



Assure or Insure Cyber Risk? Nonprofessional Investors' Willingness to Invest^{*}

KEVIN GAUCH , *Technical University of Darmstadt*[†]

REINER QUICK , *Technical University of Darmstadt*

ABSTRACT

Organizations face severe cyber risks, which may lead companies to contract related insurance or to demand cybersecurity assurance services to signal risk management. This paper experimentally investigates how cybersecurity assurance and insurance against cyber risks impact nonprofessional investors. We conducted an experiment with a 2×2 between-subjects design with 100 UK nonprofessional investors and manipulated the assurance provision and insurance purchase to analyze their impact on willingness to invest. Our results suggest that cybersecurity assurance and cyber risk insurance positively affect willingness to invest. The results confirm the usefulness of measures to handle cyber risks and are of interest to managers, auditors, regulators, and academics.

Keywords: assurance services, cyber risk, cybersecurity, insurance, nonprofessional investors, risk management

SERVICES D'ASSURANCE EN MATIÈRE DE CYBERSÉCURITÉ OU ASSURANCE CYBERRISQUES? PROPENSION À INVESTIR CHEZ LES INVESTISSEURS NON PROFESSIONNELS

RÉSUMÉ

Les organisations sont confrontées à de graves cyberrisques, ce qui peut les inciter à souscrire une assurance pour s'en protéger ou à obtenir des services d'assurance en matière de cybersécurité pour indiquer qu'elles gèrent ces risques. La présente étude se penche de façon expérimentale sur la façon dont les services d'assurance en matière de cybersécurité et l'assurance contre les cyberrisques influencent les investisseurs non professionnels. Nous avons mené une expérience faisant appel à une conception intersujets 2×2 auprès de 100 investisseurs non professionnels du Royaume-Uni et avons

This is an open access article under the terms of the [Creative Commons Attribution-NonCommercial](https://creativecommons.org/licenses/by-nc/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited and is not used for commercial purposes.

* Accepted by Karim Jamal. We are grateful to the associate editor (Karim Jamal), the anonymous reviewers and, for their extensive comments, Jette Fabian (discussant), Christian Friedrich, Nicolas Pappert, Laura Georg Schaffner, and Steve G. Sutton (discussant). Furthermore, we thank the participants at the 2022 German doctoral colloquium on accounting and auditing research, 4th GAMOD–EIASM Workshop on Governance and Management of Digitalization, 19th EIASM Workshop on Corporate Governance, and 45th EAA congress, as well as the participants at the 12th EARNet Symposium 2023.

† Corresponding author.

manipulé la prestation des services d'assurance et la souscription d'une assurance pour analyser leur impact sur leur propension à investir. Nos résultats portent à croire que ces deux stratégies ont une influence positive sur la propension des investisseurs non professionnels à investir. Les résultats confirment l'utilité des mesures mises en œuvre pour gérer les cyberrisques et sont pertinents pour les gestionnaires, les auditeurs, les organismes de réglementation et les chercheurs.

Mots-clés : assurance, cyberrisques, cybersécurité, investisseurs non professionnels, gestion des risques, services d'assurance

1. INTRODUCTION

Over the past few decades, the increasing usage of digital technologies and the strong interconnectedness of companies have underscored the importance and role of cybersecurity as a new dimension of risk management (Amir et al., 2018; Haapamäki & Sihvonen, 2019). Knechel (2021) emphasizes, “One of the most important emerging areas of disclosure for many organizations is cybersecurity” (p. 139). Major incidents, such as the WannaCry cyberattack, have attracted the attention of company stakeholders.¹ Cyber risks severely threaten the cybersecurity of a company and are part of a company's operational risks (Aldasoro et al., 2022). Cyber risks are now at the top of every company's agenda (Hobbs, 2023; Li et al., 2018; Rothrock et al., 2018) but are usually difficult to estimate due to unreliable data (Biener et al., 2015). This threat may result in financial losses, such as system failure or the disruption of information technology (IT) systems and processes. These risks include various malicious cyber incidents (cyberattacks), where the threat actor intends to cause harm (e.g., ransomware attacks, hacking incidents, or employee data theft) (Aldasoro et al., 2022). In addition to high monetary damages, companies often suffer long-lasting reputational losses (Agrafiotis et al., 2018; Haapamäki & Sihvonen, 2019; Kamiya et al., 2021). The relevance of cybersecurity is also highlighted by the SEC regulations on improving and standardizing disclosure regarding cybersecurity risk management, strategy, governance, and incident disclosure by public companies (SEC, 2023). Furthermore, the AICPA published a guide on reporting on an entity's cybersecurity risk management program and controls (AICPA, 2017). Likewise, Chartered Professional Accountants of Canada (CPA Canada) has adapted this guide to Canadian standards (CPA Canada, 2018).

Cybersecurity is often used as a synonymous expression for information security (AICPA, 2017; Alexei & Alexei, 2022; Haapamäki & Sihvonen, 2019), which aims to ensure the continuity of business operations by minimizing security incidents, thereby reducing the impact of security risks on the company. The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 series of standards (International Organization for Standardization [ISO], n.d.) defines information security as maintaining the confidentiality, integrity, and availability of information.

1. The WannaCry virus was a global cyberattack in May 2017 with far-reaching consequences. After infecting computers, the malicious program encrypts the files and asks users to pay around US\$300, threatening data loss if the deadline passes.

However, Von Solms and van Niekerk (2013) argue that cybersecurity extends beyond the boundaries of traditional information security. In addition to protecting information, cybersecurity also includes protecting those operating in cyberspace and all their assets accessed through cyberspace (Alexei & Alexei, 2022; Von Solms & van Niekerk, 2013).

Dealing with risks is a crucial task for management as it fundamentally impacts business operations. Therefore, companies are required to actively consider and manage cyber risks in their risk management process. The well-known and generally accepted framework from COSO (2004) describes components of enterprise-wide risk management, of which risk response is one part. Two prominent cyber risk management strategies are reducing risks (e.g., assurance) and transferring risks (e.g., insurance). Consequently, an investment in cybersecurity through an appropriate IT infrastructure is essential. Therefore, the internationally recognized standard ISO/IEC 27001 describes the structure of an information security management system, which is intended to provide effective protection of information and IT systems (ISO, n.d., 2013). While companies are not obliged to follow ISO/IEC 27001, it is considered the standard cybersecurity or IT risk management framework in most organizations worldwide (Roy, 2020). Likewise, a study by Slapničar et al. (2022) reveals that companies predominantly use ISO/IEC 27001 as a cybersecurity framework.²

Companies may voluntarily engage an independent third party to provide assurance in accordance with this standard and to ensure the appropriateness and effectiveness of cybersecurity. Therefore, they might engage major audit firms offering cybersecurity assurance services according to ISO/IEC 27001 (EY, 2023; KPMG, 2023). With such a system and its assurance, cybersecurity can be significantly improved, and the likelihood of a successful cyber incident is minimized. Furthermore, cybersecurity assurance can signal the credibility of the cybersecurity management system to the company's stakeholders. In the following analysis, cybersecurity assurance is considered according to ISO/IEC 27001. Usually, such assurance services are provided by audit firms. However, the type of assurance provider might be a relevant factor. A study by the International Federation of Accountants (2021) reveals that 37% of companies worldwide chose an alternative assurance provider regarding environmental, social, and governance (ESG) report assurance, which might be similar to cybersecurity assurance services. A reason for a company to choose a third-party provider instead of an audit firm might be that such a provider potentially has higher technical competence than audit firms.

Another way to treat risks is to transfer them to insurance companies. Such companies have been offering so-called cyber insurance policies since the early 2000s, which enable risk transfer and thus partially compensate for possible damage (Eling et al., 2021). Apart from the primary purpose of transferring cyber risks, cyber insurance is assumed to have an additional positive effect: companies might increase their

2. However, it is worth acknowledging that other commonly used cybersecurity frameworks exist. For example, in 2019, the Center for Internet Security issued CIS Controls Version 7.1, and in 2019 the National Institute of Standards and Technology published its own Cybersecurity Framework (Walton et al., 2021).

investments in cyber protection to reduce their premiums. Furthermore, purchased cyber insurance may indicate the quality of cybersecurity (Marotta et al., 2017). The purchase of insurance can reduce the information asymmetry between management and stakeholders because the monitoring function is transferred to the insurer. This means that the insurance company can ensure that management takes appropriate measures to monitor cyber risks or make appropriate investments (Ashby & Diacon, 1998). Additionally, transferring risks to the insurance company can reduce the likelihood that transaction costs may occur. Consequently, relevant information regarding the risk treatment can influence the behavior of nonprofessional investors.

Cybersecurity assurance and insurance against cyber risks should change non-professional investors' perceived level of risk. This can be explained based on the general definition of risk, where risk is defined as the probability of occurrence times the financial impact (Marotta et al., 2017). Improved cybersecurity through an assurance service might reduce the probability of occurrence, whereas cyber insurance reduces the financial impact. Therefore, we assume that both measures reduce participants' perceptions of risk, leading to positive perceptions.

However, it is not only the mere implementation of risk management strategies, such as cybersecurity assurance or cyber insurance, that is essential, but also the communication of risks and measures the company takes. Investors increasingly perceive cybersecurity as a fundamental component of companies' ESG efforts and demand more information. They are concerned because the financial market reacts negatively to cyber incidents, which results in a loss of the investors' investments (Frank et al., 2023). That is why high-quality risk disclosure enables investors to align their investments with their risk preferences, and financial analysts usually support their stock recommendations by referring to specific company risks (Yeo, 2021). Management can, therefore, require an independent and voluntary cybersecurity assurance service and purchase cyber insurance so that the company signals the credibility of the cybersecurity. However, there is also no legal requirement to disclose such information.

Against this background, this paper experimentally investigates whether cybersecurity assurance and cyber risk insurance influence nonprofessional investors' decisions. Nonprofessional investors were chosen because they reflect the company's equity investors, a key stakeholder group. Participants were acquired through the online platform Prolific. Our results reveal that cybersecurity assurance and the purchase of cyber risk insurance positively impact nonprofessional investors' willingness to invest, suggesting that companies should consider using these risk management strategies.

Our study makes several contributions. First, to the best of our knowledge, this study is the first to experimentally analyze the decision usefulness of cybersecurity assurance in combination with cyber risk insurance. Cybersecurity assurance differs from other assurance services in that it verifies the effectiveness and appropriateness of a management system and does not check whether a report is free of misstatements. Whereas most studies experimentally examine cybersecurity assurance in the context of a cyber incident (Frank et al., 2019; Navarro & Sutton, 2024; Perols, 2023; Perols & Murthy, 2021), this

study investigates the impact of such assurance services during times of normal business operations. Therefore, the study contributes to companies that benefit from disclosing assurance information even if no cyber incident occurs. Furthermore, shareholders may also doubt whether audit firms are adequate assurance providers. However, our findings suggest that the assurance providers seem irrelevant to nonprofessional investors. Second, we address the existing research gap regarding new forms of assurance, following a suggestion by Hay (2019). Knechel (2021) describes the increasing relevance and need for research in cybersecurity risk management. Our study is potentially relevant to regulators and practitioners. From a regulatory perspective, we provide evidence for assurance regulation—for example, a mandate to periodically assure the cybersecurity system. However, the benefits must outweigh the costs of the assurance service (Schoenfeld, 2024). From a practitioner perspective, our results show that organizations benefit from voluntary assurance, which provides an argument that audit committees should require such services and that assurance providers should offer them. Furthermore, the findings show that information on assurance and insurance is a signal that attracts equity investors. Annual report users can benefit from the study because they know such information can be relevant. For insurance companies, this indicates a demand for companies to have cyber insurance that can be exploited.

The paper is structured as follows. Section 2 provides background information and an overview of previous research and develops the hypotheses. Section 3 describes our experimental case. Section 4 presents the results. Finally, Section 5 discusses and summarizes the study's main findings, limitations, and avenues for future research.

2. THEORETICAL BACKGROUND, PRIOR RESEARCH, AND HYPOTHESIS DEVELOPMENT

Considering the paucity of empirical evidence regarding cybersecurity assurance as well as cyber risk insurance, we additionally refer to similar prior research and a hypothesis development informed by theory.

Assurance Provision

Signaling theory and source credibility theory are both appropriate theoretical approaches to explaining the impact of cybersecurity assurance on stakeholder (i.e., nonprofessional investor) decisions.

Spence's (1973) signaling theory describes the deliberate reduction of information asymmetries through a transfer of information as a signal to the market. Through a voluntary signal, the partner conveys trust, which reinforces mutual interest in maintaining the partnership (Diong et al., 2018; Six et al., 2010; Vosselman & van der Meer-Kooistra, 2009). Research shows that the company's signal adapts to users' specific information needs (Cheng et al., 2015; Cho & Sobel, 1990; Ross, 1977; Thakor, 1990). Previous research has shown that assurance is one such signal (Cheng et al., 2015; Datar et al., 1991; Jensen & Meckling, 1976). The engagement of a cybersecurity assurance service by management, with the associated disclosure of results, can be understood as a

signal that increases confidence in the reliability of the related information security management system (Alon & Vidovic, 2015).

The literature suggests that source credibility plays a pivotal role in decision-making (Pornpitakpan, 2004; Schwarzkopf, 2006). According to source credibility theory, a source is more credible if it has greater expertise, greater competence, and greater trustworthiness (Birnbaum & Stegner, 1979; DeZoort et al., 2003; Pornpitakpan, 2004). Managers have a certain degree of discretion over what they choose to disclose. Because management holds more information than nonprofessional investors, these investors depend on credibility cues to evaluate the information disclosed to them. Disclosed information about a performed cybersecurity assurance can represent such a source of credibility (Martin, 2019; Mercer, 2004). A company might be less able to assess the quality of its cybersecurity system than an external assurance provider. Theoretically, this could be explained by the *bias blind spot*, which states that there is a tendency to view oneself with less bias than others (Scopelliti et al., 2015). Therefore, an external assurance provider is more likely to perform the assurance free of their own bias. In addition, external auditors are usually specialized in the offered assurance service and may have the advantage of experience, and they also are obliged follow the principles of the profession. Therefore, such assurance potentially increases the credibility of a company's cybersecurity management system. Consequently, stakeholders may perceive cybersecurity assurance positively and increase their willingness to invest.

So far, only a limited number of studies have been published in the context of cybersecurity assurance (Badawy, 2021; Frank et al., 2019; Navarro & Sutton, 2024; Perols, 2023; Perols & Murthy, 2021). In a 4×2 experiment with nonprofessional investors from Amazon's Mechanical Turk (MTurk), Frank et al. (2019) investigate the presence of a prior cyberattack in combination with a disclosed assessment regarding cybersecurity controls (no information, management assessed cybersecurity, cybersecurity assurance, both). Their results reveal that the disclosure of an independent cybersecurity assurance increases the investment attractiveness. Furthermore, the results are stronger if the company has disclosed a prior cyberattack. With an experiment, Perols and Murthy (2021) examine whether a joint or separate provision of cybersecurity assurance influences the willingness to invest, using business school graduate students as a proxy for nonprofessional investors. Their results indicate that, in the presence of a cybersecurity incident, investors are less likely to invest when the cybersecurity assurance is jointly (compared to separately) provisioned. Badawy (2021) experimented with students in Egypt as a proxy for nonprofessional investors to examine whether the provision of cybersecurity assurance by a Big 4 versus a non-Big 4 audit firm impacts the willingness to invest. Furthermore, they investigated whether the assurance level (limited vs. reasonable assurance) is relevant. The study revealed that the willingness to invest is significantly higher when the auditor belongs to a Big 4 company. Moreover, the assurance level is only then relevant if the assurance was engaged by the same type of audit firm. Using a $2 \times 2 + 1$ experiment with students as a proxy for nonprofessional investors, Perols (2023) examines the impact of cybersecurity assurance on the participants' willingness to invest. The author manipulates the comprehensiveness (less vs. more) of

the cybersecurity assurance and the presence of a cyber incident (no vs. yes) and uses a control group in which none of both manipulations were present. The author finds that the mere presence of cybersecurity assurance is useful in investment decision-making. Furthermore, investors are more willing to invest if the cybersecurity assurance is more comprehensive, but only if the occurrence of a cyber incident precedes. Using an experimental approach, Navarro and Sutton (2024) conducted a study with US nonprofessional investors from MTurk and investigate how voluntary assurance on cybersecurity risk management influences judgments and decision-making after the disclosure of a cyber incident. Additionally, they manipulate whether the company's decision to engage an assurance provider is consistent or inconsistent with industry practices. They find that nonprofessional investors evaluate companies with cybersecurity assurance more favorably in terms of management credibility, which leads to a higher share valuation. Furthermore, they find that investors reward (penalize) companies that engage (do not engage) cybersecurity assurance when it is not expected (expected). Moreover, Quick and Gauch (2022) performed a related experimental study in the context of voluntary assurance on the risk management system with German bankers as participants and find a positive impact on the likelihood of granting a loan, as well as on share purchase recommendations. However, neither the assurance level nor the assurance provider seems to have impacted the results, as the mere presence of the assurance was sufficient.

In addition to the positive effects mentioned, some assumptions may indicate that cybersecurity assurance does not impact investors' investment decisions. Cybersecurity assurance cannot completely prevent cyber risks; it can only reduce their likelihood. Therefore, report addressees might still perceive a high cyber risk regardless of an assurance. Furthermore, shareholders have little experience with cybersecurity assurance disclosure, as this disclosure content is rarely published in practice (Quick & Gauch, 2022; Schoenfeld, 2024). Therefore, shareholders may not appreciate this information.

To sum up, signaling theory implies that a cybersecurity assurance is a signal to company's stakeholders to elucidate risk management measures. Management can, therefore, require an independent and voluntary cybersecurity assurance service so that the company signals the credibility of the cybersecurity management system. As described above, numerous empirical research results indicate a positive impact of assurance services (e.g., Frank et al., 2019; Navarro & Sutton, 2024; Perols, 2023). Whereas those studies examine cybersecurity assurance in the context of a cyber incident, this study focuses on the impact of such assurance services during times of normal business operations. Therefore, it remains an open question whether cybersecurity assurance without a preceding incident impacts investment decisions. However, in light of the theories and prior research, we assume that cybersecurity assurance also has a positive impact on non-professional investors' willingness to invest during stable business operations, and thus we formulate our first hypothesis as follows:

HYPOTHESIS 1 (H1). *During stable business operations, nonprofessional investors are more willing to invest in a company if it has obtained a cybersecurity assurance service.*

Insurance Against Cyber Risks

Agency theory and signaling theory may be suitable approaches for explaining a preference for cyber insurance by nonprofessional investors.

Companies have a broad scope of risk management measures, including the purchase of insurance contracts. Such contracts allow companies to transfer and efficiently distribute risks to third parties (Bodin et al., 2018; Krummaker, 2019; Mayers & Smith, 1982). In the event of a claim, the insurance company covers the loss up to the sum insured. Consequently, the financial loss for the company, and thus also for the stakeholders, is minimized.

Agency conflicts arise from shareholder–manager conflicts of interest (Jensen & Meckling, 1976) and occur when information is asymmetrically distributed, and management takes actions to maximize its benefits at the expense of total shareholder wealth (Shleifer & Vishny, 1997; Watts & Zimmerman, 1990). Signaling—that is, the intentional disclosure of information as a signal to the market (Spence, 1973)—reduces information asymmetries and potentially increases trust in a company. Thus, it may explain why nonprofessional investors perceive insurance against cyber risk positively. Voluntary disclosure of such an insurance policy signals that the company is aware of the cyber risk and therefore takes measures to transfer the risks to the insurance company to protect the nonprofessional investors' invested assets. Monitoring is another means to reduce agency problems, and insurance companies can monitor management activities more effectively than shareholders (Mayers & Smith, 1982). Before issuing the insurance policy, the insurance company analyzes the company to be insured. Relevant customer factors that influence the risk will be included. In addition, insurance companies require detailed information from the company that is relevant to determining premiums. Once an insurance policy is issued, monitoring is conducted based on the coverage and under the policy's contractual framework (Holderness, 1990). Monitoring conducted by insurance companies can ensure that, for example, the management applies appropriate measures to monitor cyber risks or make related investments (Ashby & Diacon, 1998).

Prior research regarding cyber insurance has investigated a wide range of topics, such as demand for cyber insurance, insurability, and the cyber insurance market.

Using a survey among corporate professional decision-makers, de Smidt and Botzen (2018) find that, while the overall awareness of cyber risk and the perceived probability is high, the impact of a cyber incident is underestimated. Therefore, the decision-makers are reluctant to insure for cyber risk. Likewise, various authors have addressed the insurability of cyber risks. Biener et al. (2015) argue that the randomness of loss occurrence and the lack of reliable data on cyber losses are major challenges for the insurance sector. Similarly, Eling and Schnell (2016) illustrate the immense obstacles to insuring cyber risk, mainly due to a lack of data and modeling approaches. Eling et al. (2021) further elaborate that potential risk accumulation is a key issue, as all insured entities could be affected by the same cyber loss event (e.g., the WannaCry virus).

In 2015, a study by the UK government claimed that the UK cyber insurance market was in its infancy (HM Government, 2015). Over time, this has changed, and the

insurance market value has increased heavily (Mott et al., 2023). In considering the UK cyber insurance market, Mott et al. (2023) identify that ransomware attacks have significantly contributed to the “hardening” of the cyber insurance market, affecting nearly all market levels. Such hardening has helped raise security standards. However, it has also created a situation where some companies may not be able to acquire viable cyber insurance at all.³ In light of the hardening of the insurance market, a study by Bodin et al. (2018) introduces a model for selecting an optimal cyber insurance policy for organizations when one or more insurance companies offer a finite number of policies.

Shackelford (2012) argues that firms must proactively manage cybersecurity. The author suggests purchasing cyber insurance, emphasizing that, in addition to an essential investment in cybersecurity infrastructure, transferring risk to insurance companies may satisfy future expectations of investors and regulators.

Marotta et al. (2017) summarize the positive effects of cyber insurance apart from the primary purpose of transferring cyber risks: companies might increase their investments in their cyber protection to reduce their premiums. Furthermore, purchased cyber insurance may serve as an indicator of the quality of the cybersecurity. Besides that, cyber insurance might improve societal welfare by improving an overall level of cyber protection. Finally, cyber insurance can drive the adoption of advanced cybersecurity standards, as compliance with these standards helps insurers assess risk exposure more adequately.

To the best of our knowledge, there has been no research on the impact of cyber insurance on the decisions of nonprofessional investors.

As discussed above, agency theory and signaling theory underline the need of companies and investors for corporate insurance. The monitoring function of investors is transferred to the insurance company. However, the main purpose of insurance is to transfer risk. In the event of a claim, the sum insured is paid out to the company, which in turn minimizes the financial damage for the company and, thus, for the shareholders. Consequently, purchasing cyber insurance can be a positive signal for nonprofessional investors. Given this theoretical background, we assume that insurance against cyber risks positively impacts nonprofessional investor decisions, and we thus formulate our second hypothesis as follows:

HYPOTHESIS 2 (H2). *During stable business operations, nonprofessional investors are more willing to invest in a company if it has purchased insurance against cyber risks.*

Interaction

Reconsidering H1 and H2, we suggest a positive impact on the willingness to invest if the company has demanded a cybersecurity assurance service or has invested in

3. For more information regarding the cyber insurance market in different countries, see Franke (2017) for Sweden, Başı et al. (2019) for Norway, and Strupczewski (2017) for Poland.

insurance against cyber risks. In practice, there is a demand for both assurance services and corporate insurance.

Anecdotal evidence from interviews with large international insurers and audit firms suggests that both the cyber insurance market and the assurance market are growing. In the United Kingdom, the cyber insurance market was in its infancy in 2015 (HM Government, 2015) but has grown considerably since then (Mott et al., 2023). Regarding cybersecurity assurance, Schoenfeld (2024) finds that only about 29% of S&P 500 companies have commissioned such assurance. Quick and Gauch (2022) show that the largest German companies rarely disclose cybersecurity assurance or insurance against cyber risks in annual reports. The lack of disclosure may be due to companies not taking the measures or not reporting on them. Furthermore, the assurance and insurance market supply suggest that these services are regularly demanded. A lack of data does not allow a more precise assessment.

However, companies do not necessarily restrict themselves to just one of these instruments, but rather they frequently take both options. From this perspective, the question of how they interact in combination arises. A cybersecurity assurance increases the credibility of the management system and reduces the risk and likelihood that a cybersecurity incident will occur. In contrast, insurance against cyber risks transfers the risk to the insurance company and reduces the potential financial damage of an incident. Reducing the impact and the likelihood are two different risk management strategies. Therefore, an additive effect may follow. However, a substitutive effect may also be observed, such that nonprofessional investors perceive assurance as just as good as an insurance policy. The simultaneous presence of both mechanisms may then be considered unnecessary, and only one may be regarded as sufficient. Therefore, we formulate the following research question:

RESEARCH QUESTION. *Do cybersecurity assurance and insurance against cyber risk have a joint effect on nonprofessional investors' willingness to invest?*

3. EXPERIMENTAL DESIGN AND METHOD

Experimental Design

To test our hypotheses, we performed an online experiment using a 2×2 between-subjects design. Our two independent variables were cybersecurity assurance (assurance vs. no assurance) and insurance purchase against cyber risks (yes vs. no). The experimental materials were developed in English and provided to the participants. The research project was approved by the institutional review board of the authors' university. One auditor checked the case for realism and made minor changes. We conducted 15 pretests with nonprofessional investors to check plausibility, comprehension, and time duration, which resulted in some editing of the case description and minor linguistic changes.

Participants

We used G*Power to calculate an appropriate minimum number of participants, and we expected a medium effect size.⁴ Because of the expected comprehension check failures, we decided to recruit 200 nonprofessional investors as participants using the online participant pool Prolific. Prolific is designed to recruit participants for academic research. Previous comparisons of Prolific and similar platforms showed that participant quality is at least equivalent to other alternatives (Palan & Schitter, 2018; Peer et al., 2017).

We restricted our sample to participants who have already invested in shares and can, therefore, be classified as nonprofessional investors. Our participants currently reside in the United Kingdom. Although our experimental case describes a German company, we made this decision as foreign shareholding is typical for German companies. More than half of the shares of the largest listed German companies are in foreign hands (Deutsche Bundesbank, 2014). Furthermore, the number of potential participants from the United Kingdom is high enough to ensure high data quality. Finally, holding the country constant allowed us to control for the same cultural and economic background.

We paid participants 0.90 Great Britain Pounds (GBP) for completing the experiment. In addition, participants could receive a bonus of 0.30 GBP if they passed the comprehension checks.⁵ This information was available in advance to further motivate the participants to work correctly. The average time participants spent on this experiment was 6 min, 36 s. The data collection took place in December 2022.

Task and Procedure

Participants in the experiment were randomly assigned to the conditions. The participants were informed about adherence to the German Research Foundation guidelines, privacy policy, and participant rights.

We asked participants to take part in the experiment based on their experiences and expectations as nonprofessional investors. Initially, we provided participants with the scenario that they own a portfolio of shares and are considering investing in an e-commerce company. After receiving an excerpt from an annual report, they answered some case-related questions, comprehension checks, and provided demographic information.

The case description informed participants about the hypothetical company “BestProducts AG,” which operates in the e-commerce sector. The text contained information about products, markets, subsidiaries, and the number of employees. Information on the current business situation, compared to the previous year, was presented in a table using key financial figures (net sales, equity ratio, earnings before interest and taxes). Further information on the audit of the consolidated financial statements and management

4. G*Power is a power analysis program for many statistical tests used in the social and behavioral sciences. Using this open-source software, we calculated a total sample size of 101 participants. The inserted values were effect size $f = 0.25$, $\alpha = 0.10$, $\beta = 0.80$, $df = 1$, groups = 4.

5. This procedure is recommended by Buchheit et al. (2018) because such a payment is particularly important for participants from participant pools.

report, and the declaration of conformity with the German Corporate Governance Code, followed. In addition, an excerpt from the risk and opportunity report was provided, in which the manipulation (i.e., cybersecurity assurance and cyber risk insurance) was reported. In practice, and therefore also in our experiment, the risk and opportunity report included a brief description of the risk management system and the presentation of significant risks. The impact of the risks and the measures taken to mitigate them must also be disclosed (i.e., cybersecurity assurance and cyber risk insurance) (Accounting Standards Committee of Germany, 2013). As is usual practice, risk matrices indicated the cyber risk assessed by the company regarding to financial impact and likelihood of occurrence for each condition. To ensure external validity, the case materials, including the shown risk matrices, are close to practice and represent a very realistic risk report (e.g., Fresenius Medical Care, 2023; Fuchs Petro Club, 2023; Hugo Boss, 2023; ProSiebenSat.1 Media, 2023).⁶ The experimental case can be found in the [Appendix](#).

Independent Variables

Two different manipulations were used. The first independent variable (*ASSURANCE*) refers to the engagement of a cybersecurity assurance provider and has two levels: assurance provision by an audit firm versus no assurance. We chose audit firms because they dominate this assurance market. The second independent variable (*INSURANCE*) addresses insurance purchase and is also manipulated at two levels: purchase of cyber risk insurance versus no insurance.

Dependent Variable

Similar to prior research (Asay et al., 2023), the dependent variable was the participants' willingness to invest (*WILLINGNESS*). Willingness to invest is the average of the two following items, which was already used by multiple studies (e.g., Elliott et al., 2018; Friedrich, 2021). We asked the participants about their perceptions of the investment attractiveness of the hypothetical company's shares (*ATT*: "How do you generally assess 'BestProducts AG' investment attractiveness?") as well as the likelihood of including shares in their diversified portfolio (*BUY*: "How do you assess the likelihood of including 'BestProducts AG' shares in your diversified portfolio?"). For all dependent variables, we applied a 7-point Likert scale (from 1 = *very low* to 7 = *very high*). The Cronbach's alpha for the two items is 0.925, above the 0.70 cutoff (Cortina, 1993).

Mediation Variable

Through cybersecurity assurance, the cybersecurity system potentially can be improved, reducing the likelihood of an incident. Such an effect requires an appropriate assurance of service quality, which is not guaranteed in the case of financial statement audits. A lack of independence or cybersecurity competence may mitigate positive effects. Besides that, the insurance hypothesis by Wallace (1980) suggests an insurance effect of

6. To ensure a realistic scenario, the German Prime Standard's companies from 2020 were examined to create a realistic case.

voluntary assurance. Voluntary assurance mitigates a company’s legal liability by demonstrating professional care and utilizing the auditor’s legal expertise. Furthermore, the auditor’s liability exposure motivates auditors to apply professional care to argue against allegations of negligence in a litigation setting, thereby potentially increasing assurance quality (Navarro & Sutton, 2024; Wallace, 1980, 2004).⁷ Furthermore, cyber risk insurance aims to transfer the cyber risks to an insurance company that compensates the company when there is an incident, thereby reducing the company’s financial impact. Using the general definition of risk, we can also explain a possible change in the perceived level of risk. A risk is defined as the probability of occurrence times the financial impact (Marotta et al., 2017). Whereas a cybersecurity assurance might reduce the probability of occurrence, cyber insurance reduces the financial impact. That is why we assume that both measures reduce participants’ perceptions of risk. To gain insights into the decision process of our participants, we used *RISK* for a mediation analysis. The variable *RISK* was measured on a 7-point Likert scale (from 1 = *very low* to 7 = *very high*) by asking the participants to assess the company’s cyber risk (*RISK*: “How do you assess the risk situation regarding the IT & cyber risks of ‘BestProducts AG?’”).

4. RESULTS

Comprehension Checks and Final Sample

In total, 200 UK nonprofessional investors recruited from Prolific participated in the experiment.⁸ The final sample per experimental condition is shown in Table 1. Eight participants had to be excluded from the analysis because they spent less time reading the case material than a very fast reader would need to process all information.

The experiment included two comprehension checks (*CC*), which aimed to check whether the participants had correctly read the experimental case. The first question was

TABLE 1
Final number of participants per experimental condition

Experimental condition	Assurance	Insurance	Number of participants
1	—	—	23
2	—	✓	23
3	✓	—	27
4	✓	✓	27
Total			100

Notes: This table reports the composition of the experimental conditions and the number of participants per experimental condition.

7. A detailed theory discussion of Wallace’s (1980, 2004) insurance hypothesis can be found in Navarro and Sutton (2024).

8. We performed the same experiment with undergraduate and graduate business students without any significant findings. This indicates that the use of business students to proxy nonprofessional investors may be ill advised in the European environmental setting.

to test whether the participants had correctly observed the provision of cybersecurity assurance (*CC1*: “Has ‘BestProducts AG’ engaged a cyber security assurance and certification?”). The possible answers were “yes” or “no”; 72 participants did not pass this comprehension check. The second question was to check whether the participants correctly indicated a reported insurance (*CC2*: “Has ‘BestProducts AG’ purchased insurance against IT & cyber risks?”). The possible answers were again “yes” or “no”; 20 participants did not pass this comprehension check.

In total, 92 of the 192 participants failed the comprehension checks. This resulted in a failure rate of 47.9%.⁹ However, we repeated all analyses with all 200 (resp., 192) participants, and the results remained unchanged. Nevertheless, we describe the results after the exclusion of comprehension check failures. In sum, 100 participants remained in the final sample.

Descriptive Statistics

Table 2 provides demographic information that was requested in a post-experimental questionnaire. The largest group of participants is between 36 and 45 years old. Most participants are male ($N = 67$) and typically have a bachelor’s ($N = 43$) degree. The mean number of years for which the participants have held shares is more than 10 years (*SHARE*; mean = 10.21; median = 6; range = 1–40), which indicates that our participants are nonprofessional investors. Self-assessed general expertise in investing in shares (*KNOW_SHARE*), annual reports (*KNOW_AR*), and IT security (*KNOW_IT*) is moderate, with a mean value of 3.73, 3.67, and 3.72, respectively. The self-assessed general trust in audit firms (*TRUST_AF*) has a mean value of 3.85. The self-assessed risk appetite for investment decisions (*RISK_APPETITE*) has a mean value of 4.35. The response scale for these demographic questions ranges from 1 (*very low*) to 7 (*very high*).

Hypothesis Testing

To examine the impact of cybersecurity assurance and cyber risk insurance on nonprofessional investor willingness to invest, we conducted several *t*-tests (Table 3, Panel A), a full-factorial ANOVA¹⁰ (Table 3, Panel B), and contrast analyses (Table 3, Panel C). To gain further insights, we applied pairwise comparisons between all experimental conditions (Table 3, Panel D). In addition, Figure 1 shows the graphical results of the experiment for the dependent variable.

9. The failure rate for our comprehension checks is in line with those discussed in prior research on electronic survey methods (e.g., Andrews et al., 2003; Oppenheimer et al., 2009). Furthermore, other experimental studies reported similar failure rates—for example, Cheng et al. (2015), 35% (2×2 design); Brown-Liburd and Zamora (2015), 46% ($2 \times 2 \times 2$ design); Sheldon and Jenkins (2020), 42% (2×3 design); and Quick and Gauch (2021), 40% ($2 \times 2 + 1$ design).

10. Because of the violation of ANOVA conditions (normally distributed data and homogeneous variances), we performed a Scheirer–Ray–Hare Test, the non-parametric alternative. The findings confirm the ANOVA results.

TABLE 2
Demographic information

<i>AGE</i> in years	≤25	26–35	36–45	45–55	56–65	≥66
<i>N</i>	9	28	30	12	15	6
<i>GENDER</i>		Male		Female		Diverse
<i>N</i>		67		33		0
<i>SCHOOL</i>	Middle school	High school	Bachelor's	Diploma, master's		PhD
<i>N</i>	0	29	43	23		5
Variable	<i>N</i>	Mean	SD	Min	Max	Median
<i>SHARE</i>	100	10.21	9.38	1	40	6
<i>KNOW_SHARE</i>	100	3.73	1.38	1	7	4
<i>KNOW_AR</i>	100	3.67	1.48	1	7	4
<i>KNOW_IT</i>	100	3.72	1.69	1	7	3
<i>TRUST_AF</i>	100	3.85	1.66	1	7	3
<i>RISK_APPETITE</i>	100	4.35	1.42	1	7	5

Notes: *AGE* is the age of the participants (1 ≤ 25, 2 = 26–35, 3 = 36–45, 4 = 46–55, 5 = 56–65, 6 ≥ 66); *GENDER* is the gender of the participants (1 = female, 2 = male, 3 = diverse); *SCHOOL* is the highest level of education (1 = middle school, 2 = high school, 3 = bachelor's, 4 = diploma, master's, 5 = PhD); *SHARE* is the number of years the participants have been holding shares; *KNOW_SHARE* is the self-assessed knowledge of investment in shares on a 7-point Likert scale; *KNOW_AR* is the self-assessed knowledge of annual reports on a 7-point Likert scale; *KNOW_IT* is the self-assessed knowledge of IT and cybersecurity on a 7-point Likert scale; *TRUST_AF* is the self-assessed trust in audit firms on a 7-point Likert scale; and *RISK_APPETITE* is the self-assessed appetite for risk in investment decisions on a 7-point Likert scale. All Likert scales were labeled from 1 (*very low*) to 7 (*very high*).

Table 3 (Panel A) and Figure 1 show the results for the dependent variable *WILLINGNESS*—that is, participant willingness to invest in the company's shares. The means from Table 3, Panel A (also shown in Figure 1), meet our expectations. Regarding the engagement of a cybersecurity assurance provider, the mean values are higher if an assurance service was performed. Also, the mean values regarding insurance were higher if the company purchased cyber risk insurance. Regarding the *t*-test, the results show that the engagement of cybersecurity assurance (*t*-value = 3.250; *p*-value = 0.000) as well as the insurance purchase (*t*-value = 2.195; *p*-value = 0.015) have a statistically significant impact on the dependent variable *WILLINGNESS*.

Table 3, Panel B, shows the results for the ANOVA.¹¹ Both independent variables, *ASSURANCE* and *INSURANCE*, are statistically significant (*F*-value = 11.907; *p*-value = 0.000, resp., *F*-value = 5.622; *p*-value = 0.020). These two significant main effects support H1 and H2. In contrast, the ANOVA interaction term *ASSURANCE*×*INSURANCE* is not statistically significant (*F*-value = 0.719; *p*-value 0.399). Together with the pattern of results seen in Figure 1, this indicates that the

11. Reconsidering the two items *ATT* and *BUY*, we find similar results if we run their ANOVAs separately.

TABLE 3
Results for the dependent variable *WILLINGNESS***Panel A:** Descriptive statistics for *WILLINGNESS* for each experimental cell

	Assurance	No Assurance	<i>t</i> -value (<i>p</i> -value)	Row means
Insurance	5.611 (0.764) <i>N</i> = 27	4.978 (1.310) <i>N</i> = 23	2.195 (0.015**)	5.320 (1.087) <i>N</i> = 50
No Insurance	5.241 (1.004) <i>N</i> = 27	4.196 (1.677) <i>N</i> = 23		4.760 (1.440) <i>N</i> = 50
<i>t</i> -value (<i>p</i> -value)		3.250 (0.000***)		
Column means	<i>N</i> = 54 5.426 (0.903)	<i>N</i> = 46 4.587 (1.539)		

Panel B: ANOVA results with *WILLINGNESS* as the dependent variable

	Type III sum of squares	df	<i>F</i> -value	<i>p</i> -value	Partial η^2
Intercept	2490.404	1	1696.069	0.000***	0.946
<i>ASSURANCE</i>	17.484	1	11.907	0.000***	0.110
<i>INSURANCE</i>	8.255	1	5.622	0.020**	0.055
<i>ASSURANCE</i> × <i>INSURANCE</i>	1.055	1	0.719	0.399	0.007
Residuals	140.961	96			
<i>N</i> = 100					
Adjusted $R^2 = 0.131$					

Panel C: Contrast analyses for *WILLINGNESS*

Source of variance	df	<i>F</i> -value	<i>p</i> -value
Contrast 1: [-3, 1, 1, 1] for [1, 2, 3, 4]	1	14.077	0.000***
Residual between-cell variance	2	1.944	0.1487
Total between-cell variance	3	5.989	0.000***
$q^2 = 0.207$			
Contrast 2: [1, 1, 1, -3] for [1, 2, 3, 4]	1	8.712	0.004***
Residual between-cell variance	2	4.267	0.012**
Total between-cell variance	3	5.989	0.000***
$q^2 = 0.527$			
Contrast 3: [0, 1, 1, -2] for [1, 2, 3, 4]	1	2.998	0.086*
Residual between-cell variance	2	7.484	0.001***
Total between-cell variance	3	5.989	0.000***
$q^2 = 0.840$			

Panel D: Pairwise comparisons (Tukey HSD)

	<i>p</i> -value
No Assurance and No Insurance (1) versus No Assurance and Insurance (2)	0.133
No Assurance and No Insurance (1) versus Assurance and No Insurance (3)	0.016**

(The table is continued on the next page.)

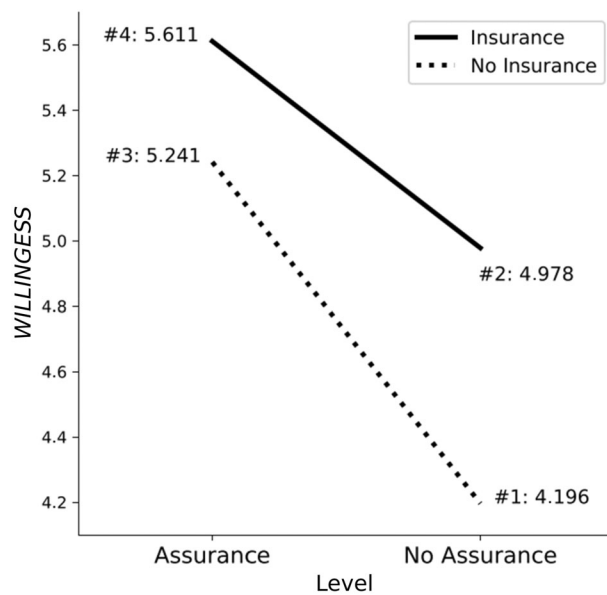
TABLE 3 (continued)

Panel D: Pairwise comparisons (Tukey HSD)

	<i>p</i> -value
No Assurance and No Insurance (1) versus Assurance and Insurance (4)	0.000***
No Assurance and Insurance (2) versus Assurance and No Insurance (3)	0.871
No Assurance and Insurance (2) versus Assurance and Insurance (4)	0.261
Assurance and No Insurance (3) versus Assurance and Insurance (4)	0.676

Notes: This table reports the results for the dependent variable *WILLINGNESS*, which is the average of the two items *ATT* and *BUY* (*ATT*, “How do you generally assess ‘BestProducts AG’ investment attractiveness?” and *BUY*, “How do you assess the likelihood of including ‘BestProducts AG’ shares in your diversified portfolio?”). Both items were measured on a 7-point Likert scale from 1 (*very low*) to 7 (*very high*). Panel A reports the mean, standard deviation (in parentheses), and the number of observations for each experimental cell, as well as *t*-test results for a comparison between the two mentioned factor levels. Panel B presents the results of a full-factorial ANOVA with the factors *ASSURANCE* (yes vs. no) and *INSURANCE* (yes vs. no), and the interaction term (*ASSURANCE*×*INSURANCE*). Panel C reports the contrast analyses with the given weights. Panel D reports the Tukey HSD results comparing all cells. The numbers in parentheses indicate the number of the condition. All *p*-values are two-tailed. *, **, and *** represent significance levels of 10%, 5%, and 1%, respectively.

FIGURE 1 Graphical results for *WILLINGNESS*



Notes: This figure depicts the graphical results for *WILLINGNESS*. The *x*-axis indicates whether a cybersecurity assurance was performed, and the *y*-axis shows the participants’ assessment regarding the dependent variable *WILLINGNESS*. The dashed line reflects the case without insurance against cyber risk, and the solid line reflects the case with insurance against cyber risk. The given values indicate the mean values. *WILLINGNESS* is the average of the two items *ATT* and *BUY* (*ATT*, “How do you generally assess ‘BestProducts AG’ investment attractiveness?” and *BUY*, “How do you assess the likelihood of including ‘BestProducts AG’ shares in your diversified portfolio?”). Both items are measured on a 7-point Likert scale from 1 (*very low*) to 7 (*very high*). Condition numbers are indicated as follows: #1, No Assurance and No Insurance; #2, No Assurance and Insurance; #3, Assurance and No Insurance; and #4, Assurance & Insurance.

two effects are additive. Regarding the effect size, Panel B of Table 3 shows, besides significant p -values, a partial η^2 for *ASSURANCE* of 0.110 (converted into Cohen's $f = 0.35$), resp. 0.055 (converted into Cohen's $f = 0.24$) for *INSURANCE*. These results reveal a medium effect size according to Cohen (1988), indicating a practical relevance of our results.

To investigate our research question regarding the interaction, we performed relevant contrast analyses with the given weights (Table 3, Panel C) (Buckless & Ravenscroft, 1990; Guggenmos et al., 2018). The result of contrast 1 indicates that the condition where a cybersecurity assurance and insurance against cyber risk is not present differs significantly from the other groups (F -value = 14.077; p -value = 0.000), demonstrating that any measure is better than no measure. Contrast 2 tested whether both measures—that is, cybersecurity assurance in combination with insurance against cyber risks—are different from the other groups. The results reveal a significant difference (F -value = 8.712; p -value = 0.004). Because the results might be driven from the group without both measures, we conducted contrast 3 with custom weights [0, 1, 1, -2] as Guggenmos et al. (2018) suggest. Contrast 3 does not provide evidence that a combination of both assurance and insurance increases the willingness to invest as the difference is not significant at traditional levels (F -value = 2.998; p -value = 0.086), while the residual between-cell variance is significant (F -value = 7.484; p -value = 0.001), indicating that the contrast does not describe the data well in that it fails to explain 84% of the explainable variance.

The results of the post hoc tests (Table 3, Panel D) only reveal statistically significant differences between experimental conditions 1 versus 3, as well as between 1 versus 4, which is consistent with our expectations. Considering the results of the Tukey honestly significant different (HSD) pairwise comparisons in Table 3, Panel D, we find a significant difference between condition 1 (No Assurance and No Insurance) and condition 3 (Assurance and No Insurance), as well as between condition 1 (No Assurance and No Insurance) and condition 4 (Assurance and Insurance), suggesting that there is a positive impact between willingness to invest, but only if an assurance is present. This partly confirms the results of contrast 1.

To ensure that our results are not biased by participant characteristics that vary systematically across cells despite random selection, we additionally performed an ANCOVA. Initially, we computed the correlations between the dependent variable and demographic variables. The dependent variable, *WILLINGNESS*, is statistically significantly correlated with the demographic variable *AGE* (coefficient = 0.191; p -value = 0.057). This statistically significantly correlated demographic variable was then added as covariate.

In general, the ANCOVA results (Table 4) are consistent with the ANOVA results. The covariate *AGE* is not statistically significant (F -value = 2.359; p -value = 0.128); therefore, *AGE* does influence the willingness to invest.

Supplementary Analysis

The results of our main analysis reveal that cybersecurity assurance and insurance against cyber risk increase the willingness to invest. We use a structural equation model to gain further insights into our participants' decision process.

TABLE 4
ANCOVA result for the dependent variable *WILLINGNESS*

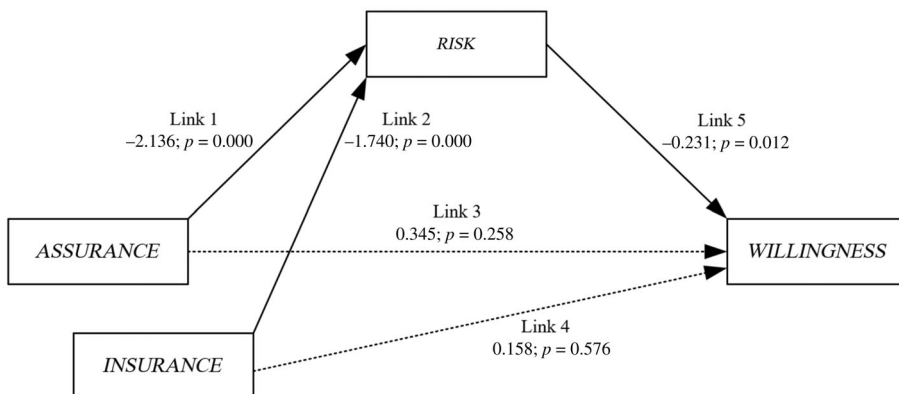
	Type III sum of squares	df	F-value	p-value	Partial η^2
Intercept	329.706	1	227.722	0.000***	0.706
<i>ASSURANCE</i>	16.155	1	11.158	0.001***	0.105
<i>INSURANCE</i>	6.832	1	4.719	0.032*	0.047
<i>ASSURANCE</i> × <i>INSURANCE</i>	1.245	1	0.860	0.356	0.009
<i>AGE</i>	3.415	1	2.359	0.128	0.024
Residuals	137.545	1			

N = 100
Adjusted R^2 = 0.143

Notes: This table reports the ANCOVA results for the dependent variable *WILLINGNESS*, which is the average of the two items *ATT* and *BUY* (*ATT*, “How do you generally assess ‘BestProducts AG’ investment attractiveness?” and *BUY*, “How do you assess the likelihood of including ‘BestProducts AG’ shares in your diversified portfolio?”). Both items were measured on a 7-point Likert scale from 1 (*very low*) to 7 (*very high*). *AGE* is the age of the participants (1 ≤ 25, 2 = 26–35, 3 = 36–45, 4 = 46–55, 5 = 56–65, 6 ≥ 66). All *p*-values are two-tailed. *, **, and *** represent significance levels of 10%, 5%, and 1%, respectively.

Figure 2 demonstrates the structural equation model. The binary independent variable *ASSURANCE* was coded with no cybersecurity assurance (equal to zero) and cybersecurity assurance (equal to one). Similarly, *INSURANCE* was coded with no insurance (equal to zero) and insurance against cyber risk (equal to one). *RISK* was included as a mediator and measured risk perception regarding the cyber risk on a 7-point Likert scale. The structural equation model results reveal that neither *ASSURANCE* nor *INSURANCE*

FIGURE 2 Structural equation model



Notes: This figure depicts the structural equation model for the experiment. The model contains *ASSURANCE* and *INSURANCE* as independent variables, *RISK* as a mediator, and *WILLINGNESS* as the dependent variable. Solid lines indicate a significant relationship, whereas dotted lines indicate a nonsignificant relationship. Every link reports the coefficient and the corresponding *p*-value (two-tailed). The model-fit measures were used to assess the model’s overall goodness to fit: the comparative fit index (1.000; above the generally accepted minimum value of 0.95, Byrne, 2013) and the root mean square error of approximation (0.000; below the 0.05 value indicating a good fit, MacCallum et al., 1996).

directly affects *WILLINGNESS* (Link 3; Link 4). However, Link 1, Link 2, and Link 5 show significant *p*-values. A cybersecurity assurance reduces the perceived risk (Link 1; coefficient = -2.136 ; *p*-value = 0.000), and, similarly, an insurance against cyber risk (Link 2; coefficient = -1.740 ; *p*-value = 0.000) reduces the perceived level of risk. Link 5 demonstrates that a higher perceived risk decreases the willingness to invest (Link 5; coefficient = -0.231 ; *p*-value = 0.012). Therefore, the model shows that if *ASSURANCE* or *INSURANCE* decreases the perceived level of risk, *WILLINGNESS* will increase.

The mean values and the pairwise comparisons regarding all experimental conditions are shown in Table 5, Panels A and B. The pairwise comparisons reveal that only the difference between conditions 2 and 3 is not significant (No Assurance and Insurance vs. Assurance and No Insurance).

To sum up, the results from the structural equation model reveal that both cybersecurity assurance and insurance against cyber risk increase the willingness to invest by reducing the company's perceived risk. However, there is no interaction between cybersecurity assurance and insurance against cyber risk.

Additional Experiment

It is not only the mere presence of cybersecurity assurance that might influence the decision of nonprofessional investors, but also the type of assurance provider. Therefore, we

TABLE 5
Means of the mediator *RISK* and pairwise comparisons

Panel A: Means of <i>RISK</i>		
	Experimental condition	Mean <i>RISK</i>
1	No Assurance and No Insurance	6.525
2	No Assurance and Insurance	4.565
3	Assurance and No Insurance	4.185
4	Assurance and Insurance	2.630
Panel B: Pairwise comparisons (Tukey HSD)		
Conditions		<i>p</i> -value
No Assurance and No Insurance (1) versus No Assurance and Insurance (2)		0.000***
No Assurance and No Insurance (1) versus Assurance and No Insurance (3)		0.000***
No Assurance and No Insurance (1) versus Assurance and Insurance (4)		0.000***
No Assurance and Insurance (2) versus Assurance and No Insurance (3)		0.724
No Assurance and Insurance (2) versus Assurance and Insurance (4)		0.000***
Assurance and No Insurance (3) versus Assurance and Insurance (4)		0.000***

Notes: This table reports the means (Panel A) of the mediator *RISK* per experimental condition and the pairwise comparison between the given groups using the Tukey HSD test (Panel B). *RISK* ("How do you assess the risk situation regarding the IT & cyber risks of 'BestProducts AG?") was measured on a 7-point Likert scale from 1 (*very low*) to 7 (*very high*). All *p*-values are two-tailed. *, **, and *** represent significance levels of 10%, 5%, and 1%, respectively.

examine whether different assurance providers influence the results in a second experiment. There are other assurance providers available in the market besides audit firms. A study by the International Federation of Accountants (2021) reveals that 37% of companies worldwide chose an alternative assurance provider regarding ESG report assurance. Results from the United States and United Kingdom show that the market share of other service providers is considerably higher (90% and 50%, respectively). In addition, the Corporate Sustainability Reporting Directive allows member states to permit third-party providers for sustainability report assurance, which should minimize the risk of greater market concentration among auditors (European Union, 2022). A wider range of assurance providers consequently raises the question of their potential influence. In Germany, the technical control board (TCB) is frequently used as an alternative to public accountants for assurance provision. It offers various services, such as product inspections, data security, and technical approvals. That is why it seems obvious that companies also choose alternative assurance providers to assure their cybersecurity systems. There might be different reasons to do so, which is why it seems necessary to investigate the impact of different assurance providers.

Differences in nonprofessional investors' perceptions of assurance provided by different organizations may be theoretically explained by the theory of professions and the source credibility theory. According to the theory of professions, auditors belong to a profession. The theory provides guidance about the dynamics of professional groups. For example, formal education and training—which is controlled by a professional body and often results in a certification (which in turn serves as an entry requirement) and a systematic knowledge base—is an essential feature of many professions (Canning & O'Dwyer, 2001; Chen & van Akkeren, 2012). Therefore, a profession is recognized as an authority that has distinct credibility within its domain. Another distinguishing trait is that the practitioners work in accordance with ethical codes—that is, with specific norms, values, and expectations concerning personal conduct. Professional standards of practice and ethics are typically agreed upon and maintained through widely recognized professional associations. In addition, an organized private-sector professional association supervises and evaluates public accountants and exercises effective disciplinary action against those with inadequate performance. A final feature of a profession is that it exists because it is functional for society and enjoys public trust, and its members apply their knowledge and skills in an altruistic and ethical manner (Ackroyd, 2016; Dent et al., 2016; Freidson, 1989; Saks, 2012).

In contrast, tech-based assurance providers may be perceived as superior with regard to risk assessments. According to source credibility theory, a source is more credible if it has greater expertise, greater competence, and greater trustworthiness (Birnbaum & Stegner, 1979; DeZoort et al., 2003; Pornpitakpan, 2004). Therefore, a tech-based assurance provider with high cybersecurity expertise might be perceived as more competent and may thus be associated with higher credibility of cybersecurity assurance services. Based on these two theories, it remains unclear which assurance provider is preferred by nonprofessional investors.

Again, using the online platform Prolific, we recruited 90 nonprofessional investors from the United Kingdom. We used the same case material as described in Experiment 1.

However, this time we provided the participants with only the scenario without insurance and did not provide a risk matrix (because of the constant risk in both scenarios). First, we used two comprehension checks to verify whether the participants had read the case correctly regarding the engagement of a cybersecurity assurance and regarding the assurance provider. In our final sample, 68 participants remained, which indicates a failure rate of 24.4%. Table 6 presents the mean values, standard deviations, and *t*-tests of the dependent variable, *WILLINGNESS*. Regarding the provider, the mean values are only marginally different and thus do not allow further interpretation. The *t*-test shows no significant difference (*t*-value = 0.098; *p*-value = 0.922). Second, we examined the *COMPETENCE* of the two different assurance providers as perceived by the participants. We asked them on a 7-point Likert scale with a response scale from 1 (*very low*) to 7 (*very high*) how competent they considered the assurance provider who provided the assurance service to be. The mean values for audit firm (mean = 5.640) and TCB (mean = 5.320) indicate that the participants perceive audit firms as more competent. However, this difference is not statistically significant (*t*-value = 1.067; *p*-value = 0.290).

5. DISCUSSION AND CONCLUSION

The increasing digitalization and interconnectedness of the economy have highlighted the importance of cybersecurity as a new dimension of risk management. Cyber risks are significant and have justifiably attracted the attention of stakeholders. External cybersecurity assurance can confirm the appropriateness and effectiveness of a cybersecurity system and can be used as a positive signal to stakeholders. Another way to manage cyber risk is the purchase of corporate insurance. Insurance can curb the financial loss of possible damage and serve as a special kind of monitoring on behalf of the stakeholders.

This experimental study investigated the impact of cybersecurity assurance and the purchase of corporate insurance covering cyber risk on nonprofessional investors' willingness to invest, using 100 nonprofessional investors. Participants were asked to assess the attractiveness of an investment and the likelihood of buying shares in a hypothetical

TABLE 6
t-test results for different assurance providers

<i>t</i> -test results for pairwise comparisons of the two providers (<i>t</i> -test)			
	Audit firm (<i>N</i> = 36)	TCB (<i>N</i> = 32)	<i>t</i> -value (<i>p</i> -value)
<i>WILLINGNESS</i>	5.181 (0.9721)	5.156 (1.073)	0.098 (0.922)
<i>COMPETENCE</i>	5.640 (1.175)	5.320 (1.249)	1.067 (0.290)

Notes: This table reports the means, standard deviation, and *t*-test results for the dependent variable *WILLINGNESS*, regarding the two assurance providers, as well as their assessed *COMPETENCE*. *WILLINGNESS* is the average of the two items *ATT* and *BUY* (*ATT*, “How do you generally assess ‘BestProducts AG’ investment attractiveness?” and *BUY*, “How do you assess the likelihood of including ‘BestProducts AG’ shares in your diversified portfolio?”). Both items were measured on a 7-point Likert scale from 1 (*very low*) to 7 (*very high*). *COMPETENCE* (“How competent was the auditor of the assurance?”) was also measured on a 7-point Likert scale. All *p*-values are two-tailed. *, **, and *** represent significance levels of 10%, 5%, and 1%, respectively.

company. Our results show that cybersecurity assurance increases the willingness to invest in shares. This is consistent with our theoretical expectation from signaling theory. Through cybersecurity assurance, the company can send a positive trust signal regarding risk treatment to its investors. Therefore, nonprofessional investors positively perceive risk reduction as a suitable measure. H1 can thus be confirmed. The purchase of cyber insurance also positively impacts the willingness to invest. This is also in line with our theoretical expectation driven by agency theory and transaction cost theory, which underlines the need for companies and investors to obtain corporate insurance. Insurance signals lower transaction costs and thus represents a special form of monitoring. Furthermore, a perfectly diversified portfolio does not exist. Hence, nonprofessional investors might perceive corporate insurance as a requirement for protecting their assets (i.e., shareholder value). H2 can thus be confirmed.

We stated a research question for the interaction effect since we have neither matching theories nor empirical findings for a possible direction. The ANOVA results do not indicate a statistically significant interaction. However, the results reveal an additive effect of both measures. Both measures themselves are beneficial for companies. Companies may consider using one or both measures to increase investor willingness to invest.

An additional experiment was performed to examine the impact of different assurance providers. Although the audit firms were considered more competent, no statistically significant difference was observed. While audit firms could be perceived as more competent regarding assurance services, the TCB could be attributed with a higher level of technical experience and competence. Thus, it can be concluded that the specific assurance provider is irrelevant to our participants, and it is only important that a cybersecurity assurance was performed.

The results of our study are of interest to regulators, companies, insurance companies, and assurance providers. From a regulatory perspective, due to the high relevance of cyber risks, introducing mandatory cybersecurity assurance and/or mandatory cyber risk insurance may be considered. However, with regard to the United States, the SEC does not mandate such assurance services, which suggests that the SEC has not determined that the benefits outweigh the costs (Schoenfeld, 2024).

Furthermore, companies could consider voluntarily engaging an assurance provider, which potentially increases company attractiveness as an investment for equity investors. However, managers must individually weigh the costs and benefits of such an assurance service (Schoenfeld, 2024). Assurance providers can learn from our findings that shareholders of potential clients perceive their cybersecurity assurance services positively and, therefore, the provider might consider expanding its supply (e.g., training, marketing). Annual report users should benefit from the study through learning that such information can be relevant. For insurance companies, our results indicate a demand for cyber insurance.

While most studies examine cybersecurity assurance experimentally in the context of a cyber incident (Frank et al., 2019; Navarro & Sutton, 2024; Perols, 2023; Perols & Murthy, 2021), this study analyzes the impact of such assurance services in times of

normal business operations. Therefore, the study contributes to the existing literature by highlighting the potential benefits of seeking assurance and disclosing relevant information, even in the absence of a cyber incident. Furthermore, our study analyzes whether the type of assurance provider impacts investors' decisions. In the context of assurance on sustainability reports, prior research predominantly reveals that assurance provided by audit firms has superior effects. However, these findings are not generalizable to the provision of cybersecurity assurance, which requires in-depth expertise in IT. We failed to reveal significant differences between assurance provision by audit firms and by a technological assurance provider, indicating that assurance and technical competence balance each other.

This research, of course, has its limitations. Strictly speaking, the results presented here are limited to the specific environment of our experimental case (i.e., a listed e-commerce company with a solid financial situation). Regarding the design, we cannot exclude that the risk matrices have driven our results. We know non-professional investors are evidently influenced by graphical displays (Dilla et al., 2013). However, the comprehension checks clearly demonstrated that participants correctly perceived the absence/presence of both cybersecurity assurance and insurance against cyber risks. Thus, it may be inferred that those participants were not merely swayed by the presence of the risk matrices driving our results but also the pure information regarding cybersecurity assurance and insurance against cyber risks. The results could be different in another (less risky) industry, at another point in time, with a financially distressed company, after a recent IT incident, or in a different jurisdiction. We also examined the views of nonprofessional investors residing in the United Kingdom. The perceptions of other groups of people, such as institutional investors, financial analysts, or lending institutions, could differ substantially. Another limitation is that assurance and insurance do not constitute direct substitutes. Assurance can only ensure that systems and measures exist and are adequate. By contrast, insurance can compensate directly for a loss. Also, only the benefits of the measures were examined, not their costs. However, assurance is costly, so engaging an external assurance provider only appears appropriate if the benefits exceed the costs. Another limitation is that there is a far greater focus on treatments than in reality, as shareholders and other stakeholders receive much more information in annual reports, and their attention might thus be less focused on cybersecurity assurance and cyber risk insurance.

Future research could conduct similar studies in other settings and/or with other subject groups. Investigating more detailed published information about cybersecurity management systems or cybersecurity assurance, or other cyber risk insurance, are promising avenues for future research. Further effects of assurance and insurance on, for example, company reputation or financial performance might also be of interest. An archival study could examine the effect of cybersecurity assurance or cyber risk insurance on abnormal returns or cost of capital. It could also be of interest to investigate the impact of specific characteristics of the assurance provider on willingness to invest—for example, tenure, Big 4 versus non-Big 4, or industry specialists.

APPENDIX: EXPERIMENTAL CASE

Introduction

First, please read the case information carefully. Afterwards you will be asked:

- to answer some case-related questions, and
- to provide demographic information.

Scenario

As you work through the study, please imagine the following scenario:

You own a significant portfolio of stocks. You are doing a regular review of that portfolio, and you are considering investing in e-commerce. On the following pages, we will present you information about the fictitious company “BestProducts AG.” Please use this information to make your investment decision. There are no right or wrong answers, and we are not interested in how others would decide in these scenarios.

Company Description

“BestProducts AG” is one of Europe’s leading e-commerce companies with a wide range of products. The range includes international, local, and its own products and brands (e.g., books, clothing, electronics). With more than 38 million active customers, the company operates in 17 European countries. In addition to the above-mentioned products, which are distributed via the online store, the company also offers electronic products such as eBooks, music, Video-On-Demand, and a cloud service. The shares of “BestProducts AG” are listed in the German Prime Standard.

Key financial ratios	1st Jan. to 31st Dec. 2021	Relative change to previous year (1st Jan. to 31st Dec. 2020)
Net Sales	€ 11.28 bn.	+6.9%
Equity Ratio	37.2%	+0.7%
Operating Income (EBIT)	€ 0.76 bn.	+1.8%

Audit of the Consolidated Financial Statements

The annual auditor of “BestProducts AG” issued an unqualified audit opinion on the consolidated financial statements and the Group management report.

Extract From the Risk and Opportunity Report

The Executive Board has implemented a group-wide risk management system. A structural and procedural organization, as well as reporting channels, were defined by the

Management Board and Supervisory Board and are documented in the risk management manual.

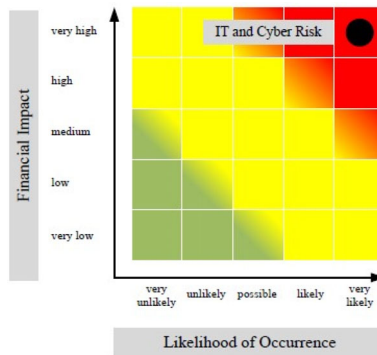
IT Risks (as a Part of the Risk and Opportunity Report)

Information technologies (IT) are of strategic importance for the business model of “BestProducts AG.” Our business processes depend to a large extent on IT services, applications, networks, and infrastructure systems. Our IT & cyber security and risk management have the task of managing threats in a cost-efficient manner.

Significant risks for us are the failure or disruption of our IT services (e.g., web store, cloud service) as well as the loss of sensitive (customer) data through unauthorized access. We are observing a significant global increase in cyber security threats and a higher level of professionalism in cybercrime. The disruption of our IT functions would have a significant negative impact on operations, earnings, and our reputation.

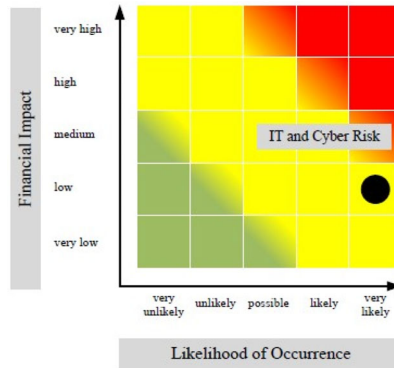
Experimental Condition 1

The following risk matrix depicts the risk assessment of the IT & cyber risks by “BestProducts AG.”



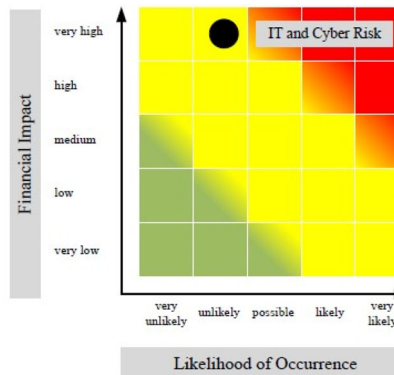
Experimental Condition 2

IT & cyber risks are covered by the purchase of insurance. This insurance covers, for example, damage caused by cyberattacks up to a loss of € 100 million. The following risk matrix depicts the IT & cyber risks of “BestProducts AG” after the insurance purchase.



Experimental Condition 3

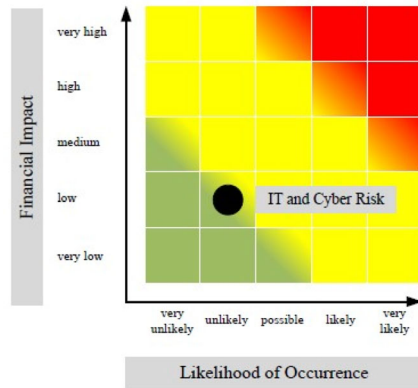
The fundament for our IT & cyber security and risk management is based on internationally recognized standards, such as ISO/IEC 27001. “BestProducts AG” has assured and certified its cyber security system by an audit firm according to ISO/IEC 27001. The following risk matrix depicts the IT & cyber risks of “BestProducts AG” after the cyber security assurance.



Experimental Condition 4

The fundament for our IT & cyber security and risk management is based on internationally recognized standards, such as ISO/IEC 27001. “BestProducts AG” has assured and certified its cyber security system by an audit firm according to ISO/IEC 27001.

IT & cyber risks are covered by the purchase of insurances. This insurance covers, for example, damage caused by cyber-attacks up to a loss amount of € 100 million. The following risk matrix depicts the IT & cyber risks of “BestProducts AG” after the insurance purchase and after the cyber security assurance.



Dependent Variables and Mediator

The following case-related questions (dependent variables; mediator) were provided to participants after they read the case materials. The response options were 7-point Likert scales with the indicated labels.

Dependent Variables

ATT: How do you generally assess “BestProducts AG” investment attractiveness?

very low O O O O O O O very high

BUY: How do you assess the likelihood of including “BestProducts AG” shares in your diversified portfolio?

very low O O O O O O O very high

Mediator

RISK: How do you assess the risk situation regarding the IT & cyber risk of “BestProducts AG”?

very low O O O O O O O very high

Comprehension Checks (CC)

The following comprehension checks were provided to participants after they read the case materials and answered the questions above. The response options were “yes” and “no.”

CC1: Has “BestProducts AG” engaged a cybersecurity assurance and certification?

CC2: Has “BestProducts AG” purchased insurance against IT & cyber risks?

Demographic Questions

KNOW_SHARE: How do you rate your expertise on stocks?

very low	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	very high
----------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------

KNOW_AR: How do you rate your expertise on annual reports?

very low	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	very high
----------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------

KNOW_IT: How do you rate expertise on IT and cyber security?

very low	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	very high
----------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------

TRUST_AF: How is your general reliance on audit firms?

very low	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	very high
----------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------

RISK_APPETITE: How do you rate your general risk appetite for investment decisions?

risk-averse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	risk-loving
-------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-----------------------	-------------

SHARE: For how many years have you owned or held stocks?

_____ years.

AGE: How old are you?

- ≤25 years
- 26–35 years

- 36–45 years
- 46–55 years
- 56–65 years
- ≥66 years

SCHOOL: What is your highest level of education?

- Middle School
- High School
- Bachelor's
- Diploma, Master's
- PhD

GENDER: What gender do you belong to?

- Female
- Male
- Diverse

REFERENCES

- Accounting Standards Committee of Germany. (2013). *Group management report* (GAS 20).
- Ackroyd, S. (2016). Sociological and organizational theories of professions and professionalism. In M. Dent, I. Bourgeault, J. L. Denis, & E. Kuhlmann (Eds.), *The Routledge companion to the professions and professionalism* (pp. 15–30). Routledge.
- Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1), Article ty006. <https://doi.org/10.1093/cybsec/ty006>
- AICPA. (2017). *Reporting on an entity's cybersecurity risk management program and controls*. AICPA. <https://doi.org/10.1002/9781119449966>
- Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, 60, Article 100989. <https://doi.org/10.1016/j.jfs.2022.100989>
- Alexei, A., & Alexei, A. (2022). The difference between cyber security vs. information security. *Journal of Engineering Science*, 29(4), 72–83. [https://doi.org/10.52326/jes.utm.2022.29\(4\).08](https://doi.org/10.52326/jes.utm.2022.29(4).08)
- Alon, A., & Vidovic, M. (2015). Sustainability performance and assurance: Influence on reputation. *Corporate Reputation Review*, 18(4), 337–352. <https://doi.org/10.1057/crr.2015.17>
- Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, 23(3), 1177–1206. <https://doi.org/10.1007/s11142-018-9452-4>
- Andrews, D., Nonnecke, B., & Preece, J. (2003). Electronic survey methodology: A case study in reaching hard-to-involve internet users. *International Journal of Human-Computer Interaction*, 16(2), 185–210.
- Asay, H. S., Hales, J., Hinds, C., & Rupar, K. (2023). Nonprofessional investor judgments: Linking dependent measures to constructs. *The Accounting Review*, 98(7), 1–32. <https://doi.org/10.2308/TAR-2021-0551>

- Ashby, S. G., & Diacon, S. R. (1998). The corporate demand for insurance: A strategic perspective. *The Geneva Papers on Risk and Insurance*, 23(86), 34–51.
- Badawy, H. (2021). The impact of assurance quality and level on cybersecurity risk management program on non-professional Egyptian investors' decisions: An experimental study. *Alexandria Journal of Accounting Research*, 5(3), 1–56.
- Bahşi, H., Franke, U., & Friberg, E. L. (2019). The cyber-insurance market in Norway. *Information & Computer Security*, 28(1), 54–67. <https://doi.org/10.1108/ICS-01-2019-0012>
- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 40(1), 131–158. <https://doi.org/10.1057/gpp.2014.19>
- Birnbaum, M. H., & Stegner, S. E. (1979). Source credibility in social judgement: Bias, expertise, and the judge's point of view. *Journal of Personality and Social Psychology*, 37(1), 48–74.
- Bodin, L., Gordon, L., Loeb, M., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, 37(6), 527–544. <https://doi.org/10.1016/j.jaccpubpol.2018.10.004>
- Brown-Liburd, H., & Zamora, V. L. (2015). The role of corporate social responsibility (CSR) assurance in investors' judgments when managerial pay is explicitly tied to CSR performance. *Auditing: A Journal of Practice & Theory*, 34(1), 75–96.
- Buchheit, S., Doxey, M. M., Pollard, T., & Stinson, S. R. (2018). A technical guide to using Amazon's Mechanical Turk in behavioral accounting research. *Behavioral Research in Accounting*, 30(1), 111–122. <https://doi.org/10.2308/bria-51977>
- Buckless, F. A., & Ravenscroft, S. P. (1990). Contrast coding: A refinement of ANOVA in behavioral analysis. *The Accounting Review*, 65(4), 933–945.
- Byrne, B. M. (2013). *Structural equation modeling with AMOS* (2nd ed.). Routledge.
- Canning, M., & O'Dwyer, B. (2001). Professional accounting bodies' disciplinary procedures: Accountable, transparent and in the public interest? *European Accounting Review*, 10(4), 725–749. <https://doi.org/10.1080/09638180127398>
- Chen, Y., & van Akkeren, J. (2012). *The theory of profession: Accountability, qualifications, entry and ethics—A preliminary discussion and early findings on the current state of forensic accountancy in Australia*. https://ro.uow.edu.au/articles/conference_contribution/The_Theory_of_Profession_Accountability_qualifications_entry_and_ethics_-_a_preliminary_discussion_and_early_findings_on_the_current_state_of_forensic_accountancy_in_Australia/27826938
- Cheng, M., Green, W. J., & Ko, J. C. W. (2015). The impact of strategic relevance and assurance of sustainability indicators on investors' decisions. *Auditing: A Journal of Practice & Theory*, 34(1), 131–162. <https://doi.org/10.2308/ajpt-50738>
- Cho, I.-K., & Sobel, J. (1990). Strategic stability and uniqueness in signaling games. *Journal of Economic Theory*, 50(2), 381–413.
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum.
- Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology*, 78(1), 98–104. <https://doi.org/10.1037/0021-9010.78.1.98>
- COSO. (2004). *Enterprise risk management: Integrated framework—Executive summary*. https://www.coso.org/files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

- CPA Canada. (2018). *CPA Canada guide: Reporting on an entity's cybersecurity risk management program and controls*. <https://www.cpacanada.ca/business-and-accounting-resources/audit-and-assurance/standards-other-than-cas/publications/soc-for-cybersecurity>
- Datar, S. M., Feltham, G. A., & Hughes, J. S. (1991). The role of audits and audit quality in valuing new issues. *Journal of Accounting and Economics*, 14(1), 3–49.
- de Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance—Issues and Practice*, 43(2), 239–274. <https://doi.org/10.1057/s41288-018-0082-7>
- Dent, M., Bourgeault, I. L., Denis, J.-L., & Kuhlmann, E. (Eds.). (2016). *The Routledge companion to the professions and professionalism*. Routledge.
- Deutsche Bundesbank. (2014). *Monthly report: September 2014*, 66(9), 1–172.
- DeZoort, F. T., Hermanson, D. R., & Houston, R. W. (2003). Audit committee member support for proposed audit adjustments: A source credibility perspective. *Auditing: A Journal of Practice & Theory*, 22(2), 189–205.
- Dilla, W. N., Janvrin, D. J., & Jeffrey, C. (2013). The impact of graphical displays of pro forma earnings information on professional and nonprofessional investors' earnings judgments. *Behavioral Research in Accounting*, 25(1), 37–60. <https://doi.org/10.2308/bria-50289>
- Diong, K. S., Foong, S. Y., & Sambasivan, M. (2018). Relational signalling in governance mechanisms and trust building. *Asian Journal of Accounting and Governance*, 9, 49–61. <https://doi.org/10.17576/AJAG-2018-09-05>
- Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24(1), 93–125. <https://doi.org/10.1111/rmir.12169>
- Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5), 474–491. <https://doi.org/10.1108/JRF-09-2016-0122>
- Elliott, W. B., Grant, S. M., & Hodge, F. (2018). Negative news and investor trust: The role of \$Firm and #CEO Twitter use. *Journal of Accounting Research*, 56(5), 1483–1519. <https://doi.org/10.1111/1475-679X.12217>
- European Union. (2022). *Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2464>
- EY. (2023). *ISO/IEC 27001 Information Security Management System—Lead Auditor & Lead Implementer Training*. https://www.ey.com/en_gl/consulting/certify-point/iso-iec-27001-2013
- Frank, M. L., Grenier, J. H., & Pyzoha, J. S. (2019). How disclosing a prior cyberattack influences the efficacy of cybersecurity risk management reporting and independent assurance. *Journal of Information Systems*, 33(3), 183–200. <https://doi.org/10.2308/isis-52374>
- Frank, M. L., Grenier, J. H., Pyzoha, J. S., & Zielinski, N. B. (2023). Implications of enhanced cybersecurity risk management reporting and independent assurance. *Current Issues in Auditing*, 17(1), P11–P18. <https://doi.org/10.2308/CIIA-2022-018>
- Franke, U. (2017). The cyber insurance market in Sweden. *Computers & Security*, 68, 130–144. <https://doi.org/10.1016/j.cose.2017.04.010>
- Freidson, E. (1989). Theory and the professions. *Indiana Law Journal*, 64(3), 423–432.

- Fresenius Medical Care. (2023). *Shaping a sustainable tomorrow: Annual report 2022*. https://www.freseniusmedicalcare.com/fileadmin/data/com/pdf/Media_Center/Publications/Annual_Reports/FME_Annual_Report_2023_EN.pdf
- Friedrich, C. (2021). Private investigations and self-disclosure of suspected fraud: Experimental evidence on forensic accounting services. *Behavioral Research in Accounting*, 33(1), 65–79. <https://doi.org/10.2308/BRIA-2020-045>
- Fuchs Petro Club. (2023). *Annual report 2022*. https://fuchs.azureedge.net/fileadmin/Home/Investor_Relations/Geschaeftsbericht/Zwischenbericht/2022/FPL_GB22_englisch_final_interaktiv.pdf
- Guggenmos, R. D., Piercey, M. D., & Agoglia, C. P. (2018). Custom contrast testing: Current trends and a new approach. *The Accounting Review*, 93(5), 223–244. <https://doi.org/10.2308/accr-52005>
- Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, 34(7), 808–834. <https://doi.org/10.1108/MAJ-09-2018-2004>
- Hay, D. (2019). *The future of auditing*. Routledge.
- HM Government. (2015). *UK cyber security: The role of insurance in managing and mitigating the risk*. <https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance>
- Hobbs, B. (2023, June 5). *The CRO cyber risk agenda: What boards should be asking*. EY. https://www.ey.com/en_us/board-matters/cyber-risk-questions-for-boards
- Holderness, C. G. (1990). Liability insurers as corporate monitors. *International Review of Law and Economics*, 10(2), 115–129.
- Hugo Boss. (2023). *Annual report 2022*. https://group.hugoboss.com/fileadmin/media/hbnews/user_upload/Investor_Relations/Finanzberichte/2022/HUGO_BOSS_Annual_Report_2022.pdf
- International Federation of Accountants. (2021). *The state of play in sustainability assurance*. <https://www.ifac.org/knowledge-gateway/discussion/state-play-sustainability-assurance>
- International Organization for Standardization (ISO). (n.d.). *ISO/IEC 27000 family: Information security management*. <https://www.iso.org/standard/iso-iec-27000-family>
- International Organization for Standardization (ISO). (2013). *Information technology—Security techniques—Information security management systems—Requirements (ISO/IEC 27001)*.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360.
- 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. *Journal of Financial Economics*, 139(3), 719–749. <https://doi.org/10.1016/j.jfineco.2019.05.019>
- Knechel, R. (2021). The future of assurance in capital markets: Reclaiming the economic imperative of the auditing profession. *Accounting Horizons*, 35(1), 133–151. <https://doi.org/10.2308/HORIZONS-19-182>
- KPMG. (2023). *KPMG Certification BV: KPMG certification services*. <https://kpmg.com/be/en/home/services/kpmg-certification.html>
- Krummacker, S. (2019). Firm’s demand for insurance: An explorative approach. *Risk Management and Insurance Review*, 22(3), 279–301. <https://doi.org/10.1111/rmir.12128>
- Li, H., No, W. G., & Wang, T. (2018). SEC’s cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30, 40–55. <https://doi.org/10.1016/j.accinf.2018.06.003>

- MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods*, 1(2), 130–149. <https://doi.org/10.1037/1082-989X.1.2.130>
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, 24, 35–61. <https://doi.org/10.1016/j.cosrev.2017.01.001>
- Martin, R. (2019). Examination and implications of experimental research on investor perceptions. *Journal of Accounting Literature*, 43(1), 145–469. <https://doi.org/10.1016/j.acclit.2019.11.001>
- Mayers, D., & Smith, C. W. (1982). On the corporate demand for insurance. *The Journal of Business*, 55(2), 281–296.
- Mercer, M. (2004). How do investors assess the credibility of management disclosures? *Accounting Horizons*, 18(3), 185–196. <https://doi.org/10.2308/acch.2004.18.3.185>
- Mott, G., Turner, S., Nurse, J. R., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. *Computers & Security*, 128, Article 103162. <https://doi.org/10.1016/j.cose.2023.103162>
- Navarro, P., & Sutton, S. G. (2024). Leveraging emerging cybersecurity reporting regulations: The effect of industry driven expectations for voluntary assurance. *Accounting Horizons*. Advance online publication. <https://doi.org/10.2308/HORIZONS-2023-088>
- Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, 45(4), 867–872. <https://doi.org/10.1016/j.jesp.2009.03.009>
- Palan, S., & Schitter, C. (2018). Prolific.ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, 17, 22–27. <https://doi.org/10.1016/j.jbef.2017.12.004>
- Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70, 153–163. <https://doi.org/10.1016/j.jesp.2017.01.006>
- Perols, R. R. (2023). The impact of the type of cybersecurity assurance service and cybersecurity incidents on investor perceptions and decisions. *Auditing: A Journal of Practice & Theory*, 43(3), 187–202. <https://doi.org/10.2308/AJPT-19-022>
- Perols, R. R., & Murthy, U. S. (2021). The impact of cybersecurity risk management examinations and cybersecurity incidents on investor perceptions and decisions. *Auditing: A Journal of Practice & Theory*, 40(1), 73–89. <https://doi.org/10.2308/AJPT-18-010>
- Pornpitakpan, C. (2004). The persuasiveness of source credibility: A critical review of five decades' evidence. *Journal of Applied Social Psychology*, 34(2), 243–281.
- ProSiebenSat.1 Media. (2023). *Annual report 2022: Moving forward*. <https://annual-report2022.prosiebensat1.com/servicepages/downloads/files/entire-p7s1-ar22.pdf>
- Quick, R., & Gauch, K. (2021). Is assurance on risk management systems relevant for bankers' decisions? *Advances in Accounting*, 55, Article 100564. <https://doi.org/10.1016/j.adiac.2021.100564>
- Quick, R., & Gauch, K. (2022). Darstellung der IT-Risiken im Risiko-und-Chancenbericht der DAX- und MDAX-Unternehmen. *Der Betrieb*, 75(8), 414–417.
- Ross, S. A. (1977). The determination of financial structure: The incentive-signalling approach. *The Bell Journal of Economics*, 8(1), 23–40.
- Rothrock, R. A., Kaplan, J., & van der Oord, A. F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, 59(2), 12–15.

- Roy, P. P. (2020). A high-level comparison between the NIST cyber security framework and the ISO 27001 information security standard. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)* (pp. 87–93). IEEE. <https://doi.org/10.1109/NCETSTEA48365.2020.9119914>
- Saks, M. (2012). Defining a profession: The role of knowledge and expertise. *Professions & Professionalism*, 2(1), 1–10.
- Schoenfeld, J. (2024). Cyber risk and voluntary Service Organization Control (SOC) audits. *Review of Accounting Studies*, 29(1), 580–620. <https://doi.org/10.1007/s11142-022-09713-0>
- Schwarzkopf, D. L. (2006). Investors' attitudes toward source credibility. *Managerial Auditing Journal*, 22(1), 18–33. <https://doi.org/10.1108/02686900710715620>
- Scopelliti, I., Morewedge, C. K., McCormick, E., Min, H. L., Lebrecht, S., & Kassam, K. S. (2015). Bias blind spot: Structure, measurement, and consequences. *Management Science*, 61(10), 2468–2486. <https://doi.org/10.1287/mnsc.2014.2096>
- SEC. (2023). *SEC 17 CFR Parts 229, 232, 239, 240, and 249, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*. <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>
- Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, 55(4), 349–356. <https://doi.org/10.1016/j.bushor.2012.02.004>
- Sheldon, M. D., & Jenkins, J. G. (2020). The influence of firm performance and (level of) assurance on the believability of management's environmental report. *Accounting, Auditing & Accountability Journal*, 33(3), 501–528. <https://doi.org/10.1108/AAAJ-11-2018-3726>
- Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. *The Journal of Finance*, 52(21), 737–783.
- Six, F., Nooteboom, B., & Hoogendoorn, A. (2010). Actions that build interpersonal trust: A relational signalling perspective. *Review of Social Economy*, 68(3), 285–315. <https://doi.org/10.1080/00346760902756487>
- Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, 44, Article 100548. <https://doi.org/10.1016/j.accinf.2021.100548>
- Spence, M. (1973). Job market signaling. *The Quarterly Journal of Economics*, 87(3), 355–374.
- Strupczewski, G. (2017). The cyber-insurance market in Poland and determinants of its development from the insurance broker's perspective. *Economics and Business Review*, 3(2), 33–50. <https://doi.org/10.18559/eb.2017.2.3>
- Thakor, A. V. (1990). Investment “myopia” and the internal organization of capital allocation decisions. *The Journal of Law, Economics, and Organization*, 6(1), 129–154. <https://doi.org/10.1093/oxfordjournals.jleo.a036982>
- Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Vosselman, E., & van der Meer-Kooistra, J. (2009). Accounting for control and trust building in interfirm transactional relationships. *Accounting, Organizations and Society*, 34(2), 267–283. <https://doi.org/10.1016/j.aos.2008.04.002>
- Wallace, W. (1980). *The economic role of the audit in free and regulated markets*. Open Education Resources. <https://scholarworks.wm.edu/cgi/viewcontent.cgi?article=1000&context=oer>

- Wallace, W. (2004). The economic role of the audit in free and regulated markets: A look back and a look forward. *Research in Accounting Regulation*, 17, 267–298. [https://doi.org/10.1016/S1052-0457\(04\)17012-4](https://doi.org/10.1016/S1052-0457(04)17012-4)
- Walton, S., Wheeler, P. R., Zhang, Y., & Zhao, X. (2021). An integrative review and analysis of cybersecurity research: Current state and future directions. *Journal of Information Systems*, 35(1), 155–186. <https://doi.org/10.2308/ISYS-19-033>
- Watts, R. L., & Zimmerman, J. L. (1990). Positive accounting theory: A ten year perspective. *The Accounting Review*, 65(1), 131–156.
- Yeo, F. (2021). Is framing more effective than regulating disclosures? The effects of risk disclosure frame and regime on managers' disclosure choices. *Contemporary Accounting Research*, 38(4), 2851–2870. <https://doi.org/10.1111/1911-3846.12711>