Eling and Schnell 2016; de Smidt and Botzen 2018).

Generally, various authors (e. g. Busenitz and Barney 1997; Shepherd et al. 2015) observed that biases and heuristics arise more often in decision-making of smaller enterprises compared to larger organizations. This may be attributed to the specific characteristics of SMEs, as they often rely on less sophisticated and formalized systems and tools for assessing and making decisions than larger organizations (López and Hiebl 2015; Quinn 2011). As biases and heuristics especially arise within subjective thinking, it is important to note that Falkner and Hiebl (2015) found in their systematic literature review about current risk management in SMEs that the subjective risk behavior of the owner often influences organizational risk management. Additionally, SME owners and managers often need to operate despite existing time and resource constraints (Aragón-Sánchez and Sánchez-Marín 2005; López and Hiebl 2015), so that especially self-perceived core processes are pursued while for example the integration of an appro-

[2] In total 57 studies are analyzed that investigated flood risk perception. Most frequently risk perception is measured by the determinant "perceived probability of flood occurrence" (18 times) and "perceived impact" (23 times), followed by the determinants of "awareness" (14 times) and "perceived worry" (11 times).

priate risk management approach is often postponed (Hoppe et al. 2021). In line with this, Wolf et al. (2018) found in their study on decision-making in Swiss SMEs that especially those decisions that are not perceived as strategically important are often decided by SME decision-makers on an intuitive and quick basis, while Ulrich et al. (2022) observed for German family-firms that cybersecurity is perceived only as slightly strategically relevant for most of the asked enterprises.

Most frequently mentioned as potential behavioral influences on cyber risk perception are the availability heuristic, the overconfidence bias and the optimistic bias. Accordingly, due to an availability bias the perceived probability of a cyberattack could depend on the existence of direct or indirect experience of cyberattacks (Tversky and Kahneman 1973 and 1974), while the overconfidence bias could cause an overestimation of own knowledge and skills in cyber risk assessment (Russo and Schoemaker 2018) which could lead to biased perceptions of organizational cyber risk preparedness and to a lower cyber risk awareness (Hoppe et al. 2021). Furthermore, differences in cyber risk perceptions for the own enterprise and comparable organizations (e. g., GDV 2022a) may indicate the influence of an optimistic bias in cyber risk perception.

2.2 Hypotheses Development

In what follows, biases and heuristics are introduced that might have an influence on cyber risk perception of German SMEs as the basis for the hypotheses development.

Availability Heuristic

People use the availability heuristic unconsciously to assess the frequency or probability of an event by the ease with which similar instances can be retrieved or constructed in mind (Tversky and Kahneman 1973 and 1974). Instead of assessing a complex target estimation about the frequency or probability of an event by the usage of full information and statistical rules, individuals unconsciously substitute it with an easier, so-called heuristic question (Kahneman, 2013) for which an answer can be accessed more easily and effortless than for the original question (Kahneman 2013). Thereby, probabilities and frequencies are unconsciously estimated by the easiness and fluency of retrieving or imagining similar events in memory (Kahneman 2013; Tversky and Kahneman 1973). Personal experience, both direct experience of a salient negative event but also indirect experience (for example media coverage of a negative event) can drive mental availability and consequently increase risk perception (e. g., Tversky and Kahneman 1973 and 1974).

The influence of the availability heuristic on risk perception has already been shown for various insurance settings, e. g., by Botzen et al. (2015) in the context of flood risks and by Thomann et al. (2012) with respect to terrorism insurance. For cyber risks, de Smidt and Botzen (2018) found, based on their questionnaire with managers of large organizations, that the perceived probability of a cyberattack is significantly influenced by the personal experience of cyberattacks, which is in line with the initial definition of the availability heuristic of Tversky and Kahneman (1973 and 1974). Also, Jalali et al. (2019) and Kamiya et al. (2021) assume the availability heuristic to affect cyber risk perception. Moreover, observations from the GDV (2020) indicate, that the cyber risk perception of SME owners and managers could be influenced by availability. According to their SME poll from 2020, 35 % of those enterprises already harmed by a cyber incident perceive great personal danger of future cyber events, whereas only 8 % of SMEs without direct experience perceive the cyberthreat for their enterprise as high (GDV 2020). Therefore, H1 is assumed as follows:

H1: An SME owner or manager who has already experienced a cyberattack is more likely to exhibit a higher perceived probability of a cyberattack occurrence than an SME owner or manager without direct experience.

Additionally, indirect experience through public information or media coverage of successful cyberattacks is assumed to increase the cognitive availability for cyber risk events and hence to influence cyber risk perception (de Smidt and Botzen 2018). However, while de Smidt and Botzen (2018) have already observed a positive relation between cyber risk perception and indirect experience among managers in large organizations who discussed the topic of cyber risks within the organization, searched for additional information on the internet, or heard about cyberattacks in the media, the influence of public information on SMEs' cyber risk perception is still unclear. Although media coverage of cyberattacks seems high, most reports focus mainly on cyberattacks against large corporations and governments (Kostyuk and Wayne 2021) which might not have an influence on the cyber risk perception of German SMEs due to a low degree of identifiability with published cyber incidents of larger organizations. This is also in line with findings of the SME survey by the GDV (2022b), where 62 % of SME decision-makers who rate organizational cyber risk as low believe that the own enterprise is too small to be targeted by cyberattacks. Furthermore, as German SMEs are often not subject to disclosure requirements, many cyberattacks against SMEs might remain unpublished so that a low cyber risk perception might be observable. Therefore, H2 is assumed as follows:

H2: An SME owner or manager who has more often heard/read about a successful cyberattack against another SME is more likely to exhibit a higher perceived probability of a cyberattack occurrence than SME owners or managers without or low indirect experience.

Overconfidence Bias

The overconfidence bias describes the tendency of individuals and organizations to frequently overestimate their own knowledge, skills, forecasting abilities and judgment qualities (Russo and Schoemaker 2018). Thereby, overconfidence can include the tendency of individuals and organizations to falsely perceive own skills and abilities as being better than they actually are, leading to an above average estimation of one's own performance in comparison to others and hence wrong estimates concerning likelihoods or other quantitative assessments (Russo and Schoemaker 2018). Consequently, due to overestimating own abilities, the subjective probability estimates of a potential loss could be underestimated (Bregu 2022).

The influence of the overconfidence bias on insurance decision-making has already been well explored (see, e. g., Bregu 2022, Sandroni and Squintani 2007). For cyber risk perception, de Smidt and Botzen (2018) have already detected an overall faith in one's own competencies, based on their questionnaire about cyber risk perception in large organizations. They observe that managers who display high confidence in own and organizational cybersecurity capabilities to prevent, mitigate, or deal with cyberattacks are only slightly concerned about the occurrence of cyber incidents in their own organization. Thus, a negative relation between trust in the cyber risk management competencies of the own organization and cyber risk perception (more specifically the perceived probability for cyberattacks) has been observed.

In line with these findings, Hoppe et al. (2021) detected a systematic deviation from actual preparedness for cyberattacks and the perceived security-level among SMEs. Based on 37 reviewed industry surveys from 2016 to 2020, Hoppe et al. (2021) find that many SMEs perceive themselves to be well prepared for a cyberattack and believe in their ability to handle a cyber event quickly after occurrence, although a relevant proportion of them already lacks basic knowledge about cybersecurity issues and hence shows overconfident perceptions in own skills and abilities. Furthermore, the SME study 2020 by the GDV (2020) reveals that 81 % of 300 participating German SME decision-makers perceived their enterprise as fully secured against cyberattacks, while the assessment of cyber risk preparedness through the analytical tool "cysmo" showed that 70 % of 1,019 examined SME homepages included external unintended content and for 25 %, the mailservers demonstrated unsafe and obsolete coding techniques. Thus, the actual level of cyber risk preparedness in SMEs was lower than perceived by SME decision-makers themselves. Therefore, H3 is formulated as follows:

H3: An SME owner or manager with a higher degree of confidence in organizational cyber risk preparedness (including knowledge and competencies concerning cyber risk management) is more likely to exhibit a lower

perceived probability of a cyberattack occurrence than an SME owner or manager with a lower degree of confidence.

Optimistic Bias

The optimistic bias describes the tendency of individuals to believe in own invulnerability and therefore underestimate the likelihood of negative events (Weinstein 1980), such as a successful cyberattack occurring in the future within the own organization. Overoptimism can either be identified indirectly, if individuals expect their own probability of certain negative outcomes and severe events as lower than for comparable others, or directly, by asking individuals to rank their own vulnerability compared to others (Helweg-Larsen and Shepperd 2001; Weinstein and Klein 1996). This deviation in probability judgements arises due to two different levels of risk judgements in mind, namely the personal-level risk judgement and the societal-level risk judgment (Tyler and Cook 1984).

The adverse consequences of the optimistic bias on organizational cyber risk perception have been shown by, e. g., de Smidt and Botzen (2018), who found that 84 % of managers from large organizations participating in their study generally believe that a cyberattack could be possible, but 60.6 % also expressed statements such as "not in my organization" and "it does happen but not here" (de Smidt and Botzen 2018, p. 255). Hence, many entrepreneurs perceive the vulnerability of their own enterprise with respect to cyberattacks as low and thus believe in an immunity regarding cyber incidents (de Smidt and Botzen 2018). Similarly, Rhee et al. (2012) observe within their survey about information security perception that the participating MIS (Management Information System) executives in U.S. organizations, on average, perceive the information security risk-exposure of their own firm to be lower than that of another average company. For SMEs, the cybersecurity survey of the GDV (2022b) shows that although many SME decision-makers (76 % of 300 participating SME decision-makers) rate cyber risk as being high for German SMEs in general, they perceive their personal risk of cyberattacks as low (only 34 % perceive the threat for the own organization as high). Therefore, H4 is formulated as follows:

H4: SME owners and managers are prone to the optimistic bias in their cyber risk perception and hence perceive the probability of cyberattacks occurring in their own organization as lower than for another comparable SME.

3. Research Method, Data Sampling, and Survey Design

3.1 Research Method and Data Sampling

To test the previously derived hypotheses, a large-scale and standardized online questionnaire in German was used that included open and closed questions. Prior to the field phase, a pre-test was conducted with test persons. Thereby, the questionnaire was sent to seven independent research assistants in order to check the general understanding, spelling as well as quantitative research settings and quality. Additionally, the questionnaire was also sent to a managing director of a small service-enterprise to check the suitability of the questionnaire for the targeted responding group of SME managers and owners.

As the investigated hypotheses focus on German SMEs, a large database accessible via the university network was used to search for enterprises that fulfill the SME definition of the European Commission. Accordingly, search results were restricted to German companies with less than 250 employees and an annual revenue of less than 50 million Euros. As the cyber risk perception of the owner or managing board is of special interest in this paper, an evaluation of the cyber risk perception of the owners or responsible managers was necessary. However, for most enterprises only global firm e-mail addresses as "info@firm.de" were available such that an instruction to forward the invitation for the online survey to the intended target group (owner, managing board or the responsible IT or risk management department) was included in the e-mail invitation. As it could not be guaranteed that all survey invitations actually reached the intended target group of respondents, a question was included in the survey that asked about the current company function of the responding person. The used online questionnaire tool "Unipark" further ensured that every addressed respondent could answer the questionnaire only once. In order to achieve a higher response rate, the responding organizations were offered the opportunity to receive the results of their questionnaire in comparison with the aggregated results and further information about potential biases in cyber risk perception.

In total, 430,439 companies were identified that fulfilled the definition of a German SME and were contacted by e-mail between August and September 2022. Thereby, 5,638 SMEs could verifiably be reached as they opened the link to the online questionnaire. In total, 1,828 companies completed the survey (completion rate of 32.42 %). From the gained data, 165 datasets were removed as they did not fulfill the SME definition from the European Commission and hence constituted large organizations. Further, 97 datasets were excluded from analysis as the responding person did not belong to the defined target group (SME owners, members of the managing board, or managers that are responsible for the IT or risk-management department) and 26 additional datasets were

removed due to low answering accuracy of the respondents. Hence, in total 1,540 datasets were analyzed.

To test for non-response bias according to Armstrong and Overton (1977), an extrapolation method for time trends was used, were the responses of first-third respondents and last-third respondents were compared by the usage of t-tests and Mann-Whitney U-tests for the relevant variables (in accordance with the procedure of Gupta and Hammond 2004; Ulrich et al. 2022) regarding frequency and probability estimates of cyberattacks against the own and other enterprises. Thereby, no significant differences in the responses of the two subgroups could be observed that would indicate a non-response bias. The data was evaluated using Microsoft Excel and SPSS.

3.2 Survey Design

Generally, in the questionnaire a focus was laid on malware-, phishing-, (D)DoS-, and ransomware-attacks as these were most frequently stated to occur in German SMES according to the survey of Dreißigacker et al. (2021). For all four kinds of cyberattacks, examples or possible attack-situations were provided in the questionnaire.[3]

The questionnaire (see Appendix A; originally sent in German to the respondents but translated in English for the following analysis) started by asking about the degree of indirect experience with malware-, phishing-, (D)DoS-, and ransomware-attacks. Respondents were asked if they already heard or read about malware- (IndExp_Malware), phishing- (IndExp_Phishing), (D)DoS- (IndExp_DoS), or ransomware-attacks (IndExp_Ransomware) against compa-

[3] The term *malware-attack* was explained by viruses and spyware spreading in computer systems.

Phishing-attacks were explained by an illustrative situation: "Imagine you will receive an e-mail with a harmful link or attachment. The e-mail appears to be trustworthy at first glance, for example, it mimics a known or trustworthy sender. However, clicking on the included link or attachment will download harmful software". *(D)DoS-attacks* were explained as follows: "An attacker 'floods' the network connections responsible for external data exchange of an IT system with a large number of requests, thereby overloading them. When the number of requests exceeds the capacity limit, the system slows down or completely collapses, making websites, e-mail functions or online shops inaccessible. For a (D)DoS attack, it is not necessary to penetrate secured IT systems. While DoS attacks originate from a single source (such as a computer or network), DDoS attacks are indirectly executed through a widespread botnet (group of several computers or networks)." Additionally, *ransomware-attacks* were explained by the following situation: "Criminals gain access to your internal systems through malware and encrypt personal files and data. The users have no access to their data until they pay the criminals a ransom. Afterwards, the data is fully or partially decrypted."

rable organizations[4] on a 7-point Likert-scale (1 = never so far, 7 = very frequently) in order to test for an influence of indirect experience on cyber risk perception (H2).

Afterwards, questions about the cyber risk perception were asked. Although, as mentioned earlier, risk perception can be measured by the two variables of perceived probability and estimated impact, in this paper a focus was laid on perceived probability, as the availability bias and the opimistic bias per definition only influence probability estimates, while for the overconfidence bias de Smidt and Botzen (2018) could only detect an influence on probability estimates. Therefore, the respondents were asked about their perceived probability of a successful[5] malware- (Prob_Malware_Own), phishing- (Prob_Phishing_Own), (D)DoS- (Prob_DoS_Own), or ransomware-attack (Prob_Ransomware_Own) within the next year against their own organization on a scale from 0 % to 100 %. As questions that include a percentage scale of estimated probabilities can lead to biased answers[6], estimated frequencies were asked as well to serve as a robustness check. Analogously to probability estimates, frequency estimates were asked for malware- (Freq_Malware_Own), phishing- (Freq_Phishing_Own), (D)DoS (Freq_DoS_Own), and ransomware-attacks (Freq_Ransomware_Own) by following the approach of de Smidt and Botzen (2018), thereby increasing the answering possibilities to a 7-point scale (1 = never, 2 = not very often, once every 50 years, 3 = seldomly, once every 10 years, 4 = occasionally, once every 5 years, 5 = often, once every 2 years, 6 = very often, every year, 7 = several times in a year).

To test whether cyber risk perception is influenced by the optimistic bias (H4), analogous questions were asked for estimates of a cyberattack occurrence for comparable organizations on a percentage (Prob_Malware_Others, Prob_Phishing_Others, Prob_DoS_Others, Prob_Ransomware_Others) and frequency scale (Freq_Malware_Others, Freq_Phishing_Others, Freq_DoS_Others, Freq_Ransomware_Others). This allows testing for the optimistic bias by using the indirect method in accordance with Helweg-Larsen and Shepperd (2001). Additionally, respondents were asked to rate their own risk of a successful cyberattack relative to a successful cyberattack against a comparable organization on a 7-point scale (1 = is much lower, 4 = is as high, 7 = is much higher).

[4] Comparable organizations were defined as "organizations of the same size and industry" as the responding enterprise.

[5] A successful cyberattack was defined in hereby analysis as "any attack leading to financial damages for the attacked organization".

[6] As an example, according to Schapira et al. (2004), questions that ask for probability estimates can lead to anchor-effects so that respondents more likely chose one of the anchor points of 0 %, 50 %, and 100 % when using a probability scale. Additionally, Fischhoff and Bruine de Bruin (1999) show that respondents often equate the probability estimate of "50 %" with the answering-phrase "I don't know".

To test the influence of the overconfidence bias on cyber risk perception (H3), questions about the own and organizational cyber risk knowledge and cyber risk management capabilities were included. Questions about the general preparedness concerning cyberattacks (Conf_Prev_General, Conf_React_General) were measured on a 6-point Likert-scale and questions about own knowledge and competencies concerning cyber risk (Knowl_Own, Compet_Prev_Own, Compet_React_Own), as well as questions about the employees' cyber risk knowledge and competencies (Knowl_Empl, Compet_Prev_Empl, Compet_React_Empl), were asked on basis of a 7-point Likert-scale (1= very low, 7 = very high). Afterwards, the eight items were combined to a single construct of "Mean_Conf" (Conbach's Alpha = 0.892)[7]. To verify whether the stated degree of confidence aligns with the actual preparedness, the respondents were asked if the organization already established a cyber incidence response plan (1 = yes, 2 = no, 3 = I am not familiar with this term, 4 = I don't know) and whether the organization performs cybersecurity trainings for the entire organization (1= no, 2 = yes, irregularly, 3 = yes, regularly, 4 = permanent online-trainings).

Furthermore, to test if cyber risk perception was potentially influenced by direct experience (H1), the approach of de Smidt and Botzen (2018) was applied and direct experience with cyberattacks (DirExp) was measured on a binary level (0 = no and 1 = yes) for different attack-locations. As direct experience is supposed to influence risk perception only for a short timeframe (see, e. g., Kahneman 2013), the respondents who were already targeted by a cyberattack were also asked when the cyber incident happened and if the cyberattack also led to financial losses (hence if the cyberattack was successful and therefore perceived as salient).

Finally, questions to check whether the firm characteristics are in line with the SME definition of the European Commission (hence, the number of employees, the annual sales, and the balance sheet total), questions about the enterprise (industry-sector, company function of the respondent) as well as socio-demographic questions about the respondent (age, sex) were integrated. Additionally, the respondents had to rate their answering accuracy on a 7-point Likert-scale.

[7] First, Likert-scales of general preparedness were transformed to a 7-point Likert-scale. Afterwards, the mean value was calculated for the eight single items, generating the variable "Mean_Conf". Cronbach's Alpha of 0.892 shows a high internal consistency of the used construct according to Taber (2018).

4. Results and Discussion

4.1 Descriptive Statistics

Sample Characteristics

Starting with the sample characteristics, according to the definition of SMEs by the European Commission as laid out in the introduction, the final sample (N = 1,540) consists of 436 (28.31 %) microenterprises, 751 (48.77 %) small enterprises and 353 (22.92 %) medium-sized enterprises (see Table B.1 in the Appendix for further details). Concerning the different industry-sectors of the analyzed sample, a high heterogeneity is observable. 14.35 % of the responding enterprises operate in the manufacturing industry (N = 221), followed by 13.06 % operating in the information and communication branch (N = 201) and other economic sectors (N = 201), while 10.45 % are active in the trading business (N = 161). A complete list that follows the classification of the business sectors according to the German Federal Bureau of Statistics is provided in Table B.2 in the Appendix. With respect to the functions of the respondents, multiple selections were possible. Of the total 1,540 respondents, 1,077 (69.94 %) are members of the management board and 662 (42.99 %) are responsible for IT, while 181 respondents (11.75 %) are working in risk management (see Table B.3 in the Appendix). Additionally, the sample consists of 83.51 % (N = 1,286) male and 13.51 % female (N = 208) respondents (2.98 % without information), and the average age of respondents is 49.35 years (N = 1,419).

Cyber Risk Perception

Table B.4 and Table B.5 in the Appendix show the estimated probabilities and frequencies of the SME owners and managers, respectively, of a successful cyberattack for their own enterprise versus a comparable organization. Overall, the mean estimated probability of the own firm suffering a cyberattack within the next year was about 37.52 % (Freq_CyberAttack_Own = 3.63, which indicates that respondents estimate a successful cyberattack to happen to them every 10 to 5 years). The perceived probability was highest for phishing-attacks (45.71 %; 4.33), followed by malware- (41.52 %; 3.97), ransomware- (34.51 %; 3.32) and (D)DoS-attacks (28.35 %; 2.91). Tables B.4 and B.5 in the Appendix further show that although the ranking of the probabilities of different cyberattacks is identical for a comparable organization, they are generally higher for all types of cyberattacks than for the own enterprise, which already indicates the potential influence of an optimistic bias.

Respondents were also asked directly to rank their own vulnerability concerning cyberattacks for their own organization against a comparable enterprise (Ta-

ble B.6 in the Appendix). With the direct method for analyzing the optimistic bias (Helweg-Larsen and Shepperd 2001), most respondents (52.85 %) indicated that their threat-level is lower than the one of comparable organizations, such that an optimistic bias seems to be detected also with the direct method of assessing an optimsitic bias in cyber risk perceptions.

Direct and Indirect Experience

Direct experience has been analyzed by asking the respondents if they already were affected by a cyberattack either within their own organization, their previous work, or privately. In total 69.28 % (1,067 from N = 1,540) confirmed to already have experienced a cyberattack, out of which 711 respondents indicated that a cyberattack already happened within the own enterprise (see Table B.7 in the Appendix).

In order to account for the diminishing influence of direct experience as time passes, the SME owners and managers were also asked about when the cyberattack happened. More than half of the respondents (57.36 % of N = 1,067) indicate that a cyberattack happened more than one year ago, while 40.58 % (of N = 1,067) experienced a cyberattack within the last twelve months (see Table B.8 in the Appendix). Additionally, as direct experience is supposed to influence cyber risk perception especially if the cyberattack constitutes a salient event, respondents were also asked if the cyberattack they experienced was successful or not, i. e. if the attack led to financial losses or could be defended successfully. Most respondents (64.85 % of N = 1,067) with direct experience stated that they could successfully defend the cyberattack (see Table B.9 in the Appendix).

Besides direct experience, also the degree of indirect experience was measured in order to analyze a potential influence on cyber risk perception. As can be seen in Table B.10 in the Appendix, the mean values for indirect experience for the different cyberattacks are quite similar, ranging from 3.44 to 4.93 on a 7-point Likert-scale (1 = never, 7 = very frequently) although here the same ranking of different cyberattacks is observable as for probability and frequency estimations. Hence, SME owners and managers have heard or read most frequently of phishing-attacks, followed by malware-, ransomware- and (D)DoS-attacks against comparable organizations.

Degree of Confidence

As described previously, the degree of confidence was measured by eight different items[8] that were aggregated to a single variable of general confidence "Mean_Conf" (Cronbach's Alpha = 0.892). Thereby, overall mean confidence is about 4.52 (SD = 1.17, N = 1,540) such that perceptions for overall confidence are in the upper half (scales for Mean_Conf ranging from 1 to 7). Table B.11 in the Appendix summarizes the descriptive values for the eight single items and the aggregated variable.

As can be seen in Table B.11 in the Appendix, the confidence regarding the preparedness in terms of general prevention and reaction in case of a cyberattack is generally high and rated in the upper half of the 6-Point Likert-scale (Conf_Prev_General = 4.36 and Conf_React_General = 4.14). However, when asking the respondents if an incident response plan has already been prepared within the enterprise, only 25.71 % confirm this, while 57.21 % have not developed such a plan yet and 15.65 % do not know the meaning of this term (see Table B.12 in the Appendix).

Additionally, it is observable that own knowledge and competencies concerning cyber risk management in terms of prevention and reaction by the respondents is perceived as higher than the knowledge and competencies of the other employees with most evaluations of knowledge and competencies ranked in the upper half of the 7-point Likert-scale (see Table B.11 in the Appendix), while in 612 (39.74 %) of the 1,540 enterprises no cybersecurity training has taken place so far (see Table B.13 in the Appendix). Hence, as suggested in hypothesis H3, an overconfident perception in organizational cyber risk preparedness, including estimations about the own and employees' knowledge in cyber risks as well as competencies in cyber risk management within the own enterprise could exist. At least, out of the 868 enterprises in which cybersecurity trainings were already performed, 739 (47.99 % of the total sample) SME owners and managers indicate that they also participated in the trainings.

[8] Respondents were asked about the general preparedness of the enterprise concerning 1) cyberattack prevention-measures (Conf_Prev_General) and 2) quick reaction in case of a cyberattack (Conf_React_General) by asking about their agreement about appropriate prepardness on basis of a 6-point Likert-scale. Questions about 3) own knowledge (Knowl_Own) and 4) competencies concerning cyber risk prevention (Compet_Prev_Own) and 5) reaction in case of a cyberattack (Compet_React_Own) as well as questions about the 6) employees cyber risk knowledge (Knowl_Empl) and 7) competencies concerning cyber risk prevention (Compet_Prev_Empl) and 8) reaction in case of a cyberattack (Compet_React_Empl) were asked on basis of a 7-point Likert-scale (1 = very low, 7 = very high).

4.2 Univariate and bivariate Statistics

To analyze the hypotheses concerning the influence of biases and heuristics on cyber risk perception (H1, H2, H3, H4), univariate and bivariate statistics were derived. Statistical tests were not only performed for the mean of perceived probability for overall cyberattacks, but also for probability estimates for malware, phishing-, (D)DoS-, and ransomware-attacks individually to uncover potential differences depending on the kind of cyberattacks. Additionally, the hypotheses were also analyzed for expected frequency estimates in order to perform a robustness check.

To test if SME owners and managers with direct experience show a higher perceived probability of a cyberattack than SME owners or managers without direct experience (H1), subgroups were composed. Although the cyberattacks occurred at least one year ago for most respondents in the sample, and although most respondents indicated a low salience due to successfully defending the cyberattack, there are substantial differences in cyber risk perceptions for the two subgroups of "direct experience" and "no direct experience" for all four kinds of cyberattacks (e. g., Prob_Cyberattack_Own_DirectExp = 40.13 %; Prob_Cyberattack_Own_NoDirExp = 31.63 %, $p < 0.001$) as shown in Table 1. Cohen's d varies between 0.219 and 0.311, indicating a small effect[9] of direct experience on cyber risk perception on a probability scale. The differences in cyber risk perception are thereby not only significant for all probability estimates, but also for estimates on a frequency scale as shown in Table 1 (e. g., Freq_Cyberattack_Own_DirectExp = 3.85; Freq_Cyberattack_Own_NoDirExp = 3.13, $p < 0.001$), which supports hypothesis H1 and thus shows the influence of the availability heuristic on cyber risk perception.

Additionally, it is observable that frequency and probability estimates are always higher for SME owners and manger that were attacked recently (within the last year) compared to respondents that were targeted more than one year ago. However, while for frequency estimates significant differences are observable, the differences in probability estimates are not significant except for phishing-attacks (see Table B.14 and B.15 in the Appendix). Moreover, availability is supposed to be driven by the salience of a cyberattack (here measured by the success of a cyberattack, hence if financial losses were caused). Therefore, the subgroups of SME owners and managers that experienced a successful cyberattack were compared to those who defended the cyberattack successfully (see right part of Table B.14 and Table B.15 in the Appendix). It can be seen that probability estimates are rated significantly higher for most cyberattacks by

[9] Small effect size from d = 0.2, medium effect size from d = 0.5 and large effect from d = 0.8 (Cohen 1992).

SME owners and manager who had to handle a successful attack while for frequency estimates the differences are not significant.

Table 1

Perceived probability and perceived frequency of the respective cyberattacks for the own enterprise depending on direct experience of a cyberattack

Prob_Own	**DirExp_Yes**		**DirExp_No**		**Sign.**	**Cohen's d**
	N	Mean (%)	N	Mean (%)	(t-tests)	
Prob_Cyberattack	1,067	40.13	473	31.63	< 0.001***	0.311
Prob_Phishing	1,067	48.84	473	38.67	< 0.001***	0.304
Prob_Malware	1,067	44.33	473	35.18	< 0.001***	0.290
Prob_Ransomware	1,067	37.14	473	28.58	< 0.001***	0.293
Prob_DoS	1,067	30.23	473	24.10	< 0.001***	0.219

Freq_Own	**DirExp_Yes**			**DirExp_No**			**Sign.**	**Transformed**[10]
	N	Median	Mean	N	Median	Mean	(U-tests)	**Cohen's d**
Freq_Cyberattack	1,067	3.75	3.85	473	3.00	3.13	<0.001***	0.3975
Freq_Phishing	1,067	5.00	4.59	473	3.00	3.74	<0.001***	0.3577
Freq_Malware	1,067	4.00	4.22	473	3.00	3.40	<0.001***	0.3809
Freq_Ransomware	1,067	3.00	3.53	473	3.00	2.84	<0.001***	0.3456
Freq_DoS	1,067	3.00	3.08	473	2.00	2.53	<0.001***	0.2630

***, **, * The statistical significance is about 99 %, 98 %, 95 % by the usage of t-tests and Mann-Whitney-U-Tests.

[10] The transformation was performed by using the transformation function of www.psychometrica.de which calculated Cohen's d in line with the suggested transformation by Cohen (1992).

In order to analyze differences in cyber risk perception due to different degrees of indirect experience (hypothesis H2), Welch-ANOVAs[11] were performed. Thereby, the variables of indirect experience for malware-, phishing-, (D)DoS-, and ransomware-attacks were divided into the three groups of "low indirect experience" (values from 1.00 to 3.49 from a 7-point Likert-scale), "medium indirect experience" (values from 3.50 to 4.49 from a 7-point Likert-scale) and "high indirect experience" (values from 4.50 to 7.00 from a 7-point Likert-scale). Analogous Kruskal-Wallis tests were performed for the ordinal variable of frequency estimates.

As can be seen in Table 2, with increasing indirect experience also the perceived probability of malware-, phishing-, (D)DoS- and ransomware-attacks increases. Thereby, the probability estimates vary significantly depending on the different degrees of indirect experience for all four kinds of considered cyberattacks (for p-values and further information on post-hoc tests with Games-Howell, see Table 2), which supports hypothesis H2. Table 2 also shows the results of the Kruskal-Wallis tests for frequency estimates of cyberattack occurrence. In line with the probability estimates, frequency estimates increase for an increasing indirect experience, whereby the p-values and results of the Bonferroni post-hoc tests can be extracted from Table 2. Values for Cohen's f show a week to medium effect[12] of increasing indirect experience on perceived probabilities for cyberattack occurrence within the own enterprise (Cohen 1988). A positive relation between the degree of indirect experience and the probability and frequency estimates was also observed by analyzing Spearman-Rho correlations (see Table B.16 in the Appendix).

[11] Welch was used since Levene tests showed that the assumption of equal variances was not fulfilled for the given dataset.

[12] Small effect size from f = 0.1, medium effect size from f = 0.25, and large effect size from f = 0.4 (Cohen 1992).

Table 2

Cyber risk estimates for the own enterprise depending on the degree of indirect experience (low: 1.00 to 3.49, medium: 3.50 to 4.49, and high: 4.50 to 7.00 on a 7-point Likert-scale)[13]

IndExp of respective cyberattacks	**Prob_Cyberattack_Own**			**Prob_Phishing_Own**			**Prob_Malware_Own**			**Prob_Ransomware_Own**			**Prob_DoS_Own**		
	N	Mean (%)	SD	N	Mean (%)	SD	N	Mean (%)	SD	N	Mean (%)	SD	N	Mean (%)	SD
Low	490	29.28	23.11	378	35.21	30.48	459	32.61	28.25	568	25.63	25.20	835	20.11	22.44
Medium	251	34.45	26.66	149	40.94	31.54	172	35.58	28.96	182	32.91	27.67	168	34.64	28.81
High	799	43.54	29.05	1,013	50.33	34.22	909	47.14	32.78	790	41.27	30.95	537	39.20	31.57
Total	1,540	37.52	27.65	1,540	45.71	33.72	1,540	41.52	31.79	1,540	34.51	29.46	1,540	28.35	28.15

Prob_Cyberattack_Own: $F(2, 676.507) = 47.938$, $p < 0.001$, Cohen's $f = 0.241$. Games-Howell post-hoc test: Probability estimates differ significantly for the groups "Low & Medium", "Low & High", and "Medium & High" IndExp. **Prob_Phishing_Own**: $F(2, 385.851) = 32.981$, $p < 0.001$, Cohen's $f = 0.199$. Games-Howell post-hoc test: Probability estimates differ significantly for the groups "Low & High", and "Medium & High" IndExp. **Prob_Malware_Own**: $F(2, 473.499) = 38.948$, $p < 0.001$, Cohen's $f = 0.220$. Games-Howell post-hoc test: Probability estimates differ significantly for the groups "Low & High" and "Medium & High" IndExp. **Prob_Ransomware_Own**: $F(2, 512.013) = 52.371$, $p < 0.001$, Cohen's $f = 0.254$. Games-Howell post-hoc test: Probability estimates differ significantly for the groups "Low & Medium", "Low & High", and "Medium & High" IndExp. **Prob_DoS_Own**: $F(2, 426.215) = 82.989$, $p < 0.001$, Cohen's $f = 0.341$. Games-Howell post-hoc test: Probability estimates differ significantly for the groups "Low & Medium" and "Low & High" IndExp.

(continue next page)

[13] Effect size Cohen's f was computed by usage of eta-squared and transformation to Cohen's f by suggested computations of Cohen (1988) due to unequal group sizes.

(Table 2 continued)

IndExp of respective cyberattacks	**Freq_Cyberattack_Own**		**Freq_Phishing_Own**		**Freq_Malware_Own**		**Freq_Ransomware_Own**		**Freq_DoS_Own**	
	N	Mean Rank	N	Mean Rank	N	Mean Rank	N	Mean Rank	N	Mean Rank
Low	490	593.19	378	586.76	459	600.41	568	604.50	835	624.02
Medium	251	754.22	149	719.60	172	729.59	182	755.94	168	887.96
High	799	884.35	1,013	846.55	909	864.13	790	893.21	537	961.52
Total	1,540		1,540		1,540		1,540		1,540	

Freq_Cyberattack_Own: Chi-Squared (2) = 131.093, $p < 0.001$, Cohen's f = 0.303. Bonferroni post-hoc test: Frequency estimates differ significantly for the groups "Low & Medium", "Low & High", and "Medium & High" IndExp. **Freq_Phishing_Own**: Chi-Squared (2) = 99.292, $p < 0.001$, Cohen's f = 0.259. Bonferroni post-hoc test: Frequency estimates differ significantly for the groups "Low & Medium", "Low & High", and "Medium & High" IndExp. **Freq_Malware_Own**: Chi-Squared (2) = 111.622, $p < 0.001$, Cohen's f = 0.277. Bonferroni post-hoc test: Frequency estimates differ significantly for the groups "Low & Medium", "Low & High", and "Medium & High" IndExp. **Freq_Ransomware_Own**: Chi-Squared (2) = 143.841, $p < 0.001$, Cohen's f = 0.318. Bonferroni post-hoc test: Frequency estimates differ significantly for the groups "Low & Medium", "Low & High", and "Medium & High" IndExp. **Freq_DoS_Own**: Chi-Squared (2) = 210.859, $p < 0.001$, Cohen's f = 0.397. Bonferroni post-hoc test: Frequency estimates differ significantly for the groups "Low & Medium" and "Low & High" IndExp.

Table 3

Cyber risk estimates for the own enterprise depending on the degree of confidence (low: 1.00 to 3.49, medium: 3.50 to 4.49, and high: 4.50 to 7.00 on a 7-point Likert-scale)

Mean_Conf	**Prob_Cyberattack_Own**			**Prob_Phishing_Own**			**Prob_Malware_Own**			**Prob_Ransomware_Own**			**Prob_DoS_Own**		
	N	Mean (%)	SD	N	Mean (%)	SD	N	Mean (%)	SD	N	Mean (%)	SD	N	Mean (%)	SD
Low	307	42.82	26.67	307	51.63	31.95	307	48.27	30.48	307	38.04	29.34	307	33.35	28.00
Medium	396	38.42	26.27	396	48.16	33.40	396	43.61	30.65	396	34.67	27.73	396	27.25	26.64
High	837	35.15	28.37	837	42.39	34.13	837	38.05	32.34	837	33.14	30.21	837	27.04	28.71
Total	1,540	37.52	27.65	1,540	45.71	33.72	1,540	41.52	31.79	1,540	34.51	29.46	1,540	28.35	28.15

Prob_Cyberattack_Own: $F(2, 1537) = 9.014$, $p < 0.001$, Cohen's $f = 0.110$. Bonferroni post-hoc test: Probability estimates differ significantly for the groups "Low & High" Mean_Conf. **Prob_Phishing_Own**: $F(2, 1537) = 9.946$, $p < 0.001$, Cohen's $f = 0.112$. Bonferroni post-hoc test: Probability estimates differ significantly for the groups "Low & High" and "Medium & High" Mean_Conf. **Prob_Malware_Own**: $F(2, 1537) = 12.957$, $p < 0.001$, Cohen's $f = 0.131$. Bonferroni post-hoc test: Probability estimates differ significantly for the groups "Low & High" and "Medium & High" Mean_Conf**. Prob_Ransomware_Own**: $F(2, 1537) = 3.128$, $p = 0.044$, Cohen's $f = 0.063$. Bonferroni post-hoc test: Probability estimates differ significantly for the group "Low & High" Mean_Conf. **Prob_DoS_Own**: $F(2, 1537) = 6.109$, $p = 0.002$, Cohen's $f = 0.090$. Bonferroni post-hoc test: Probability estimates differ significantly for the groups "Low & Medium", and "Low & High" Mean_Conf.

(continue next page)

(Table 3 continued)

Mean_Conf	**Freq_Cyberattack_Own**		**Freq_Phishing_Own**		**Freq_Malware_Own**		**Freq_Ransomware_Own**		**Freq_DoS_Own**	
	N	Mean Rank	N	Mean Rank	N	Mean Rank	N	Mean Rank	N	Mean Rank
Low	307	780.90	307	781.98	307	780.23	307	765.57	307	797.22
Medium	396	767.64	396	771.14	396	791.41	396	760.18	396	747.22
High	837	768.04	837	765.99	837	757.04	837	777.19	837	771.72
Total	1,540		1,540		1,540		1,540		1,540	

Freq_Cyberattack_Own: Chi-Squared (2) = 0.211, p = 0.900, Cohen's f = 0.032. **Freq_Phishing_Own**: Chi-Squared (2) = 0.301, p = 0.860, Cohen's f = 0.032. **Freq_Malware_Own**: Chi-Squared (2) = 1.833, p = 0.400, Cohen's f = 0.000. **Freq_Ransomware_Own**: Chi-Squared (2) = 0.454, p = 0.797, Cohen's f = 0.032. **Freq_DoS_Own**: Chi-Squared (2) = 2.303, p = 0.316, Cohen's f = 0.032.

To examine whether SME owners and managers that exhibit a high confidence level in their overall cyber risk preparedness also have a lower cyber risk perception concerning the occurrence of cyberattacks (hypothesis H3), ANOVAs were performed to analyze potential differences in probability estimates on a percentage scale, while analogous Kruskal-Wallis tests were performed for analyzing differences in frequency estimates. The respondents were thereby clustered in three groups of "low confidence" (values from 1.00 to 3.49 from a 7-point Likert-scale), "medium confidence" (values from 3.50 to 4.49 from a 7-point Likert-scale) and "high confidence" (values from 4.50 to 7.00 from a 7-point Likert-scale,) by usage of the aggregated variable "Mean_Conf". Overall, a significant difference in the perceived probability for cyberattack occurrence within the own enterprise is observable depending on the degree of confidence (see Table 3). In line with this, Spearman-Rho correlations support the suggested negative relation between an increasing degree of confidence and a decreasing perceived probability for cyberattacks against the own enterprise (see Table B.17 in the Appendix). However, for frequency estimates a significant effect of the degree of confidence is not observable (for corresponding p-values and post-hoc tests with Bonferroni, see Table 3). This is also confirmed by analyzing corresponding values for Spearman-Rho (see Table B.18 in the Appendix). However, although H3 is supported for own probability estimates by significant differences based on the ANOVAs, corresponding values for Cohen's f show that the effect of confidence on probability estimates for the own enterprise is economically negligible small.

In order to analyze the influence of an optimistic bias (hypothesis H4) by an indirect method (Helweg-Larsen and Shepperd 2001), the probability and frequency estimates for the own enterprise and for a comparable enterprise were compared for the respective cyberattacks by usage of paired t-tests and Wilcoxon signed rank-tests. As a result, a significant difference is observable for probability estimates for the own enterprise and a comparable enterprise for malware-, phishing-, (D)DoS-, and ransomware-attacks, in that probability estimates for the own enterprise are significantly lower than for comparable others with Cohen's d ranging from 0.545 to 0.710 and hence showing a medium to strong economic effect according to Cohen (1988, 1992) of the estimation target on probability estimates (see Table 4). Analogously, significant differences for frequency estimates by the different estimation-targets (own enterprise and comparable enterprise) were observed for all respective cyberattacks with large effect sizes r (see Table B.19 in the Appendix). Therefore, hypothesis H4 is supported for all considered cyberattacks.

Table 4

Probability estimates for the respective cyberattacks for the own enterprise and a comparable enterprise (of the same size and industry-sector as of the responding enterprise)

	For the own enterprise		For a comparable other enterprise		Sign.	Cohen's d
	N	Mean (%)	N	Mean (%)	(t-test)	
Prob_Cyber-attack	1,538	37.56	1,538	54.30	< 0.001***	0.710
Prob_Phishing	1,531	45.81	1,531	66.22	< 0.001***	0.673
Prob_Malware	1,538	41.56	1,538	58.97	< 0.001***	0.614
Prob_Ransom-ware	1,522	34.64	1,522	50.96	< 0.001***	0.624
Prob_DoS	1,516	28.47	1,516	41.10	< 0.001***	0.545

5. Conclusion

The aim of this paper was to analyze the influence of the availability heuristic and the optimistic bias as well as the influence of (over-)confidence concerning cyber risk preparedness on cyber risk perception for German SME owners and managers, which has not been analyzed so far. This was done based on a questionnaire survey among 1,540 German SME owners and managers.

Based on univariate and bivariate tests, it could be shown that direct and indirect experience significantly influence cyber risk awareness in terms of perceived probability, such that SME owners and managers with direct and (higher) indirect experience exhibit a higher perceived probability of a cyberattack occurrence. This positive relationship holds for all four specific kinds of cyberattacks considered (malware-, phishing-, (D)DoS-, and ransomware-attacks), such that the availability heuristic influences cyber risk perception in terms of perceived probability of future cyberattacks. In contrast, for the assessment of confidence in organizational cyber risk preparedness (including one's own and employee's knowledge about cyber risk and cyber risk management capabilities), it is observed that the cyber risk perception is lower the higher the degree of confidence, such that the degree of confidence in organizational cyber risk preparedness negatively influences cyber risk perception in terms of perceived probability for future cyberattacks against the own enterprise. However, this observation holds not for the perceived frequency of cyberattacks. In addition, there exists a significant difference in the perceived probability of a cyberattack occurrence for the own enterprise and comparable others, which indicates the presence of an optimistic bias with respect to cyber risk perception. Analogous

results have been observed by asking respondents directly to rank their own vulnerability regarding cyberattacks compared to other SMEs, such that an optimistic bias could be observed for German SME owners and managers with a direct and indirect method. To sum up, univariate and bivariate tests support the influence of the availability heuristic, an optimistic bias, and (over-)confidence concerning cyber risk preparedness on cyber risk perceptions of German SMEs, although the degree of confidence might only have a negligibly small effect on the perceived probability of cyberattacks against the own enterprise.

While the present study provides insights into cyber risk perceptions of German SMEs, several limitations exist. For example, as the invitation for the online-questionnaire was sent via e-mail, the present dataset may be biased by the circumstance that especially those SME owners and managers with a lower cyber risk perception were following the included link, while more aware SME owners and managers may not have participated in the study. However, as the main purpose of this survey was not the evaluation of general cyber risk perception, but the influence of biases and heuristics, this limitation should have no influence on general observations, although other survey methods could be used in future research to gain further insight in this regard. Additionally, although the standardized definition for SMEs of the European Commission was used, the business category of SMEs is also defined by great heterogeneity as it does not only comprise small local crafts businesses, but also high-technology start-ups and market-leaders of niche products with substantial differences in existing resources, business goals and set prospects (Hoppe et al. 2021). Future work could therefore also study differences in cyber risk awareness due to behavioral influences depending on subgroups of SMEs (micro-, small-, and medium-sized enterprises) as well as for different industries, in order to make more detailed observations and corresponding recommendations for mitigating behavioral influences.

References

Allianz Global Corporate & Specialty SE (2022): Allianz risk barometer 2022. Accessed at 10th of November 2022 under https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2022.pdf.

Allianz Global Corporate & Specialty SE (2023): Allianz risk barometer. Identifying the major business risks for 2023. Accessed at 5th of February 2023 under https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf.

Aragón-Sánchez, A./*Sánchez-Marín*, G. (2005): Strategic orientation, management characteristics, and performance: A study of Spanish SMEs. In: Journal of Small Business Management, 43(3), 287–308.

Armstrong, J. S./*Overton*, T. S. (1977): Estimating nonresponse bias in mail surveys. In: Journal of Marketing Research – Special Issue: Recent Developments in Survey Research, 14(3), 396–402.

Ashby, S./*Buck*, T./*Nöth-Zahn*, S./*Peisl*, T. (2018): Emerging IT risks: Insights from German banking. In: Geneva Papers on Risk and Insurance – Issues and Practice, 43(2), 180–207.

Botzen, W. J. W./*Kunreuther*, H./*Michel-Kerjan*, E. (2015): Divergence between individual perceptions and objective indicators of tail risks: Evidence from floodplain residents in New York City. In: Judgment and Decision Making, 10(4), 365–385.

Bregu, K. (2022): The effect of overconfidence on insurance demand. In: The Geneva Risk and Insurance Review, 47(2), 298–326.

Bubeck, P./*Botzen*, W. J. W./*Aerts*, J. C. J. H. (2012): A review of risk perceptions and other factors that influence flood mitigation behavior. In: Risk Analysis, 32(9), 1481–1495.

Busenitz, L. W./*Barney*, J. B. (1997): Differences between entrepreneurs and managers in large organizations: Biases and heuristics in strategic decision-making. In: Journal of Business Venturing, 12(1), 9–30.

Cohen, J. (1988): Statistical power analysis for the behavioral sciences (2nd edition). New York: Lawrence Erlbaum Associates.

Cohen, J. (1992): A Power Primer. In: Psychological Bulletin, 112(1), 155–159.

Dreißigacker, A./*von Skarczinski*, B./*Wollinger*, G. R. (2021): Cyberangriffe gegen Unternehmen in Deutschland – Ergebnisse einer Folgebefragung 2020. Forschungsbericht Nr. 162, Kriminologisches Forschungsinstitut Niedersachsen e.V.

Eling, M./*Schnell*, W. (2016): What do we know about cyber risk and cyber risk insurance? In: The Journal of Risk Finance, 17(5), 474–491.

Engemann, P./*Fischer*, D./*Gosdzik*, B./*Koller*, T./*Moore*, N. (2017): Im Visier der Cyber-Gangster – So gefährdet ist die Informationssicherheit im deutschen Mittelstand. Accessed at 25th of July 2022 under https://store.pwc.de/de/publications/im-visier-der-cyber-gangster.

European Union (2020): User guide to the SME Definition. Accessed 20th of February 2022 under https://ec.europa.eu/docsroom/documents/42921.

Falkner, E. M./*Hiebl*, M. R. W. (2015): Risk management in SMEs: A systematic review of available evidence. In: The Journal of Risk Finance, 16(2), 122–144.

Fischhoff, B./*Bruine de Bruin*, W. (1999): Fifty-Fifty = 50%? In: Journal of Behavioral Decision Making, 12(2), 149–163.

Gatzert, N./*Schubert*, M. (2022): Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and values. In: Journal of Risk and Insurance, 89(3), 725–763.

GDV (2020): Cyberrisiken im Mittelstand 2020. Accessed at 27th of April 2021 under https://www.gdv.de/resource/blob/61466/0456901217b39a5893bc6829b8d7d156/report-cyberrisiken-im-mittelstand-2020-data.pdf.

GDV (2021): Cyberrisiken im Mittelstand 2021. Accessed at 1st of April 2022 under https://www.gdv.de/resource/blob/73768/a43ddbdad1e32ac804b8abfbd7f0c699/d-cyber report-2021-als-pdf-data.pdf.

GDV (2022a): So steht es um die IT-Sicherheit im deutschen Mittelstand. Accessed at 15th of November 2022 under https://www.gdv.de/resource/blob/89246/562cfe54b338 cf2aacf492cdb7cd87bc/d-factsheet-cybersicherheit-data.pdf.

GDV (2022b): Deutsche Unternehmen erwarten mehr Cyberangriffe – Aber nicht auf sich selbst. Accessed at 15th of November 2022 under https://www.gdv.de/gdv/medien/ medieninformationen/deutsche-unternehmen-erwarten-mehr-cyberangriffe-aber-nicht auf-sich-selbst-84912.

Gupta, A./*Hammond*, R. (2005): Information systems security issues and decisions for small businesses – An empirical examination. In: Information Management & Computer Security, 13(4), 297–310.

Helweg-Larsen, M./*Shepperd*, J. A. (2001): Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. In: Personality and Social Psychology Review, 5(1), 74–95.

Henschel, T. (2003): Risikomanagement im Mittelstand – eine empirische Untersuchung. In: Controlling & Management, 47(5), 331–337.

Hiscox (2021): Hiscox Cyber Readiness Report 2021. Accessed at 12th of July 2021 under https://www.hiscoxgroup.com/sites/group/files/documents/2021-04/Hiscox%20Cyber %20Readiness %20Report %202021.pdf.

Hiscox (2022): Hiscox Cyber Readiness Report 2022. Accessed at 5th of January 2023 under https://www.hiscox.co.uk/sites/default/files/documents/2022-08/Hiscox-UK-Cyber-Readiness-Report-2022.pdf.

Hoppe, F./*Gatzert*, N./*Gruner*, P. (2021): Cyber risk management in SMEs: Insights from industry surveys. In: The Journal of Risk Finance, 22(3/4), 240–260.

Icks, A./*Kranzusch*, P. (2022): Zukünftige Herausforderungen im Verarbeitenden Gewerbe und Reaktionen des Mittelstands, in: IfM Bonn, Chartbook, Bonn.

IfM Bonn (2022): Mittelstand im Einzelnen – KMU im EU-Vergleich. Accessed at 20th of July 2022 under https://www.ifm-bonn.org/statistiken/mittelstand-im-einzelnen/kmu-im-eu-vergleich.

ISO 31000 (2018): Risk management – Guidelines. Accessed at 03rd of July 2021 under https://www.iso.org/obp/ui/#iso:std:iso:31000:en.

Jalali, M. S./*Siegel*, M./*Madnick*, S. (2019): Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. In: The Journal of Strategic Information Systems, 28(1), 66–82.

Kahneman, D. (2013): Thinking, fast and slow. New York: Farrar, Straus and Giroux.

Kamiya, S./*Kang*, J.-K./*Kim*, J./*Milidonis*, A./*Stulz*, R. M. (2021): Risk management, firm reputation, and the impact of successful cyberattacks on target firms. In: Journal of Financial Economics, 139(3), 719–749.

Kellens, W./*Terpstra*, T./*De Maeyer*, P. (2013): Perception and communication of flood risks: A systematic review of empirical research. In: Risk Analysis, 33(1), 24–49.

Kostyuk, N./*Wayne*, C. (2021): The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. In: Journal of Global Security Studies, 6(2), ogz077, 1–25.

Kuusisto, T./*Ilvonen*, I. (2003): Information security culture in small and medium size enterprises. In: Frontiers of E-Business Research 2003, 431–439.

López, O. L./*Hiebl*, M. R. W. (2015): Management accounting in small and medium-sized enterprises: Current knowledge and avenues for further research. In: Journal of Management Accounting Research, 27(1), 81–119.

Quinn, M. (2011): Routines in management accounting research: Further exploration. In: Journal of Accounting & Organizational Change, 7(4), 337–357.

Rhee, H. S./*Ryu*, Y. U./*Kim*, C.-T. (2012): Unrealistic optimism on information security management. In: Computers & Security, 31(2), 221–232.

Russo, J. E./*Schoemaker*, P. J. H. (2018): Overconfidence. In: Augier, M. & Teece, D. J. (Eds.), The Palgrave Encyclopedia of Strategic Management. London: Palgrave Macmillan UK, pp. 1236–1246.

Sandroni, A./*Squintani*, F. (2007): Overconfidence, insurance, and paternalism. In: The American Economic Review, 97(5), 1994–2004.

Santos-Olmo, A./*Sánchez*, L. E./*Caballero*, I./*Camacho*, S./*Fernandez-Medina*, E. (2016): The importance of the security culture in SMEs as regards the correct management of the security of their assets. In: Future Internet, 8(3), 1–27.

Schapira, M. M./*Davids*, S. L./*McAuliffe*, T. L./*Nattinger*, A. B. (2004): Agreement between scales in the measurement of breast cancer risk perceptions. In: Risk Analysis, 24(3), 665–673.

Shepherd, D. A./*Williams*, T. A./*Patzelt*, H. (2015): Thinking about entrepreneurial decision making: Review and research agenda. In: Journal of Management, 41(1), 11–46.

de Smidt, G./*Botzen*, W. (2018): Perceptions of corporate cyber risks and insurance decision-making. In: The Geneva Papers on Risk and Insurance: Issues and Practice, 43(2), 239–274.

Taber, K. S. (2018): The use of Cronbach's alpha when developing and reporting research instruments in science education. In: Research in Science Education, 48(6), 1273–1296.

Thomann, C./*Pascalau*, R./*Graf von der Schulenburg*, J.-M. (2012): Corporate management of highly dynamic risks: Evidence from the demand for terrorism insurance in Germany. In: The Geneva Risk and Insurance Review, 37(1), 57–82.

Tversky, A./*Kahneman*, D. (1973): Availability: A heuristic for judging frequency and probability. In: Cognitive Psychology, 5(2), 207–232.

Tversky, A./*Kahneman*, D. (1974): Judgement under uncertainty: Heuristics and biases. In: Science, 185(4157), 1124–1131.

Tyler, T. R./*Cook*, F. L. (1984): The Mass Media and Judgments of Risk: Distinguishing Impact on Personal and Societal Level Judgments. In: Journal of Personality and Social Psychology, 47(4), 693–708.

Ulrich, P. S./*Timmermann*, A./*Frank*, V. (2022): Organizational aspects of cybersecurity in German family firms – Do opportunities or risks predominate? In: Organizational Cybersecurity Journal: Practice, Process and People, 2(1), 21–40.

Valli, C./*Martinus*, I./*Johnstone*, M. (2014): Small to medium enterprise cyber security awareness: an initial survey of Western Australian business. In: Proceedings of International Conference on Security and Management (pp. 71–75). Las Vegas, USA. Accessed at 3rd of February 2022 under https://worldcomp-proceedings.com/proc/p2014/SAM9779.pdf.

Weinstein, N. D. (1980): Unrealistic Optimism About Future Life Events. In: Journal of Personality and Social Psychology, 39(5), 806–820.

Weinstein, N. D. (1989): Optimistic biases about personal risks. In: Science, 246(4935), 1232–1233.

Weinstein, N. D./*Klein*, W. M. (1996): Unrealistic optimism: Present and future. In: Journal of Social and Clinical Psychology, 15(1), 1–8.

Welter, F./*May-Strobl*, E./*Holz*, M./*Pahnke*, A./*Schlepphorst*, S./*Wolter*, H.-J. (2015): Mittelstand zwischen Fakten und Gefühl. IfM Bonn: IfM-Materials Number 234, Bonn.

Wolf, T./*Fueglistaller*, U./*Müller*, J. (2018): KMU und Entscheidungen. Accessed at 23rd of August 2022 under https://www.kmu-tag.ch/wp-content/uploads/2019/07/KMU_studie_2018.pdf.

Appendix A. Survey Questions

Initially, we would like to have some information about the threat of potential cyberattacks within your industry. Have you **heard or read about successful cyberattacks on comparable enterprises** (same size and same industry as your enterprise)?

Please rate the corresponding frequency on a scale of 1 (never) to 7 (very frequently).

	Never						Very frequently
I have already heard or read about **malware**-attacks against comparable enterprises.	o	o	o	o	o	o	o
I have already heard or read about **phishing**-attacks against comparable enterprises.	o	o	o	o	o	o	o
I have already heard or read about **(D)DoS**-attacks against comparable enterprises.	o	o	o	o	o	o	o
I have already heard or read about **ransomware**-attacks against comparable enterprises.	o	o	o	o	o	o	o

Please imagine a **representative, comparable enterprise** (same size and same industry as your enterprise) for the following questions.

How often, in your opinion, is the **comparable enterprise affected by successful cyberattacks?**

Please estimate the general frequency of the mentioned cyberattacks on a scale of 1 (never) to 7 (several times in a year).

	Never.	Not very often, once every 50 years.	Seldomly, once every 10 years.	Occasionally, once every 5 years.	Often, once every 2 years.	Very often, every year.	Several times in a year.
Malware-attack	o	o	o	o	o	o	o
Phishing-attack	o	o	o	o	o	o	o
(D)DoS-attack	o	o	o	o	o	o	o
Ransomware-attack	o	o	o	o	o	o	o

In your opinion, what is the probability that the **comparable enterprise will be targeted by a successful cyberattack within the next year?**

Please rate your estimated probability on a scale of 0 % to 100 % for the mentioned cyberattacks.

Malware-attack	0 %	100 %
Phishing-attack	0 %	100 %
(D)DoS-attack	0 %	100 %
Ransomware-attack	0 %	100 %

Now think about your own enterprise.

How often, in your opinion, is **your own enterprise affected by successful cyberattacks?**

Please estimate the general frequency of the mentioned cyberattacks on a scale of 1 (never) to 7 (several times in a year).

	Never.	Not very often, once every 50 years.	Seldomly, once every 10 years.	Occasionally, once every 5 years.	Often, once every 2 years.	Very often, every year.	Several times in a year.
Malware-attack	o	o	o	o	o	o	o
Phishing-attack	o	o	o	o	o	o	o
(D)DoS-attack	o	o	o	o	o	o	o
Ransomware-attack	o	o	o	o	o	o	o

In your opinion, what is the probability that **your own enterprise will be targeted by a successful cyberattack within the next year?**

Please rate your estimated probability on a scale of 0 % to 100 % for the mentioned cyberattacks.

Malware-attack	0 %	100 %
Phishing-attack	0 %	100 %
(D)DoS-attack	0 %	100 %
Ransomware-attack	0 %	100 %

"Cyberattack" in the following refers to the specific cyberattack that you believe occurs most frequently.

How would you rate **your enterprises vulnerability to cyberattacks compared to other enterprises** (of the same size and in the same industry as yours)?

Please rate your estimate on a scale of 1 (much lower) to 7 (much higher).

	Much lower			As high			Much higher
In comparison to other enterprises, the risk of a successful cyberattack against my own enterprise is …	o	o	o	o	o	o	o

Now we would like to know how well prepared your company is for potential cyberattacks. To what extent do you agree with the following statements?

Please rate your agreement on a scale of 1 (do not agree at all) to 6 (completely agree).

	Do not agree at all					Completely agree
I am confident that **sufficient and appropriate prevention measures** have been established within my company to prevent potential cyberattacks.	o	o	o	o	o	o
I am confident that my company is adequately **prepared to respond to potential cyberattacks in a timely and appropriate manner**.	o	o	o	o	o	o

How would you rate **your knowledge and competencies, as well as the knowledge and competencies of your employees**, in the field of cyber risks and cyber risk management?

Please rate your knowledge/competencies and the knowledge/competencies of your employees regarding cyber risks and cyber risk management on a scale of 1 (very low) to 7 (very high).

	Very low						Very high
My knowledge level regarding cyber risks and their impact on the enterprise is…	o	o	o	o	o	o	o
The knowledge level of my employees regarding cyber risks and their impact on the enterprise is in general…	o	o	o	o	o	o	o
My competencies in preventing cyberattacks within the enterprise are…	o	o	o	o	o	o	o
The competencies of my employees in preventing cyberattacks within the enterprise are in general…	o	o	o	o	o	o	o
My competencies in appropriately responding to a potential cyberattack are…	o	o	o	o	o	o	o
The competencies of my employees in appropriately responding to a potential cyberattack are in general…	o	o	o	o	o	o	o

Have you already established a **cyber incident response plan**?

Please choose the statement that applies.

- ☐ Yes, an incident response plan is in place.
- ☐ No, an incident response plan has not been established yet.
- ☐ I am not familiar with this term.
- ☐ I don't know.

DOI https://doi.org/10.3790/zverswiss.2024.1430701 | Generated on 2025-01-22 11:42:49

How often are **cyber security trainings** for employees offered in your enterprise? Please choose the appropriate statements (multiple answers possible).
☐ In our enterprise **no cyber security training** has taken place so far.
☐ In our enterprise, cyber security trainings take place **irregularly**.
☐ In our enterprise, cyber security trainings take place **regularly**.
☐ In our enterprise, employees can **continuously educate themselves independently through (online) training materials** on the topic of cyber security.

The next question was only asked if cybersecurity trainings are offered in the respective enterprise.

Have you personally participated in these trainings? Please choose the appropriate statement.
☐ Yes.
☐ No.
☐ I don't want to provide this information.

Have you **experienced or have you been affected by a cyberattack in the past**? We are interested in both successful cyberattacks as well as those that were successfully defended by security systems. Please check the appropriate statements (multiple answers possible).
☐ Yes, **my enterprise** has already been affected by a cyberattack.
☐ Yes, I have already experienced a cyberattack **in my previous working situation**.
☐ Yes, I have already experienced a cyberattack **in my private surroundings**.
☐ Yes, I have already **been privately affected** by a cyberattack.
☐ No, I have not yet experienced a cyberattack or been affected by one.

The next two questions were only asked if the respondent had already experienced a cyberattack in past.

How long ago did you personally experience or have you been personally affected by a cyberattack? Please choose the correct statement.
☐ Less than three months.
☐ Between three and six months.
☐ Between six months and one year.
☐ Between one and two years.
☐ More than two years ago.
☐ I don't want to provide this information.

Could the cyberattack be defended by existing security systems and measures, or was the cyberattack successful? Please choose the correct statement.
☐ The cyberattack was successfully defended by existing security measures and no financial loss occurred.
☐ The cyberattack was successful and resulted in financial loss.

As we aim to assess the perception of cyber risks among small and medium-sized enterprises, we kindly ask you to answer the following questions honestly. The questions are intended to verify the applicability of the EU definition of small and medium-sized enterprises to your company.

How many employees work within your enterprise?
☐ Up to 9 employees
☐ Between 10 and 49 employees
☐ Between 50 and 249 employees
☐ More than 249 employees

How high was the annual revenue of your enterprise on average in recent years?
☐ Up to 2 million euros.
☐ Up to 10 million euros.
☐ Up to 50 million euros.
☐ Higher than 50 million euros.

How high was the balance sheet total of your company on average in recent years?
☐ Up to 2 million Euros
☐ Up to 10 million Euros
☐ Up to 43 million Euros
☐ Higher than 43 million Euros

In the last part of this survey, we would like to get to know you and your company better.

What industry does your company belong to?
☐ Agriculture, Forestry and Fishing
☐ Mining and Quarriying
☐ Manufacturing
☐ Energy Supply
☐ Water Supply; Waste Water and Waste Management
☐ Construction
☐ Wholesale and Trade
☐ Transportation and Storage
☐ Accommodation and Food Service
☐ Information and Communication
☐ Financial and Insurance Services
☐ Real Estate and Renting
☐ Professional, Scientific and Technical Services
☐ Other Economic Services
☐ Public Administration, Defense; Social Security
☐ Education and Training
☐ Health and Social Services
☐ Arts, Entertainment and Recreation
☐ Other Service Activities
☐ Other: _____

Which functions do you take care of in the company (multiple answers possible)?
☐ Purchasing/Procurement
☐ Marketing, Sales and Logistics
☐ Production
☐ Risk Management (including Insurance Management)
☐ Law and Compliance
☐ Finance/Controlling/Accounting
☐ Human Resources
☐ IT
☐ Research and Development
☐ Management
☐ Others: _____

How old are you?

What is your gender?
☐ Male
☐ Female
☐ No answer

I have carefully completed the questions in the questionnaire. Please rate your agreement on a scale of 1 (do not agree at all) to 7 (fully agree).						
Do not agree at all						Fully agree
o	o	o	o	o	o	o

Appendix B. Further Results of the Statistical Analysis

Table B.1

Enterprise-classification, number of employees, annual turnover, and balance sheet total within the sample (N = 1,540)

Classification	**Frequency**	**Percentage**
Microenterprise	436	28.31
Small enterprise	751	48.77
Medium-sized enterprise	353	22.92
Total	1,540	100.00
Number of Employees	**Frequency**	**Percentage**
Up to 9 employees	457	29.67
10 to 49 employees	747	48.51
50 to 249 employees	336	21.82
Total	1,540	100.00
Annual Turnover	**Frequency**	**Percentage**
Up to 2 Mio. Euro	814	52.86
Up to 10 Mio. Euro	520	33.77
Up to 50 Mio. Euro	191	12.40
More than 50 Mio. Euro	15	0.97
Total	1,540	100.00
Balance Sheet Total	**Frequency**	**Percentage**
Up to 2 Mio. Euro	928	60.26
Up to 10 Mio. Euro	466	30.26
Up to 43 Mio. Euro	131	8.51
More than 43 Mio. Euro	15	0.97
Total	1,540	100.00

Table B.2

Industry classification within the sample (N = 1.540)

	Branch/Industry[14]	**Frequency**	**Percentage**
A	Agriculture, Forestry, and Fishing	14	0.91
B	Mining and Quarrying	2	0.13
C	Manufacturing	221	14.35
D	Electricity, Gas, Steam, Air Conditioning Supply	17	1.10
E	Water Supply, Sewerage, Waste Management and Remediation Activities	21	1.36
F	Construction	128	8.31
G	Wholesale and Retail Trade	161	10.45
H	Transportation and Storage	35	2.27
I	Accommodation and Food Service Activities	27	1.75
J	Information and Communication	201	13.06
K	Financial and Insurance Activities	30	1.95
L	Real Estate Activities	42	2.73
M	Professional, Scientific and Technical Activities	123	7.99
N	Other economic services	79	5.13
O	Public Administration and Defense	11	0.71
P	Education	26	1.69
Q	Human Health and Social Work Activities	81	5.26
R	Arts, Entertainment and Recreation	16	1.04
S	Other Service Activities	104	6.75
	Others (open text field)	201	13.06
	Total	1,540	100.00

[14] Constitute the classification of the business sectors of the German Federal Bureau of Statistics (WZ 2008).

Table B.3

Company function(s) of the respondents within the sample (N = 1,540)

Function(s)	Number*
Management Board	1,077
IT (Information Technology)	662
Purchasing and Procurement	206
Marketing, Sales, Logistics	194
Finance/Controlling/Accounting	193
Risk management (Insurance management)	181
Human Resources	177
Legal und Compliance	137
Research and Development	87
Others	71

* Multiple selection was possible; hence respondents could select several answering options.

Table B.4

Perceived probability of a successful cyberattack (i. e. resulting in a financial loss) for the own enterprise and a comparable enterprise within the next year*

	For the own enterprise			For a comparable other enterprise		
	N	Mean (%)	SD	N	Mean (%)	SD
Prob_Phishing	1,540	45.71	33.72	1,531	66.22	30.37
Prob_Malware	1,540	41.52	31.79	1,538	58.97	29.70
Prob_Ransomware	1,540	34.51	29.46	1,522	50.96	30.35
Prob_DoS	1,540	28.35	28.15	1,516	41.10	28.95
Prob_Cyberattack	1,540	37.52	27.65	1,538	54.30	25.72

* Answering scale for probability estimates from 0 % to 100 % in intervals of 10 %.

Table B.5

Perceived frequency of a successful cyberattack (i. e. resulting in a financial loss) for the own enterprise and a comparable enterprise*

	For the own enterprise				For a comparable other enterprise			
	N	Median	Mean	SD	N	Median	Mean	SD
Freq_Phishing	1,540	4.00	4.33	2.16	1,540	6.00	5.56	1.68
Freq_Malware	1,540	4.00	3.97	2.03	1,540	5.00	5.13	1.67
Freq_Ransomware	1,540	3.00	3.32	1.91	1,540	4.00	4.47	1.72
Freq_DoS	1,540	3.00	2.91	1.81	1,540	4.00	3.91	1.73
Freq_Cyberattack	1,540	3.50	3.63	1.73	1,540	5.00	4.77	1.43

* Answering scales for frequency estimates from 1 = Never, 2 = Not very often, once every 50 years, 3 = Seldomly, once every 10 years, 4 = Occasionally, once every 5 years, 5 = Often, once every 2 years, 6 = Very often, every year, 7 = Several times in a year.

Table B.6

The own vulnerability level for cyberattacks in comparison to comparable organizations (N = 1,540)

In comparison with another organization, the vulnerability level for a successful cyberattack within my own organization…	Frequency	Percentage
1 = is much lower.	181	11.75
2	317	20.58
3	316	20.52
4 = is as high.	637	41.36
5	54	3.51
6	24	1.57
7 = is much higher.	11	0.71
Total	1,540	100.00

Table B.7

Direct experience of a cyberattack by attack-location within the sample (N = 1,540)*

Attack-location	Frequency	Percentage
My enterprise was already targeted by a cyberattack.	711	46.17
A cyberattack happened in my previous working activity.	344	22.34
A cyberattack happened within my private surroundings.	434	28.18
I was already privately targeted by a cyberattack	203	13.18

* Multiple selection was possible; hence respondents could select several answering options.

Table B.8

Time-span since cyberattack happened for all attack-locations (N = 1,540)

Time-span since cyberattack happened	Frequency	Percentage
Less than three months.	183	11.88
Between three and six months.	102	6.62
Between six months and one year.	148	9.61
Between one year and two years.	204	13.25
More than two years.	408	26.49
No cyberattack happened/ no information provided.	495	32.14

Table B.9

Direct experience of a successful cyberattack (i. e. resulting in a financial loss) within the sample (N = 1,540)

Direct experience of successful cyberattacks	Frequency	Percentage
Successful cyberattack.	374	24.28
Cyberattack was successfully defended.	692	44.93
No cyberattack happened/no information provided.	474	30.78

Table B.10

Degree of indirect experience for the respective cyberattacks within the sample (N = 1,540)

Frequency of reading/hearing about successful cyberattacks against a comparable enterprise	N	Mean	SD
IndExp_Phishing	1,540	4.93	1.97
IndExp_Malware	1,540	4.53	2.01
IndExp_Ransomware	1,540	4.19	2.10
IndExp_DoS	1,540	3.44	2.12
IndExp_Cyberattack	1,540	4.27	1.80

Table B.11

Degree of confidence for general cyberattack preparedness, organizational knowledge in cyber risks and competencies in cyber risk management within the sample (N = 1,540)

Degree of confidence	N	Min	Max	Mean	SD
Conf_Prev_General	1,540	1	6	4.36	1.21
Conf_React_General	1,540	1	6	4.14	1.29
Conf_Prev_General_Transformed[15]	1,540	1	7	5.03	1.45
Conf_React_General_Transformed[15]	1,540	1	7	4.77	1.55
Knowl_Own	1,540	1	7	5.13	1.43
Knowl_Empl	1,540	1	7	4.07	1.55
Compet_Prev_Own	1,540	1	7	4.55	1.56
Compet_Prev_Empl	1,540	1	7	3.86	1.65
Compet_React_Own	1,540	1	7	4.84	1.51
Compet_React_Empl	1,540	1	7	3.92	1.70
Mean_Conf	1,540	1	7	4.52	1.17

[15] Initial 6-point Likert-scales of general preparedness were transformed to a 7-point Likert-scale by increasing the maximum value to 7 and increasing each value iteratively by 0.2.

Table B.12

Establishment of a cyber incident response plan within the sample (N = 1,540)

	N	Frequency	Percentage
An indecent response plan exists.	1,540	396	25.71
An incident response plan has not been developed so far.	1,540	881	57.21
I don't know the term.	1,540	241	15.65
I don't know.	1,540	22	1.43

Table B.13

Execution of cybersecurity trainings within the sample (N = 1,540)*

Within our enterprise…	N	Frequency	Percentage
No cybersecurity training has taken place so far.	1,540	612	39.74
Cybersecurity trainings take place irregularly.	1,540	575	37.34
Cybersecurity trainings take place regularly.	1,540	293	19.02
Opportunities for our employees to execute cybersecurity trainings by themselves online are provided.	1,540	250	16.23

* Multiple selection was possible; hence respondents could select several answering options.

Table B.14

Probability estimates for the own enterprise depending on previous direct experience (recent: within the last year; past: more than one year ago) and salience (succ: successful, i. e. resulting in a financial loss)

Prob_Own	DirExp_Recent		DirExp_Past		Sign.	Cohen's d	DirExp_Succ		DirExp_NoSucc		Sign.	Cohen's d
	N	Mean (%)	N	Mean (%)	(t-test)		N	Mean (%)	N	Mean (%)	(t-test)	
Prob_Cyber-attack	433	42.03	612	39.05	0.089	0.107	374	43.14	692	38.48	0.009***	0.167
Prob_Phishing	433	51.73	612	47.09	0.029*	0.137	374	51.66	692	47.27	0.044*	0.129
Prob_Malware	433	45.80	612	43.55	0.269	0.070	374	47.38	692	42.63	0.022*	0.147
Prob_Ransom-ware	433	38.27	612	36.68	0.404	0.052	374	41.34	692	34.81	<0.001***	0.217
Prob_DoS	433	32.33	612	28.87	0.063	0.119	374	32.19	692	29.20	0.110	0.103

***, **, * The statistical significance is about 99 %, 98 %, 95 % by the usage of t-tests.

Table B.15

Frequency estimates for the own enterprise depending on previous direct experience (recent: within the last year; past: more than one year ago) and salience (succ: successful, i. e. resulting in a financial loss)

Freq_Own	DirExp_Recent (N = 433)		DirExp_Past (N = 612)		Sign. (U-test)	Transformed[16] Cohen's d	DirExp_Succ (N = 374)		DirExp_NoSucc (N = 692)		Sign. (U-test)	Transformed[16] Cohen's d
	Median	Mean	Median	Mean			Median	Mean	Median	Mean		
Freq_Cyberattack	4.00	4.01	3.50	3.68	< 0.001***	0.255	3.87	3.93	3.75	3.81	0.247	0.063
Freq_Phishing	5.00	4.88	4.00	4.36	< 0.001***	0.255	5.00	4.66	5.00	4.54	0.496	0.000
Freq_Malware	4.00	4.44	4.00	4.07	0.002***	0.191	4.00	4.24	4.00	4.21	0.933	0.000
Freq_Ransomware	4.00	3.70	3.00	3.41	0.036*	0.127	3.00	3.68	3.00	3.45	0.057	0.110
Freq_DoS	3.00	3.37	3.00	2.86	< 0.001***	0.238	3.00	3.16	3.00	3.04	0.309	0.063

***, **, * The statistical significance is about 99 %, 98 %, 95 % by the usage of Mann-Whitney-U-Tests.

[16] The transformation was performed by using the transformation function of www.psychometrica.de which calculated Cohen's d in line with the suggested transformation by Cohen (1992).

Table B.16

Spearman-Rho correlations between probability and frequency estimates for the own enterprise and indirect experience

Spearman-Rho	N	Correlation	Sign.	Effect size*
IndExp_Phishing (N = 1,540)				
Prob_Phishing_Own	1,540	0.191	< 0.001***	Small
Freq_Phishing_Own	1,540	0.287	< 0.001***	Small
IndExp_Malware (N = 1,540)				
Prob_Malware_Own	1,540	0.213	< 0.001***	Small
Freq_Malware_Own	1,540	0.292	< 0.001***	Small
IndExp_Ransomware (N = 1,540)				
Prob_Ransomware_Own	1,540	0.245	< 0.001***	Small
Freq_Ransomware_Own	1,540	0.328	< 0.001***	Medium
IndExp_DoS (N = 1,540)				
Prob_DoS_Own	1,540	0.325	< 0.001***	Medium
Freq_DoS_Own	1,540	0.405	< 0.001***	Medium

* Small effect size from r = 0.1, medium effect size from r = 0.3, and large effect size from r = 0.5 according to Cohen (1992).

Table B.17

Spearman-Rho correlations between probability estimates for the own enterprise and mean confidence

	Mean_Conf (N = 1,540)			
Spearman-Rho	**N**	**Correlation**	**Sign.**	**Effect size***
Prob_Cyberattack_Own	1,540	–0.158	< 0.001***	Small
Prob_Phishing_Own	1,540	–0.164	< 0.001***	Small
Prob_Malware_Own	1,540	–0.172	< 0.001***	Small
Prob_Ransomware_Own	1,540	–0.114	< 0.001***	Small
Prob_DoS_Own	1,540	–0.111	< 0.001***	Small

* Small effect size from r = 0.1, medium effect size from r = 0.3, and large effect size from r = 0.5 according to Cohen (1992).

Table B.18

Spearman-Rho correlations between frequency estimates for the own enterprise and mean confidence

	Mean_Conf (N = 1,540)			
Spearman-Rho	**N**	**Correlation**	**Sign.**	**Effect size***
Freq_Cyberattack_Own	1,540	–0.32	0.205	Medium, not significant
Freq_Phishing_Own	1,540	–0.31	0.223	Small, not significant
Freq_Malware_Own	1,540	–0.48	0.058	Medium, not significant
Freq_Ransomware_Own	1,540	–0.016	0.528	Negligible
Freq_DoS_Own	1,540	–0.26	0.317	Small, not significant

* Small effect size from r = 0.1, medium effect size from r = 0.3, and large effect size from r = 0.5 according to Cohen (1992).

Table B.19

Perceived frequency for the own enterprise versus a comparable other enterprise within the sample (N = 1,540)

	Own (N = 1,540)		**Others (N = 1,540)**		**Sign.**	**Effect size r***
	Median	Mean	Median	Mean	(Wilcoxon)	
Freq_Cyber-attack	3.50	3.63	5.00	4.77	< 0.001***	0.609
Freq_Phishing	4.00	4.33	6.00	5.56	< 0.001***	0.528
Freq_Malware	4.00	3.97	5.00	5.13	< 0.001***	0.528
Freq_Ransom-ware	3.00	3.32	4.00	4.47	< 0.001***	0.555
Freq_DoS	3.00	2.91	4.00	3.91	< 0.001***	0.535

* Effect size for the Wilcoxon signed-rank test was calculated as correlation-coefficient of Pearson by r = |z/ sqr(N)|. Small effect size from r = 0.1, medium effect size from r = 0.3, and large effect size from r = 0.5 according to Cohen (1992).