Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side

Bennet Simon von Skarczinski  
*PricewaterhouseCoopers Germany*, bennet.simon.von.skarczinski@pwc.com

Lukas Boll  
*Criminological Research Institute of Lower Saxony (KFN)*, lukas.boll@kfn.de

Frank Teuteberg  
*Osnabrück University*, frank.teuteberg@uni-osnabrueck.de

Follow this and additional works at: [https://aisel.aisnet.org/ecis2021_rp](https://aisel.aisnet.org/ecis2021_rp)

**Recommended Citation**  
von Skarczinski, Bennet Simon; Boll, Lukas; and Teuteberg, Frank, "Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side" (2021). *ECIS 2021 Research Papers*. 72.  
[https://aisel.aisnet.org/ecis2021_rp/72](https://aisel.aisnet.org/ecis2021_rp/72)

This material is brought to you by the ECIS 2021 Proceedings at AIS Electronic Library (AISeL). It has been accepted for inclusion in ECIS 2021 Research Papers by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
UNDERSTANDING THE ADOPTION OF CYBER INSURANCES FOR RESIDUAL RISKS - AN EMPIRICAL LARGE-SCALE SURVEY ON ORGANIZATIONAL FACTORS OF THE DEMAND SIDE

Research Paper

Bennet von Skarczinski, PricewaterhouseCoopers, Hanover, Germany, bennet.simon.von.skarczinski@pwc.com

Lukas Boll, Criminological Research Institute of Lower Saxony (KFN), Hanover, Germany, Lukas.boll@kfn.de

Frank Teuteberg, University of Osnabrueck, Germany, frank.teuteberg@uni-osnabrueck.de

Abstract

This research paper analyzes technological, organizational, and environmental (TOE framework) adoption factors of cyber insurances (CI) by conducting a computer-assisted telephone interview study with 2,483 German firms. Considering our screening of related literature, this study, to our knowledge, is the first large-scale empirical study analyzing organizational adoption factors of CI on the demand side. We distinguish between firms that have or have not considered CI and those that have or have not adopted CI following considerations. Our regression results indicate that there are statistically significant factors on the consideration and adoption of CI across all TOE dimensions. Subsequently, we discuss the extent to which CI is perceived as an appropriate tool to manage information security and derive propositions for the education of firms and further research in academia.

Keywords: Cyber Insurance, IT-Security Investments, TOE Framework, Adoption of Information Security Measures

1 Introduction

Besides the numerous advantages, digitization also has challenges, such as the increase in cyber attacks on firms (Legner et al., 2017). Due to the enormous potential damage of cyber risks, information security (IS) represents a priority objective to the management (Bulgurcu et al., 2010; Kankanhalli et al., 2003; Luftman and Ben-Zvi, 2010; Ransbotham and Mitra, 2009). In order to protect themselves from such IS risks, firms are implementing various IS measures on technical and organizational levels. However, no matter how hard firms try, residual IS risks will always remain (Marotta et al., 2017; Pal and Golubchik, 2010). Reasons for this include constantly evolving attack vectors, flaws or human failure, vulnerabilities of third parties, and economic considerations.

A risk management instrument to deal with such residual IS risk is cyber insurance (CI) (Bandyopadhyay, 2012; Geer, 2003; Gordon et al., 2003; Moore, 2010). CI is designed to transfer the financial risks related to network and computer incidents to a third party (Böhme et al., 2010). In exchange for the payment of a regular premium, a CI provider assumes losses from a variety of specified incidents, including data breaches, business interruption, and network damage (CISA, 2021).

Introduced to the market more than 20 years ago, CI have been a growing phenomenon (Dambra et al., 2020; Kshetri, 2020). Advantages of CI, including the transfer of financial risk, societal welfare by increasing overall IS, and the dissemination of IS standards, have been widely discussed (Marotta et al., 2017; Pal and Golubchik, 2010).
2017). However, CI has fallen short of its expectations to play a major role in information security management (ISM) (Bandyopadhyay et al., 2009; Böhme et al., 2010). Three main perspectives examine why CI have not yet arrived in operational practice to the expected extent.

Literature has raised challenges of CI on both the supply and the demand side, as well as on necessary conditions for the existence of a CI market (Romanosky et al., 2019). Considering the market and supply side, interdependent security (Böhme et al., 2010; Bolot and Lelarge, 2008), correlated risk (Böhme, 2005; Böhme and Kataria, 2006), information asymmetries (Bandyopadhyay et al., 2009; Shetty et al., 2010), and a lack of historical data (Wrede et al., 2020) have been found to negatively affect price-fixing mechanisms which thus lead to unreasonable insurance premiums (Bandyopadhyay et al., 2009; EIOPA, 2018; Eling and Schnell, 2016; Johnson et al., 2011). At least theoretically, those challenges have been well researched (Bahşi et al., 2019; Dambra et al., 2020) while the demand side lacks research (Eling and Schnell, 2016; Wrede et al., 2020). Compared to the US, CI are rarely used and remain unknown by many firms in Europe (Eling and Schnell, 2016). To determine how widespread CI is in Europe and other regions, authors resort to commercial reports due to the lack of representative and empirical studies (e.g. Eling and Schnell, 2016; Marotta et al., 2017). Along with the minimal dissemination of CI, the factors influencing CI demand have hardly been investigated (Tøndel et al., 2015; Wrede et al., 2020). In this context, Bandyopadhyay (2012) questions why firms do not widely use CI for mitigating residual IS risks. Prior descriptive research indicates that the adoption of CI varies by firm-specific factors (e.g. higher adoption within large firms and the finance industry (UK Department for Culture, Media and Sport, 2020)). However, our literature review did not find any academic research that further investigated these questions using inferential statistics.

Research on IS rarely considers the adoption process at the organizational level (Hameed and Arachchilage, 2016). To address this shortcoming, we apply the TOE framework of DePietro et al. (1990). With a focus on the organizational adoption of IS-related technical innovations, the TOE framework has been used to identify and analyse technological, organizational, and environmental adoption factors (e.g. Hameed and Arachchilage, 2020; Herath et al., 2020; Salleh et al., 2015). We empirically extend this approach to the field of CI to shed light on the understanding of the demand side of CI. Because of the lack of representative empirical studies, little is known about the dissemination of CI and its organizational adoption factors. Thus, we formulate the following research questions (RQ):

RQ1: How large are the adoption shares of CI among firms?

RQ2: What empirical CI adoption factors exist, on an organizational level, among

I: firms that considered to adopt CI in contrast to those that did not?

II: firms that adopted CI in contrast to those that, following CI considerations, did not?

The division of RQ2 into two parts is intended to prevent apples from being compared with pears. It prevents firms that simply have not yet thought about CI from being equated with CI deniers.

By carrying out regression analyses and computer-assisted telephone interviews (CATI) with a stratified random sample of 2,483 German firms with more than nine employees across all industries, we contribute towards the empirical-based understanding of CI adoption. The motivation for our work can be summarized into three aspects. First, by improving the understanding of CI adoption factors on the demand side, better insurance solutions can be created. This protects the operations of firms, while the general introduction of insurance conditions and market standards leads to a higher IS protection level in society (Majuca et al., 2006). Second, by strengthening academic research, dependence on potentially biased commercial literature is reduced. And thirdly, we meet the widespread call of literature to provide more empirical and real-life data analysis on CI (Bahşi et al., 2019; Dambra et al., 2020; Marotta et al., 2017; Romanosky et al., 2019; Wrede et al., 2020).

We structure our work as follows. Section two summarizes existing work on how widespread CI is, what CI adoption factors have thus far been identified, and which research gaps exist. Section three presents our theoretical framework and derives hypotheses. Our methodology and sampling are illustrated in section four, while the results of RQ1 and RQ2 are reported in section five. We discuss propositions of our results in section six and conclude our work in section seven.
2 Related Work

In line with our research questions, we focus on empirical research that analyzes factors of CI adoption on the demand side. For more comprehensive literature overviews on the supply side, market mechanisms, and other perspectives, we refer the reader to previous work (Böhme et al., 2010; Dambra et al., 2020; Eling, 2020; Eling and Schnell, 2016; Kshetri, 2020; Marotta et al., 2017; Wrede et al., 2018; Wrede et al., 2020). Since our dataset focuses on the institutional level of CI adoption, we also exclude behavioral aspects of individual decision makers. To identify related work in the field of general adoption of IS measures, CI adoption, and grey literature on CI, we applied iterative Google Scholar searches. For all papers that caught our interest, we, after reading, applied backward and forward searches to identify further literature. In parallel, we screened CI relevant articles marked as “empirical” provided in the comprehensive literature overview of Eling and Schnell (2016) on cyber risk and CI.

The inadequacy of previous work about the institutional CI adoption can be summarized as 1) lack of comprehensive theoretical support, 2) lack of sufficient empirical evidence, or 3) lack of scientific rigor.

In his recent literature review on cyber risk and insurance, Eling (2020) concludes that empirical cyber risk research remains in its infancy and consistent theory and methodology are still missing. Also, Hameed and Arachchilage (2020) find there is hardly any distinct theoretical model with the aim to explain IS adoption. However, the adoption of general IS measures has been subject to sound research. Herath et al. (2020) present a PLS-model structured by the TOE framework including survey data of 368 IS managers. They show that besides characteristics of the new technology, the support from top management and external factors influence the adoption of IS solutions. Gordon et al. (2018) surveyed 158 IT executives and found associations between IT security budgets and the importance of IS on the internal control system, perceived potential losses, and competitive advantages of cyber security. Hsu et al. (2012) show that besides institutional influences, economics-based and organizational factors have significant influences on the adoption of ISM. Chang and Ho (2006) showed that, among others, industry type and firm size are significant factors when implementing ISM. While these studies indicate that institutional level factors influence the adoption of IS measures, none of these studies include CI. Since CI has a less technical and more financial nature compared to traditional IS measures (e.g. encryption, two-factor authentication), it seems questionable as to whether the insights of existing literature can be applied to CI adoption. Further sufficient empirical evidence on CI adoption we could not find, which also explains the omnipresent call for empirical research in this realm (Bahşi et al., 2019; Dambra et al., 2020; Marotta et al., 2017; Romanosky et al., 2019; Wrede et al., 2020).

In the absence of empirical scientific literature on CI, we searched grey literature. There are several reports of consulting and insurance firms that survey the dissemination and potential use of CI (Advisen Ldt. and PartnerRe Ltd., 2018; BDO Australia Ldt., 2019; CIAB, 2017; Hiscox Ltd., 2020; Marsh GmbH, 2019). Hiscox Ltd. (2020) surveyed 5,569 security professionals across all firm sizes and found that 26% have a standalone CI policy. The proportion of respondents that have purchased CI as a result of a previous incident has risen to 20%. However, the report lacks any further explanation as to why and what kind of firms adopt CI coverage. A report by PartnerRe & Advisen (2018) states that top drivers of adopting CI are news of cyber-related losses experienced by others (56%), own experienced losses (50%), third party requirements (42%), increased education (40%), board management demand (39%), and regulatory changes (33%). As main reasons against the adoption of CI, the Ponemon Institute LLC (2013) states that premiums are too expensive (52%), there are too many exclusions/restrictions in the policy (44%), and that the minimal security level required is not met (26%). While these reports provide further indications of factors for or against the adoption of CI, their analyses are based on non-transparent methodologies, non-representative samples, or non-EU data. The methodologically appropriate annual survey of the UK Department for Digital, Culture, Media & Sport (2020) stated that

---

1 Search strings on CI adoption: “cyber insurance empirical analysis”, “cyber insurance (investment or adoption)”, “information security insurance”; Strings on general IS adoption: “Organizational adoption of information security measures”, “information security investment process”, “information security Technology Organization Environment”; Google search strings on grey CI literature: “Cyber insurance report”, “Cyber insurance survey”, “Cyber security survey”; Search period of 09/2020 - 10/2020
28% of the interviewed 1,348 businesses have insurance protection against IS risks as part of a wider business insurance, whereas another 4% have specific CI policies. Moreover, large firms show a higher proportion of some kind of CI (large: 53%; medium: 52%; small: 44%; micro: 29%), with CI also being more prevalent in the finance/insurance industry (51% vs. 32% overall). However, distinct theoretical support and further inferential statistical analyses are also missing.

Considering this background, the contribution of our work to the existing body of knowledge seems apparent. To our knowledge, we provide one of the first demand-side and large-scale\(^2\) empirical studies on CI adoption factors on an organizational level.

3 Theoretical Basis and Hypotheses

Adopting CI within firms, like any other investment, requires a decision-making process. Rationality forms a critical part of strategic decision-making processes (Dean and Sharfman, 1993). A large amount of research, especially when focussing on the organizational level, uses rational choice and other economic approaches to analyze how decision makers allocate budgets to protect their information assets (Beebe et al., 2014; Bodin et al., 2005; Cavusoglu et al., 2004; Cavusoglu et al., 2008; Herath and Herath, 2008; Wang et al., 2008). Although the rational choice approach has been criticized for neglecting behavioral biases related to the individual level of decision makers (Kahneman and Tversky, 1979; Slovic et al., 1977), we apply rational choice as a decision mechanism embedded into a technological, organizational, and environmental context using the TOE framework (DePietro et al., 1990). By controlling for the influence of the interviewees’ position and their risk perceptions, we partly address those concerns but maintain our focus on the organizational level of the phenomenon.

The TOE framework, however, constitutes that the process by which a firm adopts and implements technological innovations is influenced by the technological, the organizational, and the environmental context (DePietro et al., 1990). The technological context describes the existing technologies in use and relevant technical skills available and may include both equipment as well as processes. The organizational context refers to the firm’s characteristics and resources, including the firm’s size, degree of centralization, degree of formalization, managerial structure, human resources, and culture (DePietro et al., 1990; Teo et al., 2006). The external arena in which a firm conducts its business, including its industry, competitors, and trading partners, however, represent the environmental context.

Since much of the empirical IS research, and therefore also associated theories, focuses on individual and employee behavior (Herath et al., 2020), TOE enables an important theoretical perspective for studying a firm’s contextual adoption factors of innovation (Zhu et al., 2006). It therefore optimally supports our research interest and available dataset relating to the institutional level of CI demand.

Furthermore, TOE has been broadly supported in empirical work (Baker, 2012; Kuan and Chau, 2001) and has been applied in IS research (Bradford et al., 2014; D’Costa-Alphonso and Lane, 2010; Hameed and Arachchilage, 2020; Herath et al., 2020; Li, 2015; Salleh et al., 2015). Herath et al. (2020) suggest that organizational factors contribute to the adoption of IS solutions and deemed TOE well suited to analyze those aspects. Furthermore, Bandyopadhyay (2012) proposes the application of TOE in the context of CI. Due to its minimal dissemination, the absence of clear market standards, and above all, the novel integration of CI into the central ISM, we, in line with Bandyopadhyay (2012), consider the instrument CI as a techno-financial innovation and therefore suitable for analysis using the TOE.

---

\(^2\)“Large scale” refers to sample size, while the lower limit of “large” is not fixed. Large samples are needed to reach statistical power and precision. It further implies probability sampling and the commitment to certain quality criteria (Mohler and Rosenbladt, 2009).
Our theoretical background, which assumes that CI is adopted to cover residual risk (Bandyopadhyay, 2012; Geer, 2003; Marotta et al., 2017; Moore, 2010), is outlined in Figure 1. Firms consider a more or less concrete CI performance offer they received from the supply side and their individual residual IS risk, manifested in and determined by the constructs of the three TOE contexts. Although the supply side is treated as a black box in our research, we include it to theoretically explain important mechanisms affecting the adoption of CI on the demand side. These include challenges like information asymmetries, correlated risk, and interdependent security complicating the appropriate pricing of CI policies leading to potentially overpriced offers (Bandyopadhyay et al., 2009; EIOPA, 2018; Eling and Schnell, 2016; Johnson et al., 2011). From a firms perspective, those overpriced offers could, under the assumption of rational choice, lead to a decision against CI. On the other hand, interdependent security often leads to complexity, which can thus result in IS risks that firms cannot necessarily control, e.g. the outage of a cloud service provider resulting in revenue losses, which in turn strengthens the validity of CI protection. In contrast, insurance company’s minimum IS requirements could prevent firms from purchasing CI protection. Instead, investments into additional IS measures could reduce the residual risk to an acceptable amount.

Researchers have used different constructs when operationalising TOE, since there is a unique set of factors for each specific innovation being studied (Baker, 2012). We thus derived constructs for each of our TOE contexts from related IS literature (Bradford et al., 2014; D’Costa-Alphonso and Lane, 2010; Hameed and Arachchilage, 2020; Herath et al., 2020; Li, 2015; Salleh et al., 2015) and mapped them to our pre-existing IS and CI focused dataset. The mapping was intensively discussed in a doctoral colloquium at KFN as well as tested for adequate intercoder reliability (Cohen’s Kappa: .89) between two of the three authors. To prevent firms that simply have not thought about CI from being equated with CI deniers, we apply the same theoretical framework to analyze whether firms have considered CI. Hence, we derive the following hypotheses:

**Technology** Firms that are more complex are more likely to consider CI (H1.1) or adopt CI (H1.2). Under control of the other independent variables, firms with more complexity and thus more security exposure (e.g. higher interconnectedness of systems and processes, as well as more data and infrastructure) have more residual risk and additional CI cover thus seems rational. In contrast, Ogut et al. (2005) argue a higher degree of interdependence makes firms invest less in IT security and CI because interdependence reduces the effectiveness of IS spending. However, considering regulations (e.g. German GmbHG §43 (1); AktG §93 (1); GDPR article 5 (1f)) that require risks of a firm to be adequately addressed, we assume effectiveness considerations are deprioritized.

Firms that considered CI (H2.1) or adopted CI (H2.2) have more information security measures in place than those that did not consider or purchase CI. Firms that contemplate IS in-depth could understand CI to be an integral part of a holistic risk management strategy. In this context, CI represents a complementary contribution to protection procedures already implemented by firms (Bandyopadhyay, 2012; Bolot and Lelarge, 2009; Gordon et al., 2003; Wrede et al., 2018; Young et al., 2016). Moral hazard (Ehrlich and Becker, 1972) could indeed reduce the incentive of insured firms to invest in self-protection, but we assume that regulatory requirements such as the General Data Protection Regulation (GDPR), coverage limitations, and minimal requirements of CI (Young et al., 2016) make it factually impossible for firms not to take further IS measures.

![Figure 1. Theoretical Background.](image-url)
Organizations. Firms that show a higher degree of IS compliance are more likely to consider CI (H3.1) or adopt CI (H3.2). Perceptions of compatibility were utilized to explain innovation usage by firms (Herath et al., 2020; Tornatzky and Klein, 1982). We conceptualize this compatibility not only in technical terms, but also in how far staff and management are aware of risks and comply with security policies, thereby enabling the proper handling of CI as an innovation. In this regard, management support was also identified as an important driver to adopt IS measures (Hsu et al., 2012; Kankanahalli et al., 2003). Further IS-TOE research incorporated management support within the organizational context (Hameed and Arachchilage, 2020; Salleh et al., 2015). Greater compliance and managerial support both mean that firms more actively engage in increasing IS and are therefore more likely to adopt CI. Moreover, missing explicit responsibilities for dealing with IS risk hinder the adoption of CI on the demand side (Moore, 2010). In addition, CI seems to have a compliance and IS enhancing effect on firms (Kesan et al., 2008; Majuca et al., 2006; Talesh, 2018; Young et al., 2016).

Firms that have more available resources are more likely to consider CI (H4.1) or adopt CI (H4.2). The availability of financial, technological, and human resources are important factors within the adoption of security solutions (Herath et al., 2020). Human resources are needed to implement and maintain basic technical and organizational IS measures in order to meet CI coverage prerequisites. Financial resources in particular determine whether innovations can be afforded (Rosner, 1968). Straub et al. (2008) stated that ISM is also an “economic decision” and typically “requires resources”.

Firms that experienced cyber attacks in the last 12 months are more likely to consider CI (H5.1) or adopt CI (H5.2). The experience of firms with IT systems have been used in the organizational context of TOE as a factor to analyze technological adoption (D’Costa-Alphonso and Lane, 2010). Recent experiences of cyber attacks could therefore highlight a firm’s current shortcomings of systems, processes, or awareness and induce decision makers to take further and immediate IS measures to mitigate residual risk. In this regard, Shackelford (2012) stated that past incidents could increase the perception of protection and thus favor CI.

Firms with higher risk perceptions are more likely to consider CI (H6.1) or adopt CI (H6.2). Firms that report a high perceived risk of being affected by a cyber attack in the next 12 months are more likely to benefit from CI protection in the near future. For example, Mukhopadhyay et al. (2013) show that firms’ investments in CI differs according to their risk profiles. Gordon et al. (2018) demonstrated, that the IT security budget is associated with perceived potential losses.

Environment. Firms that considered CI (H7.1) or have adopted CI (H7.2) differ from those that did not consider or purchase CI in terms of their industry affiliation. Industries differ in their IT-intensity and business models and therefore their risk exposure (Biener et al., 2015). Furthermore, an industry difference in the intra-organizational exchange of security practices could influence the consideration or adoption of CI (Herath et al., 2020). Tunçalp (2014) shows that the dissemination and adoption of ISM systems differs between industries.

4 Methodology and Sampling

From August 2018 to January 2019, we carried out computer-assisted telephone interviews (CATI) with representatives of 5,000 firms in Germany with more than nine employees. The survey was conducted within the context of a government-funded initiative to improve IS in small and medium enterprises (SME). Using a random split-half approach, 2,483 firms were surveyed on the topic of CI. We are reusing this data in the context of the current article. In the following, we outline our sampling, pre-testing, and data quality measures.

Research Objectives. Considering the research framework of a government-funded initiative to improve IS for SME, the focus on firms was predetermined. General research questions and the questionnaire were originated from a literature review (Dreissigacker et al., 2020), expert interviews with six practitioners from German cyber-security related authorities and two insurance companies (Stiller et al., 2020), as well as discussions with the project-own-regional business advisory council. Serving as a sparring partner to the project team, the council was founded in order to ensure the practical
relevance of activities throughout the 3-year research project. Various local medium-sized companies, as well as security authorities, are represented in the council.

**CATI method** The CATI method was chosen because, in comparison to postal and online surveys, the desired target interviewees (e.g. IT managers or board members) can be reached more quickly and precisely. By means of technical guidance and individual support from experienced and trained interviewers, inquiries are answered instantly, which has a positive effect on the overall data quality (Steeh and Charlotte, 2008). Moreover, through complex filter guidance by computer support, the survey can be conducted efficiently (Lavrakas, 2008). In addition telephone interviews using list samples showed acceptably high response rates (Steeh and Charlotte, 2008).

**Population** All firms that act as independent legal entities, which had their headquarters in Germany and more than nine employees, represent the population. The exclusion of micro-firms has research-pragmatic reasons, insofar they are subject to relatively strong changes (e.g. establishment, insolvency), which negatively influences the availability of contact information. Approximately 3.5 million German firms were registered in 2017, from which 89.3% are micro-firms. Examining the remaining 10.7%, the largest proportion are firms with 10 to 49 employees (78.8%), whereas firms with more than 250 employees only represent 4% of the firms in Germany with more than 9 employees. However, firms in our sample represent about 81.5% of all employees in Germany (Dreissigacker et al., 2020).

**Sample** 2,483 firms (Group A) answered three questions on the topic of CI, whereas 2,517 firms (Group B) answered additional questions on reporting incidents to the police. Both groups were asked about risk perceptions, detected cyber attacks within the last 12 months, technical and organizational IS measures deployed in the firm, as well as demographic characteristics of the firms. However, only Group A data is analyzed in this paper. The firms were represented by individuals responsible for IT and IT-security (66.8%), members of the management board (24.3%), and other firm representatives (8.9%). In order to ensure that sub-populations of interest (e.g. large firms) are adequately represented in the sample, a disproportionately stratified sample was drawn (Table 1). Therefore, large firms and those providing services of general interest are more strongly represented in the sample than in the population. To enable a separate statistical analysis for those sub-populations, the smallest bins contain 500 observations. Although it is possible to reproporotionalize our sample using sector and employee class weights, we did not do this in the following analysis because sector and employee class are controlled for. Moreover, our focus is on analyzing certain group characteristics rather than on representative statements for German firms. The sample was drawn from two commercial business databases (Bisnode, 2017; Heins & Partner, 2017), which included contact details and contact persons, as well as the industry assignment according to the German WZ08-classification, which allows for international comparison.

**Survey Conduction** A professional and IS research experienced survey institute executed the CATI-interviews. The institute was chosen after an official Europe-wide tender offering. The survey was pre-tested in two phases: 1) discussions with our council and, 2) interviews with six additional IT employees from firms of different sizes and industries. Prior to the field phase, we conducted interview training sessions in two on-site call centers to prepare the 141 interviewers. We deliberately formulated brief and clear questions to enable easy comprehension. To avoid fatigue effects, we designed the questionnaire to take at most 20 minutes. By providing interviewees with an official cover letter of the German Federal Ministry for Economic Affairs and Energy during the contact phase, we aimed to maximise participation. We additionally guaranteed a purely scientific use of the data and complete anonymity. Data protection contracts were concluded with the survey institute. If desired, the questionnaire was provided to the firms prior to the interview. To comply with ethical

<table>
<thead>
<tr>
<th>Employees class</th>
<th>Targeted sample</th>
<th>Sample Group A</th>
<th>Sample %</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-49 small</td>
<td>1,000</td>
<td>610</td>
<td>24.6</td>
</tr>
<tr>
<td>50-99 medium</td>
<td>1,000</td>
<td>576</td>
<td>23.2</td>
</tr>
<tr>
<td>100-249 medium+</td>
<td>1,000</td>
<td>549</td>
<td>22.1</td>
</tr>
<tr>
<td>250-499 large</td>
<td>1,000</td>
<td>497</td>
<td>20.0</td>
</tr>
<tr>
<td>&gt;500 large+</td>
<td>500</td>
<td>251</td>
<td>10.1</td>
</tr>
<tr>
<td>Public service providers</td>
<td>500</td>
<td>incl. above</td>
<td>incl. above</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>5,000</strong></td>
<td><strong>2,483</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

Table 1. Sample quota plan.

**Data Analysis** Technical data quality checks were carried out in real-time by the CAT-interview software. To test the internal consistency, we applied further data plausibility checks on the distribution and correlation of our variables. The questionnaire containing descriptions of the single items as well as extensive descriptive data analyses of the sample, on the basis of weighted data, can be found in the official research report (Dreissigacker et al., 2020).

Dependent variables are illustrated in Figure 2. Independent and control variables are described in Table 2. Variables with four-item response scales were dichotomized, while metric, dichotomous, and categorical items were not recoded. We apply descriptive analysis ($\chi^2$), visual inspection, and binary logistic regression models using Stata statistical software (Version 15). All logistic regression models statistically control for the number of employees, industry, and interviewee position. Diagnostic tests (multicollinearity, test for specification errors, goodness of fit) did not show any need to change the regression models. To preserve a high number of observations when using listwise deletion, independent variables were grouped according to the TOE framework into four regression models. Each model applied to firms considering CI (RQ2 I) and adopting CI (RQ2 II). Logistic regression results are reported as average marginal effects (AME) (StataCorp, 2017), as well as corresponding standard errors (SE) and statistical significance ($p$-value). In contrast to odds ratios and logits, which only express the direction of the impact, AMEs are not distorted in the presence of heteroscedasticity and can be interpreted more precisely as they indicate the mean change of the likelihood of the event of interest in percentage points if the relevant explanatory variable changes by one unit (Auspurg and Hinz, 2011; Bergmann et al., 2018). All reported regression analysis results indicate correlations between independent and dependent variables, rather than representing directions of causal relationships.

### 5 Results

**RQ1: How large are the adoption shares of CI among firms?** Out of our stratified random sample, 19.5% (N=484) of respondents reported having CI, which was defined as any kind of insurance against...

<table>
<thead>
<tr>
<th>Sample: Cyber Insurance (N=2,483)</th>
<th>Adopted CI</th>
<th>Considered CI</th>
<th>Result Decision Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>yes (19.5%, N=484)</td>
<td>yes (19.5%, N=484)</td>
<td>positive (19.5%, N=484)</td>
<td></td>
</tr>
<tr>
<td>no (51.7%, N=1,283)</td>
<td>yes (20.3%, N=503)</td>
<td>positive (20.3%, N=503)</td>
<td></td>
</tr>
<tr>
<td>d.k. (26.8%, N=665)</td>
<td>no (29.2%, N=726)</td>
<td>negative (20.3%, N=503)</td>
<td></td>
</tr>
<tr>
<td>n.s. (2.1%, N=51)</td>
<td>d.k. (2.2%, N=54)</td>
<td>negative (20.3%, N=503)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d.k. (26.8%, N=665)</td>
<td>unknown (31%, N=770)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>n.s. (2.1% N=51)</td>
<td>d.k. don’t know; n.s. not specified</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2. Filter path diagram and dependent variables.**

IS violations and therefore also covers extended business interruption insurances. Of those firms which reported to have CI, the largest proportion would recommend other firms to adopt CI coverage (62.6%; N=303) and 25 firms actually tried to claim their CI (5.2%). Out of 1,283 (51.7%) firms that do not have CI, 726 reported that they had not yet considered the topic, meaning they did not go through the decision process (Figure 2). 503 firms considered CI but eventually did not adopt CI. Of those, 168 (33.4%) argued that costs are too high. In total, 716 interviewees either did not know if their firm has CI (26.8%) or they did not specify (2.1%), and are therefore treated as missing in the regression analyses.

---

*Twenty-Ninth European Conference on Information Systems (ECIS 2021), Marrakesh, Morocco*
The majority of answers were given by interviewees who reported being responsible for IT or IT security. Interviewees of the management board were more likely to know whether their firms did or did not have CI (Figure 3). Firms with a greater number of employees were more likely to be represented by IT managers, while smaller firms were more likely to be represented by board managers. Therefore, the number of employees and the position of the interviewees were chosen as control variables besides industry affiliation in all regression models (RQ2). Visual and descriptive analyses (Chi²-tests) show that firms with CI report higher annual revenues than firms without CI (p < 0.001). In addition, firms in the finance and insurance industry (WZ08-K: 56.5%) show a significantly higher adoption rate of CI than any other industry (Figure 3). Also, the CI adoption rate in the health sector (WZ08-Q: 25.2%) is significantly higher than in the education sector (WZ08-P: 12.5%). Further descriptive statistics and our independent variables are shown in Table 2.

RQ2: What empirical CI adoption factors exist, on an organizational level, among firms that considered to adopt CI in contrast to those that did not? Our logistic regression analysis shows that complexity items (e.g. outsourcing technology, providing special products or services, or having multiple firm locations with own IT infrastructure in Germany or abroad) do not correlate with going through a decision processes (H1.1). In terms of IS measures, firms that train their employees in IS security (AME = 0.109, SE = 0.035, p < 0.001) and those that regularly perform risk and vulnerability analyses/penetration tests (AME = 0.097, SE = 0.036, p < 0.001) considered purchasing CI significantly more often. Therefore, firms with instances of employee IS training are on average 11% more likely to have considered CI than firms that do not conduct such training. Consequently, firms that regularly perform vulnerability analyses are on average 10% more likely to have considered CI than firms that do not regularly conduct vulnerability analyses (H2.1). However, the lack of time constructs in operationalization leads to the need to exclude causal relationships from this interpretation. Rather, we focus on correlation. Interviewees, who state that “a lot is done in the company for IT security” (AME = 0.149, SE = 0.065, p < 0.01), were more likely to report that their firm underwent the decision process. In contrast, those who state that their management is aware of IT risks (AME = -0.141, SE = 0.061, p < 0.01), were significantly less likely to report a decision process focusing on CI (H3.1). Regarding available resources, our analysis reveals that neither IT / IT security staff nor budget correlate with considering CI (H4.1).
Table 2. Descriptive statistics of independent variables and assignment to TOE context.

Firms which have been affected by spy- (AME = 0.114, SE = 0.044, p < 0.01) or ransomware (AME = 0.102, SE = 0.039; p < 0.001) at least once in the last twelve months, report considering CI more often. This means that such firms are on average 10% or 11%, respectively, more likely to also have considered CI in the past. Contrary effects are shown for firms experiencing malware attacks (AME = -0.071, SE = 0.035, p < 0.01) (H5.1). Risk perceptions do not significantly correlate with the consideration of CI (H6.1). Firms from the financial and insurance sector (WZ08-K classification) are more likely to have undergone the decision process of acquiring CI in contrast to other industries (AME = 0.460, SE = 0.086, p < 0.001) (H7.1). Compared to small firms (10-49 employees), bigger firms (100-500+ employees) are more likely to have considered CI in the past (AME = 0.085-0.229, SE = max. 0.045, p < 0.01). The range in AME values leads to the conclusion that all firms with 100 to 500+ employees are more likely to consider CI compared to small firms. Firms with 50-99 employees did not differ significantly from

<table>
<thead>
<tr>
<th>Variable</th>
<th>TOE</th>
<th>Portion or mean (SD)</th>
<th>Span</th>
<th>Variable</th>
<th>TOE</th>
<th>Portion or mean (SD)</th>
<th>Span</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outsourcing communication (1=yes)</td>
<td>T: Cpx (2)</td>
<td>38.0% 0 - 1</td>
<td></td>
<td>Mgt. IS awareness (1=(rather)high)</td>
<td>O: Comp (1)</td>
<td>90.3% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Outsourcing network (1=yes)</td>
<td></td>
<td>46.4% 0 - 1</td>
<td></td>
<td>Staff IS Awareness (1=(rather)high)</td>
<td></td>
<td>84.9% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Outsourcing web presence (1=yes)</td>
<td></td>
<td>68.2% 0 - 1</td>
<td></td>
<td>IS overall effort (1=(rather)high)</td>
<td></td>
<td>88.8% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Cloud software/storage (1=yes)</td>
<td></td>
<td>32.2% 0 - 1</td>
<td></td>
<td>IT Budget (EUR)</td>
<td></td>
<td>529,777 (3,001,272)</td>
<td>200 - 85m</td>
</tr>
<tr>
<td>Multiple sites Germany (1=yes)</td>
<td></td>
<td>42.9% 0 - 1</td>
<td></td>
<td>IT security budget (EUR)</td>
<td></td>
<td>87,404 (289,651)</td>
<td>100 - 7.5m</td>
</tr>
<tr>
<td>Site abroad (1=yes)</td>
<td></td>
<td>13.5% 0 - 1</td>
<td></td>
<td>Amount IT staff</td>
<td></td>
<td>8.7 (25.7)</td>
<td>0 - 400</td>
</tr>
<tr>
<td>Special products/services (1=yes)</td>
<td></td>
<td>34.7% 0 - 1</td>
<td></td>
<td>Amount IT security staff</td>
<td></td>
<td>1.8 (5.2)</td>
<td>0 - 150</td>
</tr>
<tr>
<td>Special reputation (1=yes)</td>
<td></td>
<td>41.5% 0 - 1</td>
<td></td>
<td>Amount experienced attacks last 12m</td>
<td></td>
<td>42.5 (246.6)</td>
<td>0 - 5,982</td>
</tr>
<tr>
<td>Export activity (1=yes)</td>
<td></td>
<td>41.4% 0 - 1</td>
<td></td>
<td>Exp. ransomware last 12m (1=yes)</td>
<td></td>
<td>15.8% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Password requirements (1=yes)</td>
<td></td>
<td>87.4% 0 - 1</td>
<td></td>
<td>Exp. spyware last 12m (1=yes)</td>
<td></td>
<td>12.3% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Individual user rights (1=yes)</td>
<td></td>
<td>92.7% 0 - 1</td>
<td></td>
<td>Exp. other malware last 12m (1=yes)</td>
<td></td>
<td>23.0% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Regular Backups (1=yes)</td>
<td></td>
<td>98.5% 0 - 1</td>
<td></td>
<td>Exp. Manual hacking last 12m (1=yes)</td>
<td></td>
<td>2.8% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Anti-Virus Software (1=yes)</td>
<td></td>
<td>98.9% 0 - 1</td>
<td></td>
<td>Exp. (D)DoS last 12m (1=yes)</td>
<td></td>
<td>7.0% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Regular Updates (1=yes)</td>
<td></td>
<td>96.5% 0 - 1</td>
<td></td>
<td>Exp. Defacing last 12m (1=yes)</td>
<td></td>
<td>3.2% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Firewall (1=yes)</td>
<td></td>
<td>98.7% 0 - 1</td>
<td></td>
<td>Exp. CEO fraud last 12m (1=yes)</td>
<td></td>
<td>14.6% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Advanced Firewall (1=yes)</td>
<td></td>
<td>75.3% 0 - 1</td>
<td></td>
<td>Exp. phishing last 12m (1=yes)</td>
<td></td>
<td>26.4% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Outsourced IS measures (1=yes)</td>
<td></td>
<td>37.8% 0 - 1</td>
<td></td>
<td>Untargeted attack 12m (1=(rather)high)</td>
<td></td>
<td>35.0% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Written IS policies (1=yes)</td>
<td></td>
<td>74.7% 0 - 1</td>
<td></td>
<td>Targeted attack 12m (1=(rather)high)</td>
<td></td>
<td>8.5% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Emergency plans (1=yes)</td>
<td></td>
<td>66.0% 0 - 1</td>
<td></td>
<td>Industry Finance/ Insurance (1=yes)</td>
<td></td>
<td>4.3% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>IT security certification (1=yes)</td>
<td></td>
<td>27.8% 0 - 1</td>
<td></td>
<td>Employee size (see Table 1)</td>
<td></td>
<td>-</td>
<td>0 - 1</td>
</tr>
<tr>
<td>Compliance checks (1=yes)</td>
<td></td>
<td>73.3% 0 - 1</td>
<td></td>
<td>Interviewee Mgt. Board (1=yes)</td>
<td></td>
<td>24.3% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>Risk assessment/pentest (1=yes)</td>
<td></td>
<td>56.7% 0 - 1</td>
<td></td>
<td>Interviewee IT/IT-security (1=yes)</td>
<td></td>
<td>69.8% 0 - 1</td>
<td></td>
</tr>
<tr>
<td>IS training (1=yes)</td>
<td></td>
<td>59.0% 0 - 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure simulations</td>
<td></td>
<td>35.9% 0 - 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend: Res = resources; Sec = IS measures; Comp = IS compliance; Cpx = complexity; Risk = risk perceptions next 12 months; Att = experienced attacks last 12 months; X = (regression model); SD = standard deviation; m=million
those with 10–49 employees. Additionally, interviewees employed in IT/IT security (AME = 0.103, SE = 0.038; p < 0.001), as well as management board members (AME = 0.097, SE = 0.039; p < 0.01), are more likely to report that their firms considered CI, compared to other interviewees.

RQ2 II: What empirical CI adoption factors exist, on an organizational level, among firms that adopted CI in contrast to those that, following CI considerations, did not? Looking at complexity, firms with multiple locations and their own IT infrastructure in Germany tend to have CI significantly more often (AME = 0.074, SE = 0.034, p < 0.01), but no effect for locations abroad is shown. The outsourcing of software or storage to an external cloud correlates positively (AME = 0.074, SE = 0.036, p < 0.01), whereas the outsourcing of e-mail /other communication systems correlates negatively with the adoption of CI (AME = -0.077, SE = 0.037, p < 0.01) (H1.2). However, firms with written emergency guidelines show a significantly increased probability of 16% (AME = 0.159, SE = 0.059; p < 0.001) to actually adopt CI (H2.2). IS compliance items do not show statistically significant correlations with the decision for or against CI (H3.2).

Regarding resources, no significant correlation between IT or IT security staff / budget and the decision for or against CI can be observed (H4.2). Experiences with different types of cyber attacks in the last 12 months do not show significant correlation with CI adoption, except for CEO-fraud (AME = -0.114, SE = 0.052, p < 0.01). This means that firms that have experienced such an attack are less likely to have CI (H5.2). Risk perception cannot be positively or negatively linked to CI adoption (H6.2). However, firms in finance or insurance (WZ08-K) are more likely to adopt CI than other firms, showing an increase in average probability of 24.5% (AME = 0.245, SE = 0.064, p < 0.001) (H7.2). Pseudo-R² values (McKelvey and Zavoina, 1975) rated low to moderate for all regression models of RQ2 I and RQ2 II (0.039 - 0.192).³ However, this empirical study does not focus on a high proportion of explained variance. Rather, significant correlations between technical, organizational, and environmental factors on the consideration and adoption of CI should be shown.

Table 3: Results of hypotheses testing.

<table>
<thead>
<tr>
<th>Hypotheses</th>
<th>Hx.1 (Consider CI)</th>
<th>Hx.2 (Adopt CI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: Complexity</td>
<td>not supported</td>
<td>partly supported</td>
</tr>
<tr>
<td>H2: IS measures</td>
<td>partly supported</td>
<td>partly supported</td>
</tr>
<tr>
<td>H3: IS compliance</td>
<td>partly supported</td>
<td>not supported</td>
</tr>
<tr>
<td>H4: Resources</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>H5: Experienced attacks</td>
<td>partly supported</td>
<td>not supported</td>
</tr>
<tr>
<td>H6: Risk perceptions</td>
<td>not supported</td>
<td>not supported</td>
</tr>
<tr>
<td>H7: Industry affiliation</td>
<td>supported</td>
<td>supported</td>
</tr>
</tbody>
</table>

6 Discussion

We analyzed which TOE factors are associated with (1) firms simply considering CI protection and (2) firms adopting CI as a techno-financial innovation. Based on our results, we derive five propositions, each including possible explanations and future research questions, for academia as well as the demand side of CI.

Proposition #1: Further analysis on the CI decision process  Our analysis showed different relevant factors of considering and adopting CI across all three TOE contexts. However, many other factors showed no significant effects. Interestingly, looking at the key factors identified, there are almost no interferences between the two groups RQ2 I (consideration of CI) and RQ2 II (adoption of CI). Firms that perform regular IS training are 11%, whilst those that carry out vulnerability assessments are 10%, more likely to consider CI than firms that do not perform such measures. However, they are not more likely to adopt CI. In contrast, firms with written emergency guidelines are more likely to adopt CI, but do not show an effect in group RQ2 I. A reason for the latter could be reversed causality by minimal requirements of insurance companies when selling CI, which we could not analyze within our study. However, we could not find indications that insured firm invest less in IS as assumed under moral hazard (Srinidhi et al., 2015). In turn, it is also not obvious that firms that adopted CI have more IS measures.

³ According to Langer (2016) “the McKelvey & Zavoina Pseudo-R² is the best estimator for the ‘true R²’ of the OLS regression”
in place. A contra-intuitive finding is that two of the IS compliance items point in different directions. While firms in which “a lot is done for IT security” are 14.9% more likely to consider CI, firms with a higher risk awareness and compliance of the managing board are 14.1% more likely to not consider CI. A possible explanation might be that the latter board members are satisfied with their IS measures and therefore do not consider additional CI. Moreover, firms that have experienced ransom- or spyware attacks in the last 12 months are more likely to consider CI, but not to actually adopt CI. An explanation here could be the relatively short inquired time frame of at most 12 months. During the 12 months after an attack, firms may consider, yet may not permanently adopt CI. Furthermore, it is not known when the consideration of CI took place. The same logic might apply to the finding that firms that experienced CEO-fraud are 14% more likely to not have CI. Other plausible factors, as stated in our development of hypotheses (e.g. IT budget or risk perceptions) do not show effects at all. Solely firms of the finance and insurance sector are more likely to consider and adopt CI, as also indicated by others (UK Department for Culture, Media and Sport, 2020). Larger firms, furthermore, are more likely to adopt CI. Our findings ultimately indicate that there must be additional relevant factors for the consideration or adoption of CI protection. Further research should therefore focus on the actual decision process of firms adopting CI and challenge in how far firms systematically and rationally access their IS capabilities, as well as their residual risk.

**Proposition #2: Combine TOE framework with theories focusing on individual technology adoption** Associated with the organizational decision process are behavioral aspects of decision making (Beebe et al., 2014; Goodhue and Straub, 1991; Hsu et al., 2012), as well as aspects of bounded and procedural rationality (Ranganathan and Sethi, 2002). These could, in practice, overlay all TOE factors within the consideration or adoption of CI. Following on from proposition #1, we suspect further adoption factors on the individual level of decision-makers. Since there are, apart from post-adoption user acceptance models, hardly any distinct theoretical models on IS security adoption and cyber risk management (Eling, 2020; Hameed and Arachchilage, 2020), we propose to combine the TOE framework with theories focusing on the individual adoption behavior of IS decision makers.

**Proposition #3: Establish organizational learning in ISM and formalize decision processes** Caused by the missing or low influence of key factors (e.g. IT security budget, risk perceptions, complexity, or experienced cyber attacks) in our analysis, we, in line with Weishäupl et al. (2018), assume that ISM decision processes lack formalization and standardization. The risk with low consideration of TOE factors in CI adoption is the overweighting of individual, and possibly biased, assumptions of decision makers (Dor and Elovici, 2016). Regulatory requirements (e.g. German GmbHG or AktG, GDPR) force board members to appropriately address risks to the firm by taking suitable measures. Therefore, firms should establish and maintain transparent and reproducible decision processes on adopting IS measures, which allows for a documentation that such requirements were met. Moreover, transparent decision processes should build a common understanding on the adoption of IS measures across involved actors. Our results indicate that there might be knowledge gaps between interviewees since management board members were less likely to state that they did not know if CI was adopted (Mgt: 10% vs. IT/IT security: 32%). In turn, if CI is supposed to be part of an integrated ISM process, responsible IT/IT security managers should be similarly represented. However, this indicates that IT/IT security managers might perceive CI less as a tool to manage IS risks.

**Proposition #4: Educate decision makers by providing neutral and transparently reported information on the actual costs and benefits of CI adoption** Firms do not seem to widely perceive CI as an appropriate tool to manage IS (see Bandyopadhyay et al., 2009). Less than 20% of firms have some form of CI cover. Of those that underwent a decision process, over half decided against CI. Examining only valid responses, approximately 42% of firms have not even considered CI. Of those that decided in favor of CI, two fifths do not know if they would or would not recommend CI to other firms. Firms may not even consider CI due to a lack of general IS awareness, as Eling and Schnell (2016) formulated the fatal misjudgment “it will not happen to me” and “my data is not interesting enough” or the mistaken belief that other insurances already cover these IS risks (Marotta et al., 2017; OECD, 2017). However, when examining our data, most interviewees assign themselves relatively high awareness and
compliance scores (Table 2: Mgt. awareness: 90.3%; staff awareness: 84.9%; IS effort: 88.8%). It is therefore questionable whether decision makers overestimate their own risk awareness and subsequently draw wrong conclusions. Reasons why firms, following CI consideration, did not adopt CI seem manifold. 33.4% of firms that considered but did not adopt CI stated that the costs of CI are just too high. Contrary to media reports, various research repeatedly states that costs of cyber attacks are still low for many firms (Biener et al., 2015; Paoli et al., 2018; Romanosky, 2016; UK Department for Culture, Media and Sport, 2020). Meland et al. (2017) analyzed additional existing uncertainty factors of adopting CI, including the perception of immature CI products, coverage limitations, and difficulties in understanding CI policies. For managers to seriously concern themselves with the advantages and disadvantages of CI, and thereby actively influence the supply side of CI by their demand behavior, we believe further awareness campaigns are needed.

**Proposition #5: Critically discuss the actual contribution of CI to improve IS**

As stated in section five (RQ1), only 5.2% (N=25) of firms with some form of CI cover tried to claim indemnity. Of those, six firms stated that no indemnity was received. A further eight firms stated that the indemnity did not cover the whole damage. Assuming a certain deductible on the CI payment, it seems legitimate to discuss how far CI truly transfers relevant parts of residual risks. Firms may also not draw on existing CI cover for tactical reasons (Bandyopadhyay et al., 2009). Asymmetric information and interdependent security, for instance, potentially lead to expensive and niche CI products (Dambra et al., 2020; Meland et al., 2017). On the other hand, CI seems to have a compliance and IS enhancing effect on firms (Kesan et al., 2008; Majuca et al., 2006; Talesh, 2018; Young et al., 2016). Further research to analyze whether IT security budgets spent on preventing or detecting IS measures, instead of CI, are more efficient thus seems necessary. Especially if, as a result of additional preventing or detecting IS measures, interdependent risks in the society would be reduced.

### 7 Conclusion

Considering our screening of related work and comprehensive literature overviews on cyber risk and insurance (Eling, 2020; Eling and Schnell, 2016), we provided one of the first demand-side empirical analyses of technological, organizational, and environmental key factors of firms’ consideration or adoption of CI. However, our research has limitations. By interviewing only a single individual that represents a firm, the data collected may be affected by subjective attitudes, knowledge, and motivation (self-reporting, social desirability). Varying response behavior could influence the data collected, which although we cannot eliminate, we partly addressed by controlling the interviewee position. For sampling, we accessed two commercial firm databases. According to their self-declaration, the databases should in total include all registered firms in Germany with more than 9 employees. If this self-declaration is not met, some firms in the population may lack the chance for sample inclusion. Since the structure of the sample (i.e. industries, employee classes) corresponds to the general population, there is no indication of structural biases. The self-selection-bias of specific firms generally not participating in such surveys cannot be rejected. Our participation rate is 11.6% and therefore comparable with similar IS surveys (CSI, 2011: 6.4% (paper & email survey); Gordon et al., 2018: 10% (paper survey); Hall et al., 2011: 27.0% (paper survey; an web pilot survey was discarded: 8.4%); Paoli et al., 2018: 4.9% (web survey); Rantal, 2008: 23% (paper survey)). Whilst there may be other TOE relevant factors that our sample data simply did not address, we identified statistically significant factors across all TOE dimensions. Contrary to our theoretical derivation, other factors do not seem to correlate with the consideration or adoption of CI. Since even less significant results are required to increase the body of knowledge and avoid publication bias (Amrhein et al., 2019; Egger and Smith, 1998; Rothstein et al., 2005), our research contributes to the understanding of why/why not firms consider and adopt CI to address residual IS risks. Since our findings suggest that firms less systematically consider TOE factors, future research should perform closer analysis on CI decision processes. The individual perspective of decision makers, their potentially overestimated risk assumptions, and compromised rationality should also be subject to future research.
References


*Twenty-Ninth European Conference on Information Systems (ECIS 2021), Marrakesh, Morocco*


von Skarzinski et al. / Adopting Cyber Insurance


