Toward enhancing the information base on costs of cyber incidents: implications from literature and a large-scale survey conducted in Germany

Received 10 August 2021
Revised 13 November 2021
21 March 2022
Accepted 9 May 2022

Bennet Simon von Skarczinski
Cybersecurity and Privacy, PricewaterhouseCoopers GmbH, Hannover, Germany
Arne Dreißigacker
Criminological Research Institute of Lower Saxony, Hannover, Germany, and
Frank Teuteberg
University of Osnabrück, Osnabrück, Germany

Abstract

Purpose – Literature repeatedly complains about the lack of empirical data on the costs of cyber incidents within organizations. Simultaneously, managers urgently require transparent and reliable data in order to make well-informed and cost-benefit optimized decisions. The purpose of this paper is to (1) provide managers with differentiated empirical data on costs, and (2) derive an activity plan for organizations, the government and academia to improve the information base on the costs of cyber incidents.

Design/methodology/approach – The authors analyze the benchmark potential of costs within existing literature and conduct a large-scale interview survey with 5,000 German organizations. These costs are directly assignable to the most severe incident within the last 12 months, further categorized into attack types, cost items, employee classes and industry types. Based on previous literature, expert interviews and the empirical results, the authors draft an activity plan containing further research questions and action items.

Findings – The findings indicate that the majority of organizations suffer little to no costs, whereas only a small proportion suffers high costs. However, organizations are not affected equally since prevalence rates and costs according to attack types, employee classes, and other variables tend to vary. Moreover, the findings indicate that board members and IS/IT-managers show partly different response behaviors.

Originality/value – The authors present differentiated insights into the direct costs of cyber incidents, based on the authors' knowledge, this is the largest empirical survey in continental Europe and one of the first surveys providing in-depth cost information on German organizations.

Keywords Impact of data breaches, Management of information security, IT-security investments, Cost-benefit benchmark, Cyber losses

Paper type Research paper

1. Introduction

The digitization of organizations entails challenges, such as the increase of cyber-attacks (Legner *et al.*, 2017). Based on the large potential damaging effect of cyberattacks, information

This work was created in addition to, and used data from, the research project "Cyber-attacks against companies in Germany", which was funded by the German Federal Ministry for Economic Affairs and Energy [BMWi-VID5-090168623-01-1/2017].

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 2 No. 2, 2022
pp. 79-112
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-08-2021-0020

security (IS) represents a priority objective to decision makers (Bulgurcu *et al.*, 2010; Ransbotham and Mitra, 2009). In order to protect their organizations from cyber-attacks, responsible managers must make suitable decisions. In light of limited resources, this decision-making includes, but is not limited to, the alignment of IS strategy, prioritization of IS topics, implementation of security measures and business decisions, such as entering specific markets or utilizing certain technologies. Such decision-making has been subject to research from various disciplines, such as information systems, business administration, computer science, and economics (Ranganathan and Sethi, 2002; Weishäupl *et al.*, 2018; Demetz and Bachlechner, 2013; Cavusoglu *et al.*, 2004).

In this context, research has raised the question of what the economic cost of IS breaches is (Gordon and Loeb, 2006b). The importance of this question is based on the assumption that information security management (ISM) is subject to the principle of economic efficiency, which demands a balance between the costs and benefits of IS (Gordon and Loeb, 2006a; Brecht and Nowey, 2013; Iannacone and Bridges, 2020; Connolly and Borrion, 2020). Contextually, economic analyses examine IS investments as the acquisition of hardware, software, processes, knowledge and other factors in anticipation of favorable future economic returns (Kwon and Johnson, 2014; Chari *et al.*, 2008). A well-developed IS investment rationale provides managers with a set of criteria to justify investments in IS and permits the evaluation of economic feasibility (Iannacone and Bridges, 2020; Cavusoglu *et al.*, 2015). Moreover, managers require analytic, decision-focused and quantitative techniques to answer the question: "How much is enough?" (Hoo, 2000).

Besides cost-benefit considerations, non-economic aspects such as strategic attempts (e.g. retention of customer goodwill or trust; also see Lloyd, 2020) or mimetic, coercive and normative pressures influence an organization's ISM decision-making (Cavusoglu *et al.*, 2015). Although institutional pressures, such as regulatory requirements, can immediately influence the cost-benefit equation to a certain extent, it is evidenced that newer and more relevant regulations, such as the European General Data Protection Regulation (GDPR), address "appropriateness" as well as "consideration of technology available and implementation costs" when describing the implementation of measures (GDPR: recitals of the GDPR (83) and article 6.3). Despite all external pressures, managers must articulate the value of their activities in business terms since, especially in difficult economic times, only IS investments that can demonstrate a clear business value will be funded (Brecht and Nowey, 2013; Kesswani and Kumar, 2015). A cost-benefit analysis is therefore deemed a sound basis for ISM decision-making (Gordon and Loeb, 2006a).

Certain IS options usually result in implementation and operation costs (EBA, 2017) e.g. license costs of a firewall, proportionate wages of security staff) and can therefore, like other objects of operational accounting/controlling, be quantified relatively easily (Gordon and Loeb, 2006a). Therefore, our research does not focus on implementation or operation costs. The benefits of IS options are, in contrast, often presented as the avoidance of future damaging costs (Gordon and Loeb, 2006a; Brecht and Nowey, 2013; Kesswani and Kumar, 2015). These benefits, however, are hard to estimate (Cavusoglu *et al.*, 2004; Brecht and Nowey, 2013; Makridis and Dean, 2018; Wolff and Lehr, 2017) given that success hereby equates to the lack of a cyber-security incident and potential outputs can also be intangible (Kwon and Johnson, 2014). Similar to previous research (Paoli *et al.*, 2018), we therefore focus on costs that are measurable and directly assignable to a cyber-incident, with the knowledge that our analysis only represents a lower limit of the phenomenon.

Despite the large number and wide variety of publicly available literature on cyber-attacks perpetrated against organizations, the existing research database is repeatedly criticized for being fragmented, incomparable, partly contradictory and lacking a foundation (Makridis and Dean, 2018; Wolff and Lehr, 2017; Anderson *et al.*, 2013; Florencio and Herley, 2012). Such criticisms ranges all the way to the accusation that hardly any reliable data exist

on this phenomenon and that many actors are unable to distinguish between reliable and unreliable data, which in turn leads to poorly informed decisions (Ryan and Jefferson, 2003). The major need for well-founded research, as proclaimed in the literature (Armin *et al.*, 2015; Sen and Borle, 2015; Agrafiotis *et al.*, 2018), and specifically a benchmark for decision makers (Cavusoglu *et al.*, 2004; Brecht and Nowey, 2013) thus seems necessary. Against this background, the aim of this article is to support the quantification of the benefit aspect of the ISM cost-benefit calculus in terms of avoidable cyber incident-related costs.

Despite the lack of a common procedure to systemize and measure the costs of cyber incidents (Paoli *et al.*, 2018; Hughes *et al.*, 2017), we follow the request of the existing literature to provide a benchmark for these costs that, we believe, are measurable and suitable to at least illustrate the minimum dimension of this phenomenon. Our research focuses on small- and medium-sized enterprises (SME) as these usually have less systematic ISM and fewer resources available to prepare and perform advanced ISM analysis (Ključnikov *et al.*, 2019; Gallagher *et al.*, 2016).

To enhance the information based on ISM, we follow a three-step approach (Figure 1).

We assume that organizations aim to reduce uncertainty regarding decision-making and apply economic cost-benefit considerations but, due to a lack of data, are dependent on external benchmarks to quantify ISM benefits in terms of avoided cyber incident-related costs.

As a first step, we therefore conduct a literature review to, on the one hand, analyze the extent to which the existing literature is suitable to serve as a benchmark for the costs of cyber incidents within organizations, and on the other hand, identify the major findings of the literature. Secondly, based on the identified shortcomings of the literature, we conduct own field research by interviewing 5,000 mainly SMEs in Germany using a stratified random sample and computer-assisted telephone interviews (CATI). Given the lack of reliable and differentiated empirical data available on the costs of cyber incidents for German SMEs, we address the following research questions:

RQ1. How are German organizations, based on our random sample of 5,000 organizations, affected by cyber incidents?

RQ1a. What types of cyber incidents do organizations report as the most severe?

RQ1b. Which direct and incident-related costs arise, and to what extent, following the organization's most severe cyber incident in the last 12 months?

Thirdly, following the provision of empirical results, we, on a meta-level examine the implications that can be derived from related literature and our own research. To sustainably enhance ISM decision-making, we address our second research question:

RQ2. What can be done across the three agents "Organizations", "Government/Society," and "Academia" to improve the information base available on costs of cyber incidents to better enable ISM decision-making?

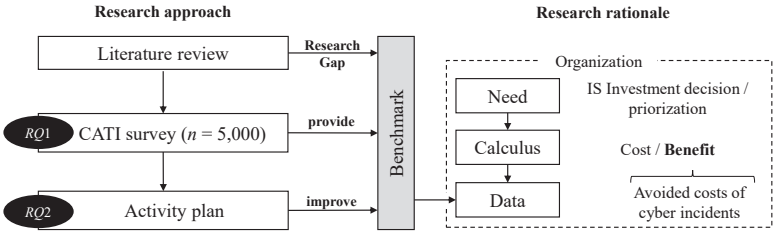

Figure 1.
Research approach and rationale

We have thus drafted an activity plan, containing action items and further research topics, that outlines some practical steps for the three agents to generate better information and use existing information more constructively. We use a triangulation approach to derive items for the activity plan. These data sources include our data-based results, qualitative aspects of discussions with our project-own-regional business advisory council, project stakeholders and other organizations, as well as expert interviews with seven representatives of German security authorities in tandem with findings of relevant literature.

Conducting a CATI-study with 5,000 German organizations, which is to our knowledge the largest empirical survey in continental Europe and one of the first attempts of providing differentiated cyber incident costs for German SMEs, we provide managers, researchers and other stakeholders with representative, neutral and transparent findings.

However, whilst working together with practitioners that accompanied our three-year research project, we repeatedly noticed a focus on the reporting of raw results and a neglect of methodical and operationalization-based aspects. Besides our content-related findings, we therefore also highlight what can be done across organizations, government/society and academia to enhance the origination and use of information on costs of cyber incidents. We therefore consider this article as basic and preparatory work upon which further analyses will be built.

Whilst we provide a brief summary of related work in section 2, we will illustrate the operationalization and results of the CATI-survey in section 3. Section 4 discusses implications and proposes the activity plan, whilst section 5, the conclusion, summarizes our findings and implications and outlines limitations.

2. Implications from related literature

In this section, we derive benchmark quality criteria, describe our approach to search for related literature, and analyze the extent to which existing literature is suitable to serve as a benchmark for costs of cyber incidents within organizations.

2.1 Quality criteria

Before analyzing the extent to which the existing literature can serve as a benchmark to organizations, the quality criteria must be defined. Hence, we derived four kinds of criteria from the literature. At first **(**assignability), organizations must be able to assign themselves to a dedicated peer group (Biemer, 2010). The industry affiliation and size (i.e. revenue or employees) have been shown to affect ISM and are commonly used as control variables in related research designs (Sen and Borle, 2015; Choudhury and Kwon, 2016; Romanosky, 2016; Buil-Gil *et al.*, 2021). The use of official standards allows for an unambiguous assignment and international comparison (e.g. EU Regulation (EC) No 1893/2006 NACE, EU Commission Recommendation (2003/361/EC)). Furthermore, the regionality of the peer group also seems to be important (Wang and Kim, 2009) since different regulations, IS maturities and cultural aspects are pertinent. Secondly (relevance and determinability), benchmarks must use dimensions and measures of practical ISM relevance (Biemer, 2010; McManus and Eloff, 2006). This includes the use of monetary business terms (Brecht and Nowey, 2013; Gordon and Loeb, 2006a) and an operationalization that is detailed enough to allow managers to derive dedicated ISM actions. Moreover, focusing on SMEs, benchmark data should be easy to use and should not require deeper statistical processing (McManus and Eloff, 2006). Thirdly (representativeness), the benchmark data must be of appropriate quality and allow for generalizability and the transfer of findings to other organizations. Such quality criteria also include requirements related to sampling (Neyman and Pearson, 1928) and sample sizes, as well as significance measures/probabilities of errors (Biemer, 2010; Cohen, 1992; AAPOR, 2016). Fourthly, and finally (transparency), benchmarks must be transparent about the

definitions and methodology used, and must appropriately describe the relevant limitations (AAPOR, 2016).

2.2 Search approach

We focused on literature, written in the English language that empirically collects and analyzes the costs of cyber incidents in order to potentially provide monetary benchmarks to organizations. We excluded research that was not detailed or descriptive enough to serve as a benchmark on an organizational level (e.g. stock price analysis, macro-economic research or research focusing on statistical modeling). Given that, the largest part of available literature is not scientific, but rather commercial and governmental (Gehem *et al.*, 2015), we distinguish between scientific and grey literature. We searched for relevant scientific literature in three databases [1], each using four different strings [2]. Sorting by relevance, we considered the first 100 results for every search iteration. Additionally, we applied forward and backward searches on results catching our interest. When searching for grey literature, we used duckduckgo.com and applied the same approach and search strings, but added the keyword "report".

2.3 Cost benchmarking – appropriateness of the literature

The results of our research are summarized in Appendix 1, Table A1. Given that we aimed to analyze the extent to which the existing literature is suitable to serve as a benchmark for costs of cyber incidents within organizations, we did not comprehensively evaluate the literature, but only considered its benchmark potential.

As stated before, there is a lack of reliable data. We identified three academic (Paoli *et al.*, 2018; Romanosky, 2016; Eling and Wirfs, 2019), and three governmental studies (Rantala, 2008; Richards, 2009; DCMS, 2020), as well as seven, partially recurring, commercial reports (Vanson Bourne, 2014; Ponemon Institute and HP, 2016; Accenture, 2019; Cisco, 2019; IBM, 2020; Hiscox Ltd., 2020; Kaspersky Lab, 2019) matching our previously described quality criteria. We expected to find more commercial literature; however, very few reports provided actual and detailed costs of cyber incidents. The commercial literature did not describe sample types, the underlying population, or statistical significance/error probabilities (see Appendix 1). Few commercial reports consistently differentiated by company size, industry, cost types and attack types. In addition, none of the commercial reports covered a single dedicated country, which makes the, at times, small sample sizes even less informative. It often remained unclear as to how many organizations were analyzed since only the number of interviewees was reported. We therefore conclude that the aforementioned commercial literature cannot fulfill the need of decision makers to provide reliable benchmark data. Governmental studies, on the other hand, use random samples and large sample sizes and allow organizations to assign themselves to the data set using size and industry differentiations. Most governmental studies did not differentiate between ISM-relevant costs and attack types. Moreover, they were not available for countries in continental Europe. Academic literature, in contrast, is clear about populations, statistics, operationalization and limitations but lacks large random samples to brighten the dark field of cyber-attacks. Considering the phenomenon of cyber-attack costs and literature aiming to provide external ISM-relevant benchmarks to organizations, available statistics, as Anderson *et al.* already concluded in 2013, seem to remain insufficient and fragmented.

2.4 Cost benchmarking – major findings

Romanosky (2016) analyzed 921 publicly available events from commercial databases, differentiating between data breaches (median: $170 k; mean: $5.9 M), security incidents ($330 k; $9.2 M), privacy violations ($1.3 M; $10.1 M), and phishing ($150 k; $20 M). When

looking at industries, management ($2 M), retail trade ($1.75 M) and information ($1.25 M) show the highest weighted losses per event, whereas those relating to real estate/rental/leasing, professional services and transportation are below $0.5 M. These costs refer to those that were incurred as a direct result of the incident but exclude lost revenue, lost market value, cost of customers, etc. Moreover, Romanosky (2016) states that, costs of phishing and privacy violations were in decline from 2005 to 2014, whereas costs of data breaches increased during this time. However, he notes that his analysis was affected by major events of large firms. Romanosky (2016) concludes that the cost of cyber incidents is less than $200 k for most firms, which corresponds to only a fraction of the millions of dollars commonly cited elsewhere. On average, businesses lose 5% of their annual revenue to fraud and corruption. The costs of cyber incidents, however, only represent 0.4% of lost revenue, which translates to only a small proportion of the cost of doing business. Hence, public concerns may be slightly excessive.

Paoli *et al.* (2018) surveyed 300 SME businesses in Belgium in 2016. For five, mostly legally, defined attack types, they explored material harm by personnel and other costs. For the most serious type of data/system interference, 64.2% of incidents caused no value of lost or damaged assets and 17.3% were below €10 k. Similar comparisons can be made regarding lost revenue: in 60% of the incidents no harm was reported, whilst a further 22.1% stated losses below €10 k. Overall, they found evidence that most affected businesses did not report major harm or costs and only one-fifth of the impacted businesses rated the harm to operational activities as serious or more.

Eling and Wirfs (2019) analyzed 1,579 cyber risk events stemming from an operational risk database, which includes losses above $100 k, and compare these to non-cyber operational risk losses. Mean ($43.5 M vs. $98.5 M), standard deviation ($426.4 M vs. $1,154.4 M), median ($1.5 M vs. $5.1 M) and skewness ($27.1 M vs. $50 M) were found to be significantly smaller for cyber than for the non-cyber losses. Additionally, costs are unevenly distributed across the continents. A high proportion of incidents occurred in the financial industry, however, mean ($30.6 M vs. $82.1 M) and median losses ($1.2 M vs. $4.5 M) are lower than in other industries which might indicate a higher protection level. Looking at company sizes, a U-shaped relation between the loss amount and the number of employees can be observed, indicating heavier, but not statistically significant, tails for small- and large-sized companies.

Rantala (2008) conducted one of the first large-scale studies relating to this topic. Surveying 8,000 US organizations, she demonstrated the prevalence of cyber-attacks in 2005 according to eight incident types. Without further differentiating the costs, Rantala found that 79% of the organizations that had detected such incidents reported on the associated monetary losses, which show an overall median of $6 k, but vary by incident types.

Richards (2009) surveyed 4,000 Australian businesses on costs directly associated with cyber incidents. Without further differentiating the costs, he states that 93% of small, 84% of medium and 67% of large businesses suffered costs below AUD 10 k relating to all incidents in the last financial year. For all businesses, median costs are zero, mean costs are AUD 699, and maximum costs are AUD 600 k. However, costs are higher, if those that did not experience cyber incidents are excluded (mean of: small businesses: AUD 2,431; medium: AUD 12,405; large: AUD 49,246). The top three industries, which include manufacturing (mean: AUD 13,295), retail trade (mean: AUD 9,870) and administrative and support services (mean: AUD 5,790), demonstrate the highest costs.

The DCMS (2020) surveyed 1,685 organizations. Across all organizations, median direct costs (including staff being prevented from carrying out their work; lost, damaged, or stolen outputs, data or assets; lost revenue) relating to the most disruptive attack in the last 12 months are zero, which reflects the fact that most breaches or attacks do not have any material outcomes. Average direct costs for micro/small businesses (median: £0, mean: £580) are lower than for medium/large businesses (median: £0, mean: £1,090).

Ponemon/HP (2016) state that costs of cybercrime are rising, with mean costs of $9.5 M, median costs of $6.7 M and minimum costs of $270 k evident across mainly large organizations around the globe. Accenture/Ponemon (2019) also state that total costs are rising and report average annual costs of $13 M for mainly large organizations. According to Cisco (2019), 33% of organizations worldwide with more than 100 employees paid less than $100 k following their most severe breach and only 8% paid more than $5 M. Regarding SMEs, Kaspersky (2019) found average financial impacts of data breaches according to different attack types (e.g. DDoS: $162 k, targeted attacks: $138 k, malware infection: $117 k) and cost types (external support: $14 k, lost business: $13 k, compensation: $5 k, fees: $4 k). IBM/Ponemon (2020) state that average total costs of data breaches for mainly large organizations are $3.9 M worldwide, although high regional differences exist. Costs are highest in healthcare ($7.1 M), energy ($6.4 M) and finance ($5.9 M). Loss of business (mean: $1.5 M), along with detection and escalation (mean: $1.1 M), are the highest cost categories. According to Hiscox (2020), the median cost to the 1,971 primarily SME companies that suffered cyber incidents over the past 12 months increased and was $57 k (>1,000 employees: $504 k). Energy ($337 k), finance ($166 k), and manufacturing ($100 k) are the industries with the highest median costs. On average, a ransomware attack costs $927 k, while other malware costs $492 k.

A direct comparison of the reported costs of the aforementioned literature is not possible due to the different populations and diverse operationalizations. Apart from Romanosky (2016) and Eling and Wirfs (2019) who, due to their sampling databases, only analyzed major incidents, costs reported by commercial literature tend to be higher compared to academic and governmental research. To summarize our findings, we conclude that there is generally little research on the topic of costs of cyber incidents within organizations. Whilst academic research lacks representative samples, governmental research lacks an ISM focus and commercial literature lacks transparency and representativeness, especially for organizations based in continental Europe. Due to the shortcomings of the existing literature, we have conducted our own field research.

3. Findings from the large-scale survey

In this section, we report on the operationalization and findings of our large-scale survey which, in contrast to our official project report (Dreissigacker *et al.*, 2020), focuses on the costs of cyber incidents. From August 2018 until January 2019, we carried out CATI mainly with IS/IT-managers and board members of 5,000 organizations in Germany that had more than nine employees.

3.1 Research method

3.1.1 Research question and focus. Given the connection to a government-funded initiative to improve IT-security for SME, the focus on organizations was apparent. The research questions were derived from a literature review (see Dreissigacker *et al.*, 2020), seven expert interviews with practitioners from German cyber security related authorities (Stiller *et al.*, 2020), as well as discussions with the project-own-regional business advisory council. This council was founded as a "sparring partner" to the project team in order to ensure the practical relevance of research throughout the three-year research project. The council consists of representatives from a variety of local medium-sized companies and security authorities.

3.1.2 Selection of method. The CATI survey method was chosen because, in comparison to postal and online surveys, the desired target persons (i.e. managers responsible for IT/IT-security or board members) can be reached more quickly and with greater accuracy.

By means of technical guidance and individual support provided by experienced and trained interviewers, inquiries could be answered right away, which has a positive effect on the overall quality of the data (Steeh and Charlotte, 2008). Moreover, computer-assisted complex filter guidance ensures that the survey can be conducted efficiently (Lavrakas, 2008). In addition, telephone interviews using list samples have shown acceptably high response rates (Steeh and Charlotte, 2008).

3.1.3 Population. The sample population consists of all enterprises that are listed as independent legal entities with their headquarters in Germany and who have more than nine employees. The exclusion of micro-enterprises has research-pragmatic reasons, insofar as they are subject to relatively significant changes (e.g. insolvency, establishments), which can negatively influence the availability of contact information. Approximately 3.5 M German companies were registered in 2017, of which 89.3% are classed as micro enterprises. When considering the remaining 370 k organizations (10.7%), the largest proportion are organizations with 10–49 employees (78.8%), whereas organizations with more than 250 employees only represent 4% of the organizations in Germany that have more than nine employees (Destatis, 2017). However, the organizations in our sample represent approximately 81.5% of all employees in Germany (Dreissigacker *et al.*, 2020). Based on a representative survey of German SMEs in 2017, it can be assumed that almost all (94%) organizations in Germany have workplaces with Internet access (Hillebrand *et al.*, 2017), meaning that cyber security is thus a relevant topic.

3.1.4 Sample. We used a stratified random sample of 5,000 organizations. In order to ensure that sub-populations of interests (e.g. organizations with more than 500 employees) were adequately represented in the sample, a disproportionately stratified sample was drawn according to a quota plan (Table 1) [3]. Large organizations and organizations providing services of general interest are thus more strongly represented in the sample than in the population (oversampling).

We targeted respondents working as members of executive boards and within IS/IT since we assumed that they are most likely able to provide information on cyber incidents. This target group could be reached for the most part (see Table 1), with small organizations being more likely to be represented by executive members and larger organizations being more likely to be represented by individuals responsible for IS/IT. Based on the experiences of the survey institute, as well as discussions in our project-own advisory council, we refrained from asking for standardized and more detailed job roles as these are less prevalent within German SMEs.

Since, apart from executive members ($N = 212$) and IS/IT members ($N = 526$), only few participants actually reported on cyber incident costs (data protection ($N = 16$); plant safety/security ($N = 1$); internal audit ($N = 5$), other ($N = 45$), not specified ($N = 0$)), we grouped these interviewee positions together ("other").

Although it is possible to reproportion our sample using sector and employee class weights, we did not do this in the following analysis because sector and employee class will be controlled for. In addition, our focus lies on cost benchmarks for certain groups and not on representative statements for all organizations in Germany. The sample was drawn from two commercial business databases "Bisnode" and "Heins and Partner", which included the industry assignment according to the German WZ08-classification, which allows for international comparison.

3.1.5 Questionnaire. The interview was based on a questionnaire containing 40 questions on the occupational function of the interviewee and related risk perceptions, cyber-attacks detected within the last 12 months, technical and organizational security measures deployed in the organization, as well as demographic characteristics of the organizations. However, more detailed questions on the most severe cyber incident experienced in the last 12 months were acutely targeted. Particularly the data from this section forms the basis of our analysis

	10–49	50–99	100–249	250–499	>500	Public services	Total
Targeted sample quota	1,000	1,000	1,000	1,000	500	500	5,000
Actual sample (including WZ08 Industry Classification A to S, without T,U)							
Executive/Management Board	614	292	164	78	23	Included	1,171
IT and IS	404	761	860	864	456	on the left	3,345
Data Protection	27	23	22	17	11		100
Plant Safety/Security	2	3	1	1	0		7
Internal Audit	11	10	10	4	2		37
External Service Provider	0	0	0	0	0		0
Other**	131	89	60	41	12		333
Not specified	1	3	3	0	0		7
Total	1,190	1,181	1,120	1,005	504		5,000

Note(s): * Multiple selections of occupational positions were recorded in line with the dominance order shown (e.g. a respondent doing internal audit and information security was set to information security only) ** these include the areas of finance and accounting, sales and operations

Table 1.
Sample quota plan and actual sample structure by employee class and interviewee position*

for this article. The complete questionnaire can be found in (Dreissigacker *et al.*, 2020), while an extraction on cost-relevant questions can be found in Appendix 3.

3.1.6 Survey conduction. A professional and IS research experienced survey institute conducted the CAT-interviews. The institute was chosen following an official Europe-wide tender offering. We pre-tested our survey in two phases: (1) by discussing it with our council, and (2) by interviewing six additional IT employees from organizations of different sizes and industries, predominantly by way of telephone interviews. To prepare the 141 interviewers, interview training sessions were conducted prior to the field phase in two on-site call centers. Once trained, the interviewers guided participants through the structured questionnaire using the CATI-system. Any comprehension questions and/or further explanations of terms could thus be promptly clarified by the interviewers. All responses were directly recorded in electronic form and checked against validation rules (i.e. correct sequence of questions, unrealistic values). We deliberately used straightforward and briefly formulated questions in order to enable easy comprehension. To avoid fatigue effects, we designed the questionnaire to take a maximum of 20 min. With the aim of increasing participation, we provided interviewees with an official cover letter of the Federal Ministry for Economic Affairs and Energy during the contact phase. Additionally, we ensured complete anonymity and that any data collected would be strictly limited to scientific use. Data protection contracts were concluded with the survey institute. Moreover, if desired, the questionnaire was provided to the participants prior to the interview. In order to comply with ethical standards in IS research; we followed the principles of the Menlo-Report (DHS, 2012).

3.2 Conceptualization of cyber incidents and costs

In the subsequent section, we will briefly illustrate our conceptualization of cyber incidents and their costs in order to operationalize the research object.

3.2.1 Cyber incident. Presumed that an external or internal threat initiates a cyber-attack which is either stopped by a security measure/control or leads to a IS/cyber incident by exploiting a vulnerability causing a consequence to an organization, we understand cyber-attacks leading to cyber incidents as intentional attacks against organizations that disrupt, disable, destroy or maliciously control a computing environment/infrastructure; destroy the integrity of the data or steal controlled information (NIST, 2020). Thus, the objectives of IS

(confidentiality, integrity and availability) for systems, data and processes are no longer guaranteed (ENISA, 2017).

In order to avoid exaggerated attack figures, we deliberately left out events such as junk emails, which are automatically directed to the spam folder, by asking respondents to only report attacks that required an active response by the organization, defining the term "cyber incident" for this article. Such an active response could, for example, refer to fixing software vulnerability or running certain controls.

3.2.2 Most severe cyber incident. Due to time restrictions, detailed information relating to costs, affected systems, data and other characteristics could only be surveyed for the most severe cyber incident that organizations had experienced within the last 12 months. The participants were, based on their professional judgment, asked to independently evaluate, which incident they perceived to be the most severe.

Focusing on the most severe incident, rather than the most recent incident, enables us to portray the maximum manifestation of the phenomena. Moreover, we assume that respondents would better remember the most severe cyber incident, as well as provide more precise information, than they would if having to account for a certain time period containing several different types of incidents.

3.2.3 Types of attacks. To enable a deeper analysis, we differentiate between eight attack types, which were primarily derived from the established Commercial Victimization Survey of the UK HO (2018): ransomware, spyware, attacks using other malware (e.g. viruses, botnets and exploits), manual hacking (e.g. hardware manipulation and unauthorized configuration), (D)DoS (Distributed) Denial of Service) attacks, defacing of web content, CEO-fraud and phishing. This less legal and relatively broad classification was chosen for three reasons. Firstly, the classification should be independent of specific attack vectors, techniques and tools in addition to affected domains, systems or data that can change over time. Secondly, the classification ought to be easily comprehensible and find acceptance among the respondents, as well as complement the limited complexity that is possible during a telephone interview. Thirdly, the classification should be ISM specific enough to reflect the interaction between realistic attack types and certain security measures implemented by organizations, which, in our opinion, is hard to realize using only legal definitions.

3.2.4 Systematizing costs. A variety of literature proposing frameworks or taxonomies on the consequences and costs of cyber incidents exists (e.g. Agrafiotis *et al.*, 2018). Despite this, there is no common definition and/or understanding of costs, meaning that terms are often used interchangeably (Paoli *et al.*, 2018; Florencio and Herley, 2012). To promote comparability, the cost-types used in our study are derived from the cost framework of a working group of the UK Home Office Science Advisory Council (HO, 2018), which aims to build a common understanding of the costs of cybercrime. This framework, whose logic is also used in other literature (e.g. Anderson *et al.*, 2013), differentiates between anticipation costs (e.g. purchase of antivirus software, cyber insurance), costs as a consequence of cybercrime (e.g. direct losses, infrastructure damage), and costs in response to cybercrime (e.g. compensation payments to clients). Given that we are not measuring the general operating costs of security, but incident costs only, we focus on the costs incurred as a consequence, as well as the costs incurred in response, to cybercrime. We further differentiate and delimit indirect costs (e.g. reputational damage) relating to consequence and response costs since these are hardly quantifiable and allocatable to a single incident (Wolff and Lehr, 2017).

We therefore limit our analysis to costs that are quantifiable during the course of an interview, which naturally results in limitations relating to complexity. We differentiate between six cost items reported by the interviewees (as the total amount in €) for the most severe cyber incident experienced by the organization in the last 12 months (Figure 2). The first four items are direct or cash effective costs, whereas the other two items are opportunity

costs. Costs that are not covered in our analysis include individual, social and macroeconomic costs, as well as anticipation and indirect costs.

3.2.5 Total costs. The possibility of calculating total costs (i.e. the €-sum for the six cost items) is fundamental to our operationalization in numerous ways. By in–or excluding observations, we differentiate between two variations of costs: (1) "Secured total costs" only include organizations that gave valid (yes or no) statements to all six cost items. In doing so, we prevent the underestimation of costs. By excluding cases with zero costs, we represent the upper range of costs. (2) "Unsecured total costs" include organizations reporting at least one cost item, no matter if another item is reported as unknown or not specified. By including cases with zero costs, we represent the lower range of costs.

3.3 Empirical results

3.3.1 How many organizations are affected by, and report the related costs of, cyber incidents?. Apart from the question of "what costs do organizations suffer?", we believe that it is crucial to understand the ground upon which these findings are based. In order to allow for a brief and transparent overview, we plotted a filter-path diagram (Figure 3) from the population behind our sample to subgroups of interests, including the frequency of observations, as well as percentage shares based on different filter paths.

We contacted 43,219 organizations to reach our targeted sample of 5,000 organizations, which corresponds to a response rate of 11.6%. Out of the 5,000 organizations interviewed, 2,004 (40.0%) organizations reported experiences of a most severe cyber incident within the last 12 months. Further, 130 (2.6%) respondents said they did not know, whereas 2,866 (57.3%) organizations did not report a severe cyber incident. Of the organizations that did not report a cyber-incident in the last 12 months, 26.4% (n = 1,320) had never experienced a cyber-incident in which an active response was required. In comparison to large + organizations (13.5%), small organizations (38.6%) were significantly more likely to state that they had never experienced such an incident. The overwhelming majority of organizations (1,937 of 2,004) provided valid statements in response to the cost items (yes or no), whereas 67 organizations gave only partially valid answers (yes, no, do not know, not specified). None of the organizations solely responded with "do not know" or "not specified". More than a quarter of the sample reported at least one cost item, and a further 19.9% quantified actual €-costs. This indicates that organizations, which had reported a severe cyber incident, show the ability or willingness to provide information on costs. Interviewees were mainly responsible for IS/IT (66.9%) or were members of the management board (23.4%). As the company size increased, the proportion of management interviewees decreased, whereas the proportion of IT interviewees increased. Looking at the actual €-costs, smaller organizations were more likely to not report a severe cyber-attack, but at the same time, were less likely to report severe attacks with no related costs. In contrast, larger

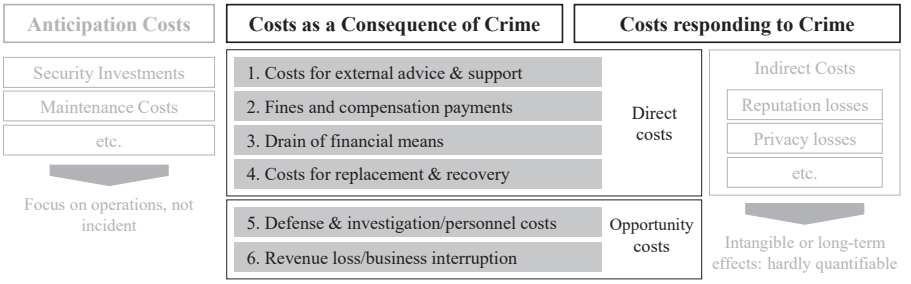

Figure 2.
Direct and opportunity costs of cyber incidents on an organizational level

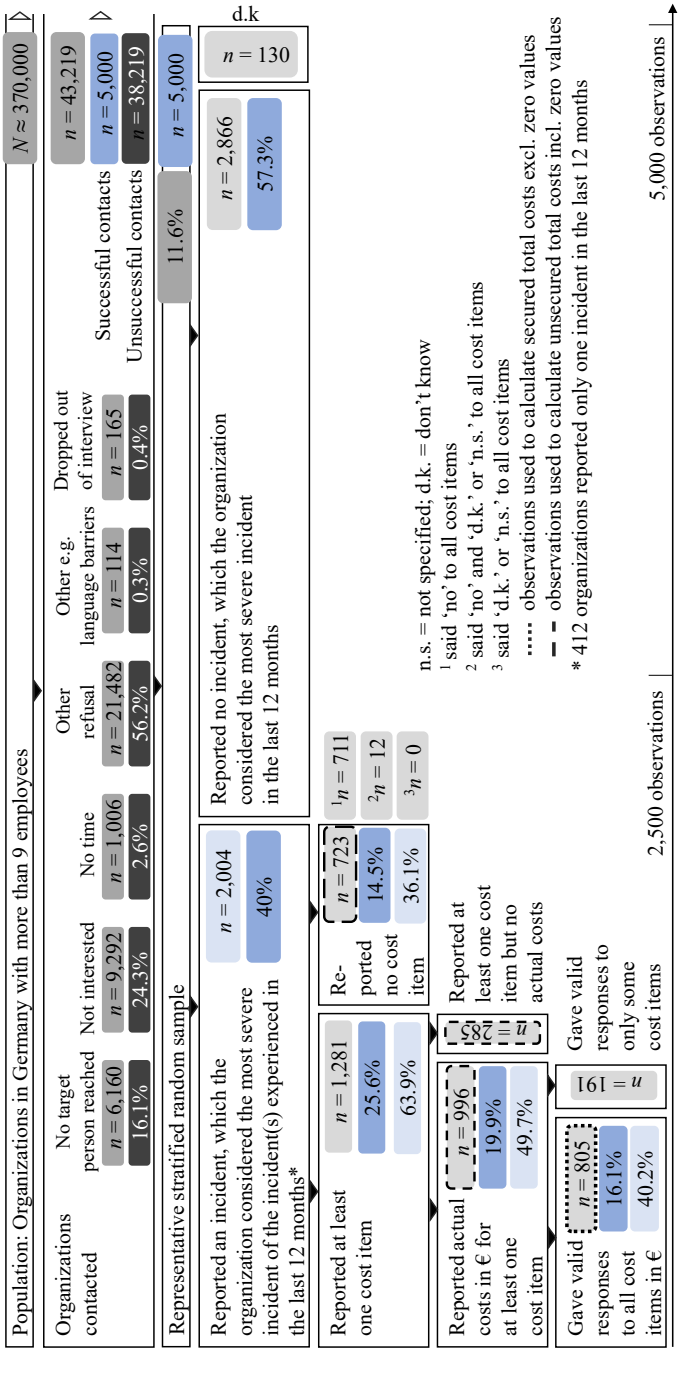

Figure 3.
Filter-path diagram of observations focusing on the costs of cyber incidents

organizations were more likely to report their most severe attacks, but were also more likely to report attacks that did not cause any costs. Proportions of reported actual costs ultimately lie between 17.8% and 24.0%, showing no significant differences. However, applied Chi-square-tests indicate significant group differences within the size of organizations that reported no €-costs, no costs at all or organizations reporting no severe incidents (Figure 4).

With regard to industries, significant group differences exist among organizations reporting €-costs, with organizations from the information sector (WZ08-J classification) showing the highest proportion (25.0%) and organizations from the finance industry (10.5%) showing the lowest (Figure 5).

Besides the characteristics shown, it is possible that there are other factors that can describe the attributes of organizations who report costs of cyber incidents. When taking the proportion of organizations that reported actual €-costs (19.9%, see Figure 3) into consideration, there are few differences between certain company characteristics, such as whether an organization has critical infrastructure (23.1%; $n = 627$), whether the organization exports (21.7%; $n = 1{,}997$), and whether it has locations abroad (24.8%; $n = 699$). However, when considering whether an organization has certain security measures, such as business continuity plans (45.8%; $n = 1{,}259$), certifications (47.1%; $n = 467$) or staff training (46.2%; $n = 1{,}090$), in place, the proportions of reported costs double. Therefore, the willingness or ability of organizations to provide cost information seems to depend less on what the organization embodies in terms of structural company characteristics, but more on what the organization does in term of IS arrangements.

3.3.2 Which cyber incidents do organizations report to be most severe?. Overall, organizations are not equally affected by attack types and do not show equal distributions relating to employee classes. Organizations have been primarily affected by phishing (25.8%), ransomware (25.6%) and other malware (18.0%), but less by CEO-fraud (12.3%), (D) DoS (6.2%) and Spyware (5.5%), and rarely by manual Hacking (2.6%), Defacing (2.0%) or a

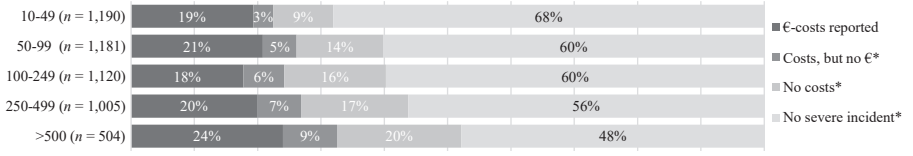

Figure 4.
Portions (%) of organizations reporting costs of most severe cyber incident by employee class; *$p < 0.05$ (Chi-square)

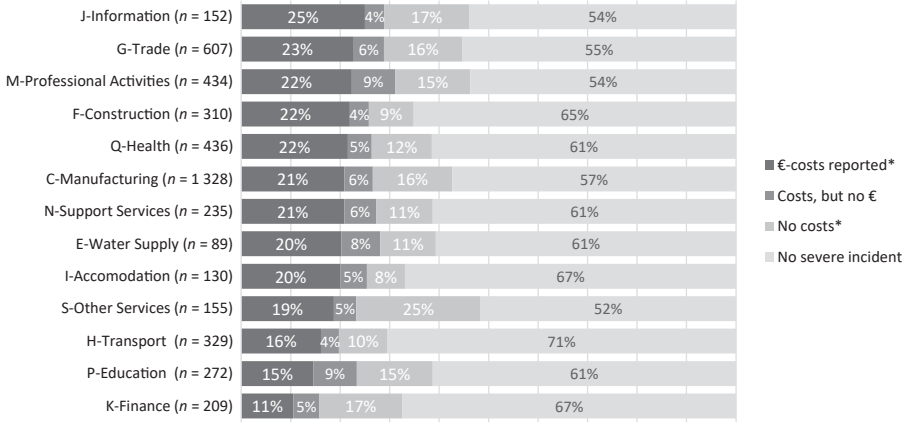

Figure 5.
Proportions (%) of organizations reporting costs of the most severe cyber incident by WZ08 industry classification; *$p < 0.05$ (Chi-square); excl. WZ08-A,D,L,R due to low observations

combination of attack types (1.5%; see Appendix 2, Figure A1). Besides our eight predetermined attack types, almost no other attacks were reported (0.2%). There are some significant differences regarding company size (no overlapping confidence intervals with $\alpha = 5\%$). In comparison to large + organizations, small organizations more frequently report spyware as their most severe incident (8.4% vs 3.4%). The use of other malware also shows a significant difference between small and large/large + organizations (24.2% vs. 12.7%/12.5%). It is thus reasonable to assume that larger organizations have better measures in place for filtering out malware. Moreover, it seems plausible that CEO-fraud is reported significantly more often by large organizations since this attack requires a certain level of anonymity within the organization, as well as larger transactions, preferably abroad, to conceal criminal activity. Phishing incidents, however, are reported frequently, and are independent of the employee class. Given that the most severe incident does not necessarily equate to the cause of significant harm, we plotted the incidents according to whether costs were reported. Although phishing has been most frequently reported ($n = 518$), 50.8% of organizations stated that no costs had been incurred and another 12.0% stated that although they had incurred costs, they cannot quantify these costs to actual € (Figure 6). Chi-square tests indicate that there are significant group differences between the reporting of attack types (€) and the reporting of attack types with no related costs.

However, there are also differences between employee classes in so far that large + organizations were less likely to report that no costs had been incurred. In addition, most organizations (55%) reported that no costs had been incurred in relation to CEO-fraud. Perceptions of CEO-fraud as the most severe incident could either be related to the feeling of being actively deceived or could simply be related to the fact that this attack was the only one experienced. Putting these numbers in the context of how often incidents had been experienced in general, it can be ascertained that attack types did not occur at the same frequency nor had the same level of impact. When considering the cases relating to certain attack types in comparison to the total amount of cyber incidents reported by organizations within the last 12 months, the proportion of experienced cyber incidents of all incidents can be determined. When considering only the organizations that reported actual €-costs ($n = 996$), 54.8% of organizations experienced at least one phishing incident (prevalence rate). Furthermore, phishing incidents account for 40.9% of all incidents, whereas incidents of this attack type only make up 19.8% of the most severe incidents. In other words, many organizations reported numerous experiences of phishing incidents, but rarely mentioned this type of attack in connection with the most severe incident. A similar pattern is evident in relation to spyware (prevalence: 30.6%; proportion of all incidents: 14.7%; most severe: 7.2%) and to a lesser extent to other malware (53.2%/27.8%/21.5%), whereas ransomware (42.2%/3.2%/31.2%), CEO-fraud (29.5%/2.4%/8.2%) and (D)Dos) incidents (18.7%/4.6%/6.7%) appear to occur less frequently, but to a more severe extent.

There are some noticeable differences regarding the employee classes. While small and large + organizations report a similar frequency of spyware incidents (21.5%/20.7%), small

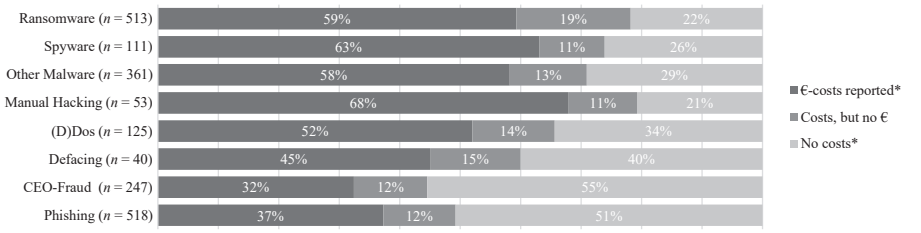

Figure 6.
Proportions (%) of organizations reporting costs of the most severe cyber incident by attack type ($n = 1{,}968$); *$p < 0.05$ (Chi-square)

organizations are more likely to report spyware as the most severe incident (11.0%), when compared to large + organizations (5.0%). This indicates that large firms are either better at coping with spyware incidents or simply consider other incidents to be more harmful. Conversely, small organizations report more phishing incidents than large + organizations (42.9%/37.2%) but are in fact less likely than large + organizations to perceive them as the most severe incident (17.7%/22.3%). One possible explanation may be that larger organizations offer more potential fraud scenarios due to their size, complexity, and anonymity of staff. Regarding the employee classes, however, there seems to be no indication of a linear relationship.

When considering the attack types according to industry sector, it becomes clear that sectors are mainly affected by ransomware; other malware and phishing (see Appendix 2, Table A2). C-manufacturing and E-water supply sectors; where the other malware is replaced by CEO-fraud, constitute exceptions to this finding. Some variance is apparent when focusing on the highest value according to attack type. Ransomware accounts for the highest proportion within water supply, which may be a result of targeted attacks on critical infrastructure. Water supply also has the highest value for CEO-fraud, which is surprising since this sector is not commonly known for large organization sizes and international transactions. Due to the low number of water supply cases ($n = 35$), further investigation is difficult. The same applies to accommodation ($n = 41$), which shows the highest values for spyware (14.6%) and manual hacking (7.3%). Here, it would be conceivable that attacks are mainly aimed at guests and their personal or credit card data. It seems plausible that (D)DoS attacks predominantly target information and communication sector organizations (15.7%), whereas phishing attacks show the highest proportion in the finance sector (39.7%).

3.3.3 Which costs arise, and to what extent, once organizations experience the most severe cyber incident?. 3.3.3.1 Cost items. Out of the 2,004 organizations that reported a severe cyber incident, 723 (36.1%) stated that they did not suffer any of the six cost items. Organizations generally reported one (29.1%) or two (22.1%) cost items, while only 3% reported between four and six items. For all employee classes, members of the management board were more likely than IS/IT-managers to report at least one cost item, whereby the difference within small organizations is significant (IT: 62.8% vs 79.8%). When inquiring which cost items were experienced, the largest proportion of organizations referred to costs relating to immediate defense and investigation/personnel costs (36%), followed by replacement and recovery costs (27.3%), costs for external advice and support (24.5%), as well as business interruption/revenue loss (23.3%). Drain of financial resources (2.5%), as well as compensations and fines (1.3%), seem to play an indirect role. Focusing on the average costs of the most severe incidents, as reported by organizations that suffered actual costs, drain of financial resources (31,503€) and business interruption (23,372€) show particularly high values (see Appendix 2, Table A3). Costs for external advice and support, in contrast, seem to be negligible (3,222€). However, the assumption that the total costs rise with the employee class cannot necessarily be applied to all underlying costs items since large + organizations do not show the highest, and small organizations do not show the lowest, values for each cost item.

3.3.3.2 Ransom demand. Apart from the six cost items, we also asked participants to report ransom demands. Out of the 2,004 organizations, 339 (16.9%) stated that they had received a demand to pay ransom money, whereas 90 (4.5%) organizations did not know and three did not want to comment. While the largest proportion of ransom demands is associated with ransomware incidents (72.8%), other malware (9.7%), phishing (6.5%) and CEO-fraud (6.2%) incidents were also reported to have required ransom. When asked to quantify the ransom requests, 239 organizations reported actual €-amounts. Excluding one outlier observation, which reported a €100 M ransom demand regarding a ransomware attack in a construction sector organization with 100–249 employees, ransom demands averaged at 80,489€

(n = 238), with a median of 5,000€. Ransom demands ranged from 100€ to €5 M. Ransomware incidents have an average demand of 55,192€ and a median of 5,000€ (n = 160). Looking at employee classes, no linear tendency is apparent. When inquiring whether organizations had paid the ransom money, only eight (2.5%; n = 339) participants responded with "yes", while 329 (94.1%) said "no". The total sum of the eight cases in which ransom money was paid is €152 k, which could be counted as part of the criminal revenue of attackers. Five organizations stated that the attackers stopped the attack after the money was paid, two did not know, and one said the attack did not cease.

3.3.3.3 Total costs. When analyzing the total costs of a cyber-incident, we show the costs relating to all attack types and employee sizes according to the two variations outlined before (Table 2). The average costs vary between 20,348€ (median: 1,400€; n = 805) for secured total costs (excluding zero costs) and 9,922€ (median: 0€; n = 2,004) for unsecured total costs (including zero costs). The range of secured total costs reported by organizations is wide and reaches from 10€ to over €2 M. The lower median values indicate that a large proportion of organizations suffer low costs, whereas few organizations suffer large costs. However, for those organizations that suffered actual costs, the total costs tend to rise with the organizational size. Although the frequency of observations in relation to some reporting dimensions is too low for further analysis, the total costs vary by attack types. Manual hacking (50,111€), CEO-fraud (38,816€) and (D)DoS-incidents (35,457€) show the highest secured average costs. Applied t-tests conducted between attack types, employee classes and interviewee occupational position predominantly show no significant differences for both variations of total costs since some bins contain few observations and costs are not normally distributed. When industries are considered, there tend to be some differences, although sample sizes do become very small. Accommodation (median: 3,600€), water supply (median: 3,500€) and professional activities (median: 3,000€) show the highest secured total costs, while agriculture (median: 120€), public administration (median: 125€) and mining (median: 500€) show the lowest (see Appendix 2, Table A4).

The assumption that few organizations suffer high costs and most suffer low costs can be visualized using the classified total costs (Figure 7). Regarding unsecured costs (including zero costs), every second organization reporting their most severe incident stated that they had not suffered any costs. Small organizations (39%) reported no costs significantly less frequently than medium + organizations (54%).

In total, only 3.1% of the organizations reported total costs above €50 k. This result is consistent with former research, which found that outcomes and costs of cyber incidents are heavy-tailed distributed (Makridis and Dean, 2018; Edwards *et al.*, 2016; Eling and Wirfs, 2019).

In cases where actual costs had been incurred, an interesting difference regarding the interviewees is evident. While management board members were more likely to report at least one cost item, the average total costs across all employee classes reported by IS/IT-interviewees tended to be above those values reported by management interviewees (see Appendix 2, Table A6). In total, IS/IT-members reported average secured total costs of 24,071€, whereas management members reported average costs of 13,259€. Since median values relating to medium+ and large organizations show the opposite direction, it might be possible that IS/IT-members are more likely to report more extreme values.

Besides the variables discussed, there may be more factors influencing the costs of cyber incidents. In cases where organizations report the involvement of non-public client data within their most severe incident experienced in the last 12 months, the average total costs sum up to 29,003€, whereas average costs are only 7,725€ if no such data is affected. Organizations without IT-certifications suffer average costs of 56,100€, while organizations with IT-certifications only report average costs of 10,950€. Since these bivariate comparisons cannot analyze which factors are causes and which ones are effects, and additionally

		Secured total costs excl. zero costs						Unsecured total costs incl. zero costs					
		Total	10–49	50–99	100–249	250–499	>500	Total	10–49	50–99	100–249	250–499	>500
Ransom–ware	avg	19,380	30,646	7,566	15,935	25,246	12,737	10,797	18,684	5,720	10,581	12,734	6,201
	med	2,000	1,300	1,300	1,550	2,000	2,005	400	900	700	59	300	500
	n	*221*	*43*	*47*	*40*	*65*	*26*	*513*	*78*	*103*	*120*	*139*	*73*
Spyware	avg	6,347	10,728	5,440	3,480	2,535	3,040	3,654	7,197	3,533	1,624	1,193	1,722
	med	1,600	750	1,575	3,000	1,650	1,200	400	500	475	0	0	1,000
	n	62	21	18	10	8	5	*111*	*32*	*28*	*25*	*17*	*9*
Other Malware	avg	12,728	8,822	15,968	15,742	7,198	17,715	7,253	5,531	10,455	7,572	3,138	9,172
	med	1,000	750	1,000	1750	1,200	500	200	300	400	0	0	200
	n	*172*	*54*	*43*	*36*	*22*	*17*	*361*	*92*	*93*	*87*	*56*	*33*
Manual Hacking	avg	50,111	37,900	11,443	108,411	32,500	5,667	32,396	31,708	6,177	64,400	13,333	4,250
	med	2,900	2,800	2,000	2,000	32,500	5,000	1,000	2,000	300	1,000	5,000	3,500
	n	*28*	*7*	*7*	*9*	*2*	*3*	*53*	*12*	*13*	*18*	*6*	*4*
(D)DoS	avg	35,457	18,525	57,289	9,609	15,595	164,040	20,990	10,756	22,795	4,805	21,514	73,177
	med	1,500	1,100	2,000	1,000	4,003	1,200	100	100	125	34	0	5,000
	n	*55*	*18*	*9*	*13*	*10*	*5*	*125*	*31*	*24*	*26*	*31*	*13*
Defacing	avg	2,203	2,788	2,333	1,633	600		1,035	1,367	714	900	1,433	0
	med	1,245	990	2000	500	600		0	100	0	0	0	0
	n	*12*	*5*	*3*	*3*	*1*		*40*	*11*	*11*	*11*	*6*	*1*
CEO-Fraud	avg	38,816	1,449	2,381	14,521	93,489	30,222	11,054	486	1,114	3,721	34,291	6,034
	med	1,000	500	500	750	1,250	5,500	0	0	0	0	0	0
	n	*68*	*7*	*15*	*12*	*22*	*12*	*247*	*22*	*50*	*50*	*61*	*64*
Phishing	avg	18,997	5,539	37,199	19,919	4,481	24,962	7,541	3,136	14,232	6,497	1,546	12,700
	med	1,100	1,000	1,800	1,000	1,000	1,750	0	0	0	0	0	0
	n	*172*	*35*	*46*	*30*	*37*	*24*	*518*	*96*	*136*	*106*	*117*	*63*
Other	avg	41,567	41,567					24,940	41,567	0	0		
	med	4,000	4,000					700	4,000	0	0		
	n	*3*	*3*					*5*	*3*	*1*	*1*		
Combined attacks	avg	8,592		3,500	1,150	27,000		5,697	18,333	3,227	729	11,571	0
	med	1,500		3,000	1,000	2,000		400	0	1,000	600	0	0
	n	*12*		*5*	*4*	*3*		*31*	*3*	*11*	*7*	*7*	*3*
Total	avg	20,348	15,341	18,172	19,878	25,557	26,592	9,922	8,992	9,196	9,186	11,535	11,123
	med	1,400	1,000	1,300	1,500	1,650	2,000	0	250	100	0	0	0
	n	*805*	*193*	*193*	*157*	*170*	*92*	*2,004*	*380*	*470*	*451*	*440*	*263*

Table 2.
Total costs (€) of most severe cyber incidents in the last 12 months by attack type and employee class; avg = average; med = median; *n* = count of observations

disregard mediating, moderating or confounding variables, further inferential analysis is needed to understand how these costs are incurred.

4. Discussion of implications and activity plan

The following discussion is divided into two parts. Based on our results, we firstly discuss the content-related implications for organizations. Subsequently, we draft an activity plan on a meta-level, which is based on the question of how the information base relating to costs of cyber incidents can be improved to enable better decision-making.

4.1 Implications

Our empirical findings show that cyber incidents and associated costs are dependent upon individual company characteristics and thus constitute a complex research field (Table 3).

These results can serve as benchmark for SMEs and thereby influence the ISM decision-making process of many organizations. Our findings demonstrate that direct costs of cyber incidents can be extreme for German SMEs. Nevertheless, a large proportion of organizations report little to no direct costs for the most serious incident in the last 12 months. The field of research, however, remains complex. On the one hand, differences in interviewee response behavior seem to indicate that the organizations' representatives are of relevance. More often than IS/IT-interviewees, board members tend to report at least one cost item. Simultaneously, IS/IT-interviewees report higher average total costs across all employee classes. This could indicate a lack of common understanding or transparency regarding cyber incidents and their costs within organizations. Such a common understanding, however, is the basis for proper ISM and investment calculations and should at least exist among management board and IS/IT-managers.

On the other hand, the size of an organization seems to be another important factor when examining cyber incidents. Large + organizations, in comparison to small- and medium-sized organizations, were significantly more likely to report the occurrence of a severe cyber incident. Apart from the possibility that these organizations evaluated the incidents differently, it seems plausible that large organizations simply experience more cyber incidents. While smaller organizations were more likely than larger organizations to report

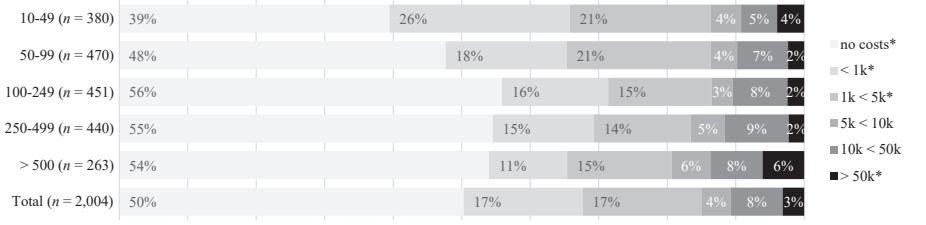

Figure 7.
Proportions (%) of classified unsecured total costs (€) in thousands, including zero costs, *$p < 0.05$ (Chi-square)

1. Cyber incident costs are extremely distributed: Most organizations report no or little costs, few report very high costs
2. Cyber incidents and associated costs appear to be dependent on individual company characteristics, but also on the types of attacks
3. Smaller organizations less often report severe incidents, while larger organizations report more often severe incidents but less often actual related costs. Ultimately, the proportions of actual costs reported after severe incidents are similar
4. IS/IT manager and board members seem to report differently on costs of cyber incidents

Table 3.
Summary of implications

spyware and other malware as the most severe incidents, larger organizations were more likely than smaller organizations to report ransomware and CEO-fraud. Possible reasons for larger organizations experiencing a greater number of severe cyber incidents could be a higher visibility, a more complex and larger IT-infrastructure, as well as the involvement of more agents in terms of staff, vendors, clients, etc. However, large organizations tended to report less actual costs related to the most severe incident, meaning that organizations of all employee classes make up similar proportions of organizations that reported actual €-costs. This might suggest that large organizations indeed report more severe cyber incidents but, at the same time, have better measures in place to reduce harm.

We found that cyber incidents can lead to extreme damages and therefore need to be taken care of by management boards. Although costs differ across certain characteristics, we found that average direct and opportunity costs relating to the most severe incidents seem manageable (secured total costs: mean 20,348€, median 1,400€; unsecured total costs: mean 9,922€, median 0€) and only affect a small proportion of organizations. It must be noted that although these findings only relate to one cyber incident, only cover the last 12 months, and neglect any further indirect costs, they are nevertheless in line with other representative literature that has found the costs of cyber incidents to be relatively low (Rantala, 2008; Richards, 2009; DCMS, 2020), when compared to statements of commercial institutions. Given that many organizations already have organizational and technical security measures in place, yet are still affected by cyber incidents (Dreissigacker *et al.*, 2020), it is possible that successful past attempts at fighting cybercrime may make the costs appear low because organizations had previously prepared themselves (also see DCMS (2020)). However, as large gaps in knowledge persist, further differentiated research is needed.

4.2 Activity plan

The discussion is based on the question of how the information base relating to costs of cyber incidents can be improved to enable better decision-making. We have thus drafted an activity plan, containing action items and further research topics, for the three agents: organizations, government/society and academia (Figure 8). Our activity plan outlines some practical steps for the three agents to generate better information and use such existing information more constructively. We use a triangulation approach to derive items for the action plan. These data sources include our data-based results, qualitative aspects of discussions with our project-own-regional business advisory council, project stakeholders and other

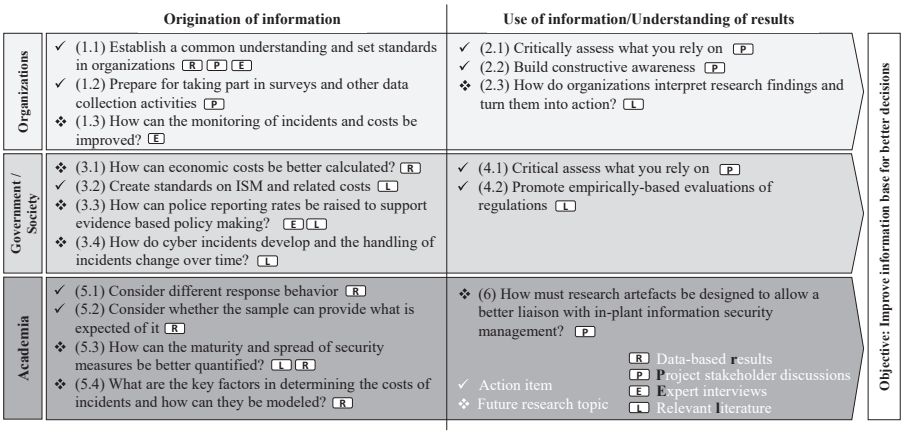

Figure 8.
Activity plan (action items and further research topics)

organizations, as well as expert interviews with seven representatives of different German security authorities in tandem with findings of relevant literature. The items within the action plan were derived throughout the whole research process, starting from population and sampling to the interpretation of outputs.

When considering what organizations could do to improve the general information base relating to costs of cyber incidents, it is particularly important to establish a common understanding regarding the definition of cyber incidents (1.1) among relevant staff and to ensure incidents are treated fairly within the organization. The occasional variations in responses between management board members and IS/IT-managers suggest that there is a lack of transparency or priority among relevant agents. Discussions with our advisory council revealed that management and IT participants have varying perspectives on cyber incidents occurring within their own organization flanked by findings of our expert interviews organizations still show a general lack of awareness with regard to IS (Dreissigacker *et al.*, 2020; Stiller *et al.*, 2020). Through the development and establishment of common frameworks and standards of IS, the government and society could support this attempt to build a prevalent understanding of IS and associated costs, not only within, but also across organizations.

Although our findings did not show substantial proportions of "do not know" or "not specified" survey responses, it is recommendable that interviewees prepare themselves (1.2). During the pre-testing phase, organizations and project stakeholders indicated that, for some questions, prior information or approvals may need to be obtained. Since interviewees represent their whole organization, they have a large responsibility in so far that a broad participation of unprepared or uninformed interviewees might systematically distort the survey findings. Future research should examine how organizations can be more precise but also more straightforward in the monitoring and tracking of incidents and their consequences within their operational accounting/controlling, including practical definitions, approaches and tools (1.3). Our results show that there are organizations that report incurred costs, yet do not quantify them. Additionally, other research finds few organizations have mechanisms in place to monitor costs of security breaches (DCMS, 2017). The distinction between operational costs and costs incurred by cyber-attacks is difficult to capture in survey situations, which is particularly true for large organizations. Additionally, more research is needed in how far indirect costs, such as reputation or information losses, can be better operationalized, quantified and integrated within the ISM. Focusing on what can be done to improve the handling and interpretation of information on an organization level, we suggest that organizations must either develop greater awareness or the competency to critically assess any external information they rely on (2.1). During presentations of our project at public events, as well as content-related discussions with project stakeholders, we often noticed a focus on the reporting of raw results and the tendency to treat all information sources as equivalent and comparable. Furthermore, an adequate understanding of how such information is created in terms of premises, sampling, operationalization, interpretation and limitations is important (Biemer, 2010; AAPOR, 2016). Some project stakeholders indicated that they are aware of cyber-attacks but feel powerless in the face of the almost unmanageable threat, while others stated that they do not consider cyber-attacks to be a substantial risk for their respective organizations (Stiller *et al.*, 2020; Dreissigacker *et al.*, 2020). An enlightened and constructive awareness that helps to promote IS compliant behavior thus seems necessary (2.2).

Besides this, it is crucial to better understand how organizations, especially small ones, use information on cyber-attacks and whether and how they derive concrete actions from it (2.3). There are indications that the information sources used by organizations differ depending on organizational size, but also on the person using the sources (Dreissigacker *et al.*, 2020). In line with this, research artefacts could be created in a more targeted way.

Due to the lack of scientific literature, a risk exists that organizations and governmental institutions rely on information sources that are non-transparent regarding their methods and/or results and may even be driven by individual motivations. When examining the economic costs of cyber incidents, for example, we noticed the use of non-representative samples that had been extrapolated in a linear manner without considering distributional and compensation effects, which led to extreme values. Given that our results showed that only a small group of organizations suffered large direct costs, while many organizations suffered little or no costs at all, the extreme amounts of economic damages published by commercial author groups seems debatable, at the very least. Effects such as revenue losses resulting from system failures due to a cyber-incident within organization "x", which could lead to higher sales of organization "y", and may thereby offset the economic costs at the national level, are not taken into account. Therefore, we assume a need for better information on valid economic costs of cyber incidents (3.1), as well as research that can validate survey findings using different scientific methods. In order to measure the economic costs of ISM, there is a need for consistent standards (3.2), which are repeatedly proposed by various actors but so far, have not been widely adapted within the society and economy (Agrafiotis *et al.* (2018); Paoli *et al.* (2018)). In addition to academic taxonomies or risk management standards, this also refers to police and other official statistics publications, as well as accounting standards. Such standards could in turn raise awareness and establish a common understanding within organizations, bring ISM/risk management and corporate management/accounting/controlling closer together to unleash synergies, as well as improve the quality and homogeneity of data and therefore raise cross-border comparability of information on the phenomenon.

Since the information value of existing police statistics is limited (Buil-Gil *et al.*, 2021), governments are facing the challenge to raise criminal reporting rates (Dreissigacker *et al.*, 2020) in order to allow for a valid picture of the situation (3.3). Reliable statistics enable evidence-based public policy making, which is thereby not based on non-transparent literature (Wolff and Lehr, 2017). Therefore, costs should be systematically recorded and, if needed, updated following the completion of forensic checks on police recorded cyber incidents. In addition to improving the police's reputation and removing the fear that the police might investigate the entire IT infrastructure of an organization that has reported a cyber-incident (DCMS, 2017), fast and efficient reporting mechanisms must be implemented. Given that cyber-attacks are a cross-border phenomenon (McGuire and Dowling, 2013) and (international) cyber incidents are insufficiently recorded within official police statistics (Buil-Gil *et al.*, 2021; Dreissigacker *et al.*, 2020), a permanent exchange of threat and incident data, at least between European member states, should be introduced.

On the societal level, it is necessary to gather representative and standardized panel data or, at least, more periodic crime research to address the rapidly changing nature of the phenomenon (e.g. development of costs, new attack vectors, ISM maturity or the shift of offline to online crime (3.4)). For this purpose, it would make sense to approach organizations as well as private users to capture both organizational and individual aspects of cyber incidents, which would further improve our understanding of interactions and distinctions.

Just like organizations, society and public authorities must spread awareness or build competency to critically deal with externally provided information (4.1). In this context, appropriate methods and criteria should be applied to validate that information. As stated in recent literature, the development of public regulations in a democracy should be fact-based, transparent and public (Wolff and Lehr, 2017). We note that this does not only apply to the initial creation of the law, but also for periodic evaluations of effectiveness (4.2), which should be supported by societal or government initiatives.

Particularly with regard to the different response behaviors of participants (5.1), questions and possible answers should be carefully chosen and pre-tested by representatives of all targeted groups. Looking at our survey, it seems possible that participants evaluated the

most severe incident differently. These tendencies are also partly evident within our results, insofar that board members tended to state more often at least one cost item. Important future research, at this point, would relate to the question of which type of interviewee should be asked about which topics (e.g. ask board about reputation losses, but IS/IT-members about prevalence rates). Another reason to pay more attention to socio-cultural aspects of participants and their organizations is that organizations that put greater effort in IS are more likely to agree to participate. On the other hand, organizations that are unaware or disinterested in IS may refuse participation on the basis that the topic is of little relevance to them. In this context, it must be closely considered what information the targeted survey sample is expected to provide (5.2). On the basis of our observations and the filter-path diagram (Figure 3), researchers must, on the one hand, assume a comparatively low participation rate and on the other hand, assume lower observations when drilling into certain aspects. Even with a large sample of 5,000 observations, we quickly reached the limit of statistical evaluation possibilities when analyzing data across several dimensions (e.g. attack type and employee class). A solution would be to determine the required sample size and statistical power in advance using suitable estimators and the desired evaluation dimensions/associations.

With regard to future survey research, we believe it is important to not only better understand what measures organizations already use, but also the maturity and extent of such measures within the organization (5.3). Since the use of standard technical security measures seems widely distributed (Dreissigacker *et al.*, 2020), we suspect a higher variance in prevalence rates and associated costs when looking at how effective these measures are. Related to this, more multivariate statistics (see Skarczinski *et al.*, 2022; Skarczinski *et al.*, 2021; Huaman *et al.*, 2021) are needed to understand how the described variables are connected and to identify which ones are technical, organizational or individual risk or protective factors in determining the costs of cyber incidents (5.4). With the aim of developing and implementing ISM measures, such as cyber insurance, further evidence-based statistical modeling of costs is needed (Eling and Wirfs, 2019).

Based on discussions with the project-own-regional business advisory council, we believe it is important to help readers make better use of academic research findings. In addition to general transparency and comprehensibility, this also includes the possibility of transferring research results to individual organizations. In this context, we assume that there is a need for future research to analyze how research artefacts should be designed to allow for a better liaison with the in-plant ISM of organizations (6). This could refer to the use of certain KPIs in security reporting and monitoring, a greater consideration of accounting-related requirements (e.g. IFRS or US-GAAP), the orientation of management approaches (e.g. IT risk management according to ISO-27001 or agile IT development), or a more practical consideration of organizational structures and roles predominated in organizations.

5. Conclusion

We assume that ISM is subject to the principle of economic efficiency, which demands a balance between the costs and benefits of IS measures. Furthermore, we argued that the costs of IS measures can be determined relatively easily, whereas the benefits (i.e. avoided costs of cyber incidents) are difficult to quantify. To enable well-informed ISM decision-making, organizations and particularly SMEs, require reliable data, for which they must primarily rely on external benchmark data.

To enhance the information base on ISM, we followed a three-step approach (Figure 1). We firstly analyzed the extent to which the existing literature was suitable to serve as a benchmark for the costs of cyber incidents within organizations and identified the major findings of this literature. We found that few studies met our benchmark criteria and provided reliable data in a structured and transparent way. Whilst the academic literature

lacks large random samples, government literature used representative samples but mostly did not differentiate between ISM specific costs and attack types. Most commercial literature, however, was not transparent about the methods, samples and operationalization used and mostly did not differentiate enough between cost and attack types, as well as industry and size classes. The literature findings differ due to diverse populations and operationalizations and are therefore hardly comparable. Nevertheless, academic and governmental research tend to report lower costs than commercial literature, which has also been noted by other authors (Romanosky, 2016; Wolff and Lehr, 2017; Paoli *et al.*, 2018).

Secondly, and based on shortcomings identified in the literature, we analyzed *how German organizations are affected by cyber incidents* (RQ1), and specifically *what types of cyber incidents do organizations report as the most severe* (RQ1a) as well as *which direct and incident-related costs arise, and to what extent, following the organization's most severe cyber incident in the last 12 months* (RQ1b). We found that only two-fifths of the 5,000 organizations reported experiencing a severe cyber incident within the last 12 months. Of these two-fifths, every second organization reported that they did not incur any costs and only 3.1% reported costs above €50 k. Although we have observations with total costs above €2 M, the majority of organizations seem to be less affected than suggested by some commercial literature. Nevertheless, we found that organizations are affected differently by cyber incidents. Larger organizations are more likely to report the experience of a most severe cyber incident and also report different attack types than smaller organizations. Ultimately, secured average costs (excluding zero costs) are 20,348€ (median: 1,400€), and unsecured average costs (including zero costs) are 9,922€ (median: 0€). Since we do not have longitudinal data, we are uncertain if costs of cyber incidents have always been comparatively low for most organizations or whether past protection attempts have shown effects.

After providing these empirical results, we conducted a meta-level analysis (RQ2) on which implications can be derived from the related literature and our research to enhance the information base on costs of cyber incidents. Our implications were based on the development of an activity plan for organizations, government/society and academia (Figure 8). It should be noted that this research is not exhaustive, and that adequate ISM must consider further cost-related aspects, such as operational ISM costs, indirect costs, costs of all attacks (in contrast to merely the most severe incident), costs of unintentional incidents and safety costs. Since the aim of this research was to provide organizations with benchmark data, our work is limited to descriptive statistics. Therefore, these and other findings still need to be analyzed using multivariate approaches to better understand how cyber incidents, company characteristics, security measures, as well as individual factors are connected and play a role in determining the costs of cyber incidents.

Our work involves several limitations, of which some are inherent to our CATI-method approach. Logically, organizations could only report on the cyber-attacks that they had detected, thereby leaving out undetected attacks. Due to our focus on SMEs in Germany, the findings discussed may not be generalizable to other countries. Moreover, our analysis is based on past figures that do not necessarily reflect the future. By interviewing a single individual to represent an entire organization, the data collected may be affected by subjective attitudes, knowledge and motivations (self-reporting, social desirability, false or no statements due to the sensitive nature of information). Additionally, the reported costs are estimated by interviewees. Variations in response behavior could influence the data collected; although we could not eliminate this, it was partly addressed by controlling the interviewee. Additionally, there could be other important factors that we have not measured. For sampling, we accessed two commercial company databases. According to their self-declaration, the databases should include all registered organizations in Germany that have more than nine employees. If these self-declarations are not correct, it is possible that some organizations in the population were not given the chance to be

included in the sample. Since the structure of the sample, in terms of industries and employee classes, corresponds to the general population, we have no indication of structural biases. The possibility of a self-selection bias, relating to specific organizations generally not participating in such surveys, cannot be rejected. Our participation rate is 11.6% and thus it sits between similar IS surveys [4]. We encourage researchers to validate our findings using different research methods.

Notes

1. AISeLibrary; ScienceDirect; Google Scholar.
2. "Costs of cyber-attacks"; "Costs of data breaches"; "Impact of security breaches"; "Cost benchmark information security".
3. Sectors WZ08-O (Public Administration and Defense), WZ08-T (Activities of Households as Employers) and WZ08-U (Activities of extraterritorial Organizations and Bodies) were excluded of the sample, because they are no private sector organizations.
4. CSI (2011): 6.4% (paper and email survey); Gordon *et al.* (2018): 10% (paper survey); Paoli *et al.* (2018): 4.9% (web survey); Rantala (2008): 23% (paper survey).

References

American Association for Public Opinion Research (AAPOR) (2016), "Evaluating survey quality in todays's complex environment", available at: https://www.aapor.org/AAPOR_Main/media/MainSiteFiles/AAPOR_Reassessing_Survey_Methods_Report_Final.pdf (accessed 15 January 2021).

Accenture (2019), "The cost of cybercrime. Ninth annual cost of cybercrime study", available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study (accessed 20 January 2021).

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S. and Upton, D. (2018), "A taxonomy of cyber-harms. Defining the impacts of cyber-attacks and understanding how they propagate", *Journal of Cybersecurity*, Vol. 4 No. 1, pp. 1-15.

Anderson, R., Barton, C., Boehme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. and Savage, S. (2013), "Measuring the cost of cybercrime", in Böhme, R. (Ed.), *The Economics of Information Security and Privacy*, Springer, Berlin, pp. 265-300.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F. and Kijewski, P. (2015), "2020 cybercrime economic costs: no measure no solution", *Proceedings, 10th International Conference on Availability, Reliability and Security: ARES 2015 24-27 August 2015, Toulouse, France*, Los Alamitos, CA, IEEE Computer Society, Conference Publishing Services, pp. 701-710.

Biemer, P.P. (2010), "Total survey error: design, implementation, and evaluation", *Public Opinion Quarterly*, Vol. 74 No. 5, pp. 817-848.

Brecht, M. and Nowey, T. (2013), "A closer look at information security costs", in Böhme, R. (Ed.), *The Economics of Information Security and Privacy*, Springer, Berlin, pp. 3-24.

Buil-Gil, D., Lord, N. and Barrett, E. (2021), "The dynamics of business, cybersecurity and cyber-victimization. Foregrounding the internal guardian in prevention", *Victims and Offenders*, Vol. 16 No. 3, pp. 286-315.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. (2004), "Economics of IT security management: four improvements to current security practices", *Communications of the Association for Information Systems*, Vol. 14, pp. 65-75.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y. and Benbasat, I. (2015), "Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources", *Information and Management*, Vol. 52 No. 4, pp. 385-400.

Chari, M.D.R., Devaraj, S. and David, P. (2008), "The impact of information technology investments and diversification strategies on firm performance", *Management Science*, Vol. 54 No. 1, pp. 224-234.

Choudhury, A.S. and Kwon, J. (2016), "A study of the effect of regulations on different types of information security breaches across different business sectors", *PACIS 2016 Proceedings*, Vol. 73.

Cisco (2019), "Anticipating the unknowns. 2019 Asia Pacific CISO benchmark study: regional overview", available at: https://www.cisco.com/c/dam/global/en_sg/assets/pdfs/cisco-2019-apac-cisco-benchmark-study.pdf (accessed 20 January 2021).

Cohen, J. (1992), "A power primer", *Psychological Bulletin*, Vol. 112 No. 1, pp. 155-159.

Connolly, L.Y. and Borrion, H. (2020), "Your money or your business: decision-making processes in ransomware attacks", *ICIS Proceedings*.

Computer Security Institute (CSI) (2011), *2010/2011 Computer Crime and Security Survey*, New York, NY, available at: https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf (accessed 18 September 2019).

Demetz, L. and Bachlechner, D. (2013), "To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool", in Böhme, R. (Ed.), *The Economics of Information Security and Privacy*, Springer, Berlin, pp. 25-47.

Dreissigacker, A., Skarczinski, B.von and Wollinger, G.R. (2020), "Cyber-attacks against companies in Germany: results of a representative company survey 2018/2019", KFN-Research Report, Vol. 158, Hanover.

European Banking Authority (EBA) (2017), "Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2)", available at: https://www.eba.europa.eu/documents/10180/2060117/Final+report+on+EBA+Guidelines+on+the+security+measures+for+operational+and+security+risks+under+PSD2+%28EBA-GL-2017-17%29.pdf (accessed 20 January 2021).

Edwards, B., Hofmeyr, S. and Forrest, S. (2016), "Hype and heavy tails: a closer look at data breaches", *Journal of Cybersecurity*, Vol. 2 No. 1, pp. 3-14.

Eling, M. and Wirfs, J. (2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research*, Vol. 272 No. 3, pp. 1109-1119.

European Union Agency for Cybersecurity (ENISA) (2017), "ENISA overview of cybersecurity and related terminology", available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology (accessed 21 December 2020).

Florencio, D. and Herley, C. (2012), "Sex, lies and cyber-crime surveys", available at: https://www.microsoft.com/en-us/research/wp-content/uploads/2011/06/SexLiesandCybercrimeSurveys.pdf (accessed 20 January 2021).

Gallagher, K.P., Zhang, X. and Gallagher, V.C. (2016), "Measuring the organizational impact of security breaches: patterns of factors and correlates", *CONFIRM 2016 Proceedings*, Vol. 36.

Gehem, M., Usanov, A., Frinking, E. and Rademaker, M. (2015), *Assessing Cyber Security: A Meta-Analyses of Threats, Trends and Responses to Cyber Attacks*, The Hague.

Gordon, L.A. and Loeb, M.P. (2006a), "Budgeting process for information security expenditures", *Communications of the ACM*, Vol. 49 No. 1, pp. 121-125.

Gordon, L.A. and Loeb, M.P. (2006b), "Economic aspects of information security: an emerging field of research", *Information Systems Frontiers*, Vol. 8 No. 5, pp. 335-337.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2018), "Empirical evidence on the determinants of cybersecurity investments in private sector firms", *Journal of Information Security*, Vol. 09 No. 02, pp. 133-153.

Hillebrand, A., Niederprüm, A., Schäfer, S., Thiele, S. and Henseler-Ungar, I. (2017), *Aktuelle Lage der IT-Sicherheit in KMU*, Bad Honnef.

Hiscox Ltd (2020), "Hiscox cyber readiness report 2020", available at: https://www.hiscoxgroup.com/sites/group/files/documents/2020-06/Hiscox-Cyber-Readiness-Report-2020.pdf (accessed 15 November 2020).

Hoo, K.J.S. (2000), "How much is enough? A risk-management approach to computer security", Consortium for Research on Information Security and Policy, Stanford.

Huaman, N., Skarczinski, B.von, Wermke, D., Stransky, C., Acar, Y., Dreißigacker, A. and Fahl, S. (2021), "A large-scale interview study on information security in and attacks against small and medium-sized enterprises", in *Proceedings of the 30th USENIX Security Symposium*.

Hughes, B.B., Bohl, D., Irfan, M., Margolese-Malin, E. and Solórzano, J.R. (2017), "ICT/Cyber benefits and costs: reconciling competing perspectives on the current and future balance", *Technological Forecasting and Social Change*, Vol. 115, pp. 117-130.

Iannacone, M.D. and Bridges, R.A. (2020), "Quantifiable & comparable evaluations of cyber defensive capabilities: a survey & novel, unified approach", *Computers and Security*, Vol. 96, p. 101907.

IBM (2020), "Cost of a data breach report 2020", available at: https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf (accessed 20 January 2021).

Kaspersky Lab (2019), "IT security economics in 2019. Global corporate IT security risks survey (ITSRS)", available at: https://go.kaspersky.com/rs/802-IJN-240/images/GL_Kaspersky_Report-IT-Security-Economics_report_2019.pdf (accessed 20 January 2021).

Kesswani, N. and Kumar, S. (2015), "Maintaining cyber security", in Burley, D., Guzman, I.R., Manson, D.P. and Potter, L.E. (Eds), *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research - SIGMIS-CPR '15, 04.06.2015 - 06.06.2015*, Newport Beach, California, USA, New York, New York, USA, ACM Press, pp. 161-164.

Ključnikov, A., Mura, L. and Sklenár, D. (2019), "Information security management in SMEs: factors of success", *Entrepreneurship and Sustainability Issues*, Vol. 6 No. 4, pp. 2081-2094.

Kwon, J. and Johnson, M.E. (2014), "Proactive versus reactive security investments in the healthcare sector", *MIS Quarterly*, Vol. 38 No. 2, pp. 451-471.

Lavrakas, P.J. (2008), *Encyclopedia of Survey Research Methods*, Sage Publications, Thousand Oaks.

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N. and Ahlemann, F. (2017), "Digitalization: opportunity and challenge for the business and information systems engineering community", *Business and Information Systems Engineering*, Vol. 59 No. 4, pp. 301-308.

Lloyd, G. (2020), "The business benefits of cyber security for SMEs", *Computer Fraud and Security*, Vol. 2020 No. 2, pp. 14-17.

Makridis, C. and Dean, B. (2018), "Measuring the economic effects of data breaches on firm outcomes: challenges and opportunities", *Journal of Economic and Social Measurement*, Vol. 43 Nos 1-2, pp. 59-83.

McGuire, M. and Dowling, S. (2013), *Cyber Crime: A Review of the Evidence: Summary of Key Findings and Implications*, Research Report, Vol. 75, UK Home Office.

McManus, L. and Eloff, J. (2006), "Using IT benchmarking principles to design an information security benchmark model", in *Proceedings of the ISSA*.

Neyman, J. and Pearson, E.S. (1928), "On the use and interpretation of certain test criteria for purposes of statistical inference: part I", *Biometrika*, Vol. 20A Nos ½, pp. 175-240.

National Institute of Standards and Technology (NIST) (2020), "Computer security resource center glossary", available at: https://csrc.nist.gov/glossary/term/Cyber_Attack (accessed 22 December 2020).

Paoli, L., Visschers, J. and Verstraete, C. (2018), "The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium", *Crime, Law and Social Change*, Vol. 70 No. 4, pp. 397-420.

Ponemon Institute and Hewlett Packard (HP) (2016), "2016 cost of cyber-crime study & the risk of business innovation", available at: https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf (accessed 20 January 2021).

Ranganathan, C. and Sethi, V. (2002), "Rationality in strategic information technology decisions: the impact of shared domain knowledge and IT unit structure", *Decision Sciences*, Vol. 33 No. 1, pp. 59-86.

Ransbotham, S. and Mitra, S. (2009), "Choice and chance: a conceptual model of paths to information security compromise", *Information Systems Research*, Vol. 20 No. 1, pp. 121-139.

Rantala, R. (2008), *Cybercrime against Businesses, 2005*, Special Report, Bureau of Justice Statistics, Washington DC, USA.

Richards, K. (2009), *Australian Business Assessment of Computer User Security: A National Survey*, AIC reports. Research and public policy series, Vol. 102, Australian Institute of Criminology, Canberra, A.C.T.

Romanosky, S. (2016), "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, Vol. 2 No. 2, pp. 121-135.

Ryan, J.J. and Jefferson, T.I. (2003), "The use, misuse, and abuse of statistics in information security research", *Proceedings of the 23rd ASEM National Conference*.

Sen, R. and Borle, S. (2015), "Estimating the contextual risk of data breach. An empirical approach", *Journal of Management Information Systems*, Vol. 32 No. 2, pp. 314-341.

Skarczinski, B.S.von, Boll, L. and Teuteberg, F. (2021), "Understanding the adoption of cyber insurance for residual risks - an empirical large-scale survey on organizational factors of the demand side", in *ECIS Proceedings*, No. 72.

Skarczinski, B.S.von, Dreissigacker, A. and Teuteberg, F. (2022), "More security, less harm? Exploring the link between security measures and direct costs of cyber incidents within firms using PLS-PM", in *Wirtschaftsinformatik 2022 Proceedings*, No. 2.

Statistisches Bundesamt (Destatis) (2017), "URS unternehmensregister", available at: https://www-genesis.destatis.de/genesis/online (accessed 12 March 2020).

Steeh and Charlotte (2008), "Telephone surveys", in Leeuw, E.D.de, Hox, J.J. and Dillman, D.A. (Eds), *International Handbook of Survey Methodology*, Psychology Press, New York, NY, pp. 221-238.

Stiller, A., Boll, L., Kretschmer, S., Wollinger, G.R. and Dreißigacker, A. (2020), "Cyber-attacks against companies in Germany: results of a qualitative interview study with experts (German)", KFN-Forschungsbericht, Hanover, available at: https://kfn.de/wp-content/uploads/Forschungsberichte/FB155.pdf (accessed 28 June 2020).

UK Department for Culture, Media and Sport (DCMS) (2017), "Cyber security breaches survey 2017. Main report", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf (accessed 17 December 2020).

UK Department for Culture, Media and Sport (DCMS) (2020), "Cyber security breaches survey 2020", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf (accessed 30 August 2021).

UK Home Office (HO) (2018), "Understanding the costs of cyber-crime. A report of key findings from the Costs of Cyber Crime Working Group", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf (accessed 20 January 2021).

US Department of Homeland Security (DHS) (2012), "The Menlo report: ethical principles guiding information and communication technology research", available at: https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/menlo_report_actual_formatted.pdf.

Vanson Bourne (2014), "Protecting the organization against the unknown. A new generation of threats", available at: https://cybersecuritylawwatch.files.wordpress.com/2014/03/protecting-the-organization-against-the-unknown-whitepaper-27396.pdf (accessed 20 January 2021).

Wang, Q.-H. and Kim, S.H. (2009), "Cyberattacks: does physical boundry matter?", in *ICIS Proceedings*, No. 48.

Weishäupl, E., Yasasin, E. and Schryen, G. (2018), "Information security investments: an exploratory multiple case study on decision-making, evaluation and learning", *Computers and Security*, Vol. 77, pp. 807-823.

Wolff, J. and Lehr, W. (2017), "Degrees of ignorance about the costs of data breaches: what policymakers can and can't do about the lack of good empirical data", available at: https://ssrn.com/abstract=2943867 (accessed 20 January 2021).

Appendix 1
Overview related literature

	Assignability				Relevance & Determinability			Representativeness						Transparency	
Author	Year Data	Region	Industry	Size	Measure Type	Cost Type	Attack Type	Method	Sample Type	Sample Size	Response Rate	Population	Statistics	Operational-ization	Limitations
Romanosky 2016	-	-	●	◐	$	◐	●	commercial db	selected public events	> 12,000 (921)	-	●	●	◐	●
Paoli 2018	2016	BEL	●	●	€; € Cl.	●	◐	web survey	convenience	310	4.9 %	●	●	●	●
Eling 2019	1995 - 2014	-	◐	◐	$	○	○	commercial db	selected public events	1,579	-	●	●	◐	●
Rantala 2008	2005	USA	●	●	$; $ Cl.	○	●	paper survey	random	8,079	23.0 %	○	○	◐	◐
Richards 2009	2008	AUS	●	●	AUD	○	○	paper, web or CATI	random	4,000	29.0 %	●	○	●	◐
UK DCMS 2020**	2019	UK	●	●	£	◐	○	phone survey	random	1,685	16.0 %	●	●	●	●
Vanson Bourne / Dell 2014	2013	INT	○	○	$ Cl.	○	○	web or CATI	-	1,440*	-	○	○	○	○
Ponemon / HP 2016**	2016	INT	●	○	$	○	●	paper survey	-	237	14.0 %	○	○	○	●
Accenture / Ponemon 2019**	-	INT	●	○	$	○	●	phone survey	-	355	-	○	○	○	●
Cisco 2019**	-	Asia-Pacific	○	○	$ Cl.	○	○	-	-	<2,000*	-	○	○	○	○
Kaspersky 2019**	-	INT	○	◐	$	●	●	-	-	4,958*	-	○	○	○	○
IBM / Ponemon 2020**	2019 - 2020	INT	●	●	$	●	◐	-	-	524	-	○	○	○	●
Hiscox 2020**	2019 - 2020	EU + USA	◐	●	$	○	◐	web survey	-	5,569*	-	○	○	○	○

Note(s): Year Data: year data was collected; Region: region data was collected; Industry: whether appropriate industry differentiation of costs is used; Size: whether appropriate company size differentiation (employee categories, revenue classes) of costs is used; Measure Type: in which business terms results are reported (Cl. = Classes); Cost Type: whether ISM relevant cost types are differentiated; Attack Type: whether, looking at costs, ISM relevant cyber attack types are differentiated; Method: of data collection, (db = data base); Sample Type: how the sample was drawn; Sample Size: count of observations (N); Response Rate: ratio of contacted and participating target subjects; Population: whether the underlaying basic and selection population was described; Statistics: whether statistical significance and error probabilities were assesssed; Operationalization: whether research approach, definitions and measurement scales were transparently described; Limitations: whether limitations of research were transparently addressed; ● = available/given; ◐ = partly available/given; ○ = not available/given; * count of interviewees instead of organizations interviewed; ** report published on a regular basis, only last included

Table A1.
Results of related literature research

Appendix 2
Additional figures and tables

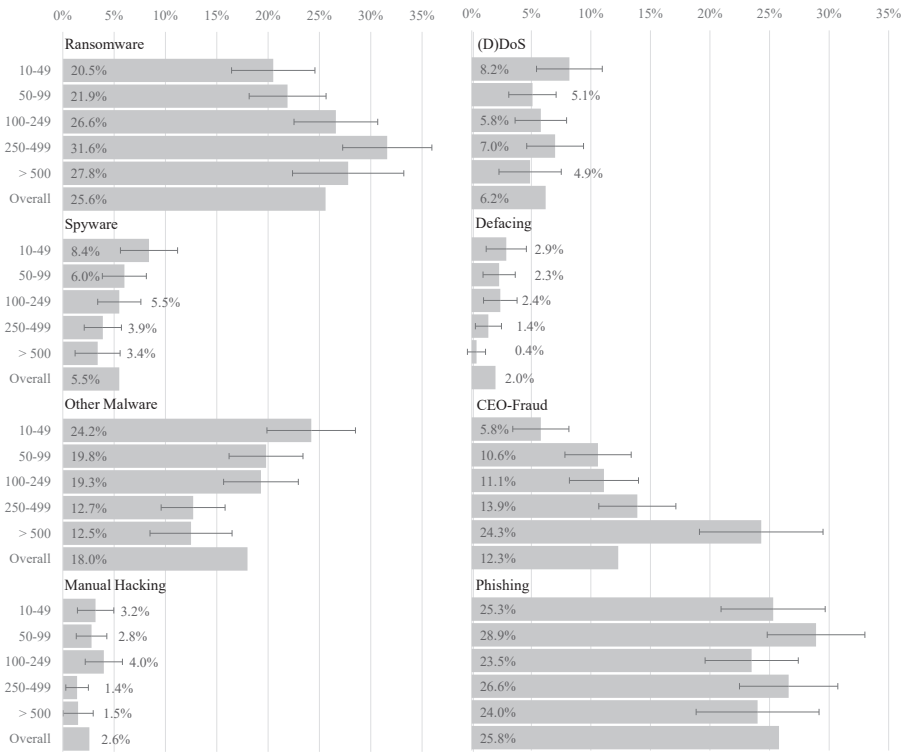

Figure A1. Proportions (%) of organizations reporting the most severe cyber incident within the last 12 months by attack type and employee class (n = 2,004; other (overall 0.2%) and combined attacks (overall 1.5%) not shown; confidence intervals α = 5%)

Table A2.
Proportions (%) of organizations reporting the most severe cyber incident within the last 12 months by sector (WZ-A,B,D,O,R as well as attack types "combined" and "other" excluded, due to $n < 30$) and attack type; italic: top 3 attack-types by sector; bold italic: highest value by attack type

	Ransomware	Spyware	Other malware	Manual hacking	(D)Dos	Defacing	CEO-fraud	Phishing	*n*
C-Manufacturing	*24.6*	5.1	15.2	1.8	5.4	2.0	*17.0*	*28.9*	553
G-Trade	*23.5*	5.2	*20.9*	3.4	6.3	1.5	10.8	*28.4*	268
M-Prof. Activities	*30.0*	6.1	*18.8*	2.0	5.1	2.0	14.7	*21.3*	197
Q-Health	*30.3*	4.9	*20.6*	1.2	4.9	2.4	7.3	*28.5*	165
F-Construction	*27.4*	6.6	*17.9*	3.8	1.9	1.9	12.3	*28.3*	106
P-Education	*29.8*	7.7	***25.0***	4.8	8.7	1.0	4.8	*18.3*	104
H-Transport	*21.9*	10.4	*16.7*	5.2	9.4	5.2	11.5	*19.8*	96
N-Support Services	*31.1*	4.4	*23.3*	4.4	6.7	1.1	10.0	*18.9*	90
J-Information	*22.9*	2.9	*22.9*	4.3	***15.7***	2.9	2.9	*25.7*	70
K-Finance	*20.6*	7.4	*17.7*	1.5	4.4	0.0	8.8	***39.7***	68
I-Accommodation	*19.5*	**14.6**	*19.5*	***7.3***	14.6	0.0	4.9	*19.5*	41
E-Water Supply	***31.4***	5.7	11.4	0.0	5.7	2.9	***20.0***	*22.9*	35
L-Real Estate	*18.2*	6.1	*21.2*	0.0	0.0	***9.1***	12.1	*33.3*	33
S-Other Services	*21.3*	2.7	*20.0*	2.7	9.3	1.3	17.3	*25.3*	75

		External advise and support	Compensations and fines	Drain off financial means	Replacement and recovery	Defense and investigation/ personnel costs	Business interruption/ revenue loss
10–49	avg	1.8 k	2.3 k	25.8 k	12.6 k	7.9 k	10.6 k
	med	775	500	3.5 k	1 k	620	2 k
	n	*92*	*5*	*6*	*111*	*124*	*66*
50–99	avg	2 k	952	47.6 k	11.6 k	15.4 k	10.4 k
	med	1 k	800	2 k	900	1 k	3 k
	n	*103*	*3*	*9*	*108*	*121*	*55*
100–249	avg	5.5 k	10.6 k	6.6 k	21.6 k	7.6 k	23.3 k
	med	1 k	6.5 k	3.5 k	1 k	1 k	5 k
	n	*79*	*6*	*6*	*78*	*103*	*49*
250–499	avg	4.5 k	50 k	16.5 k	2.9 k	13.8 k	56.4 k
	med	1 k	50 k	13 k	1 k	1 k	3 k
	n	*74*	*1*	*3*	*76*	*104*	*53*
>500	avg	4 k	27.7 k	41.9 k	8.8 k	26.3 k	14.5 k
	med	2 k	3 k	25 k	1 k	2 k	3.3 k
	n	*29*	*3*	*8*	*47*	*63*	*22*
Total	avg	3.3 k	11.7 k	31.5 k	11.8 k	13 k	23.4 k
	med	1 k	2.5 k	5 k	1 k	1 k	3 k
	n	*377*	*18*	*32*	*420*	*515*	*245*

Table A3.
Unsecured total costs (€) excl. zero costs by employee class and cost item

		Total	10–49	50–99	100–249	250–499	>500
A-Agriculture	avg	387	110	1.5 k	109		
	med	120	110	1.5 k	109		
	n	*5*	*2*	*1*	*2*		
B-Mining	avg	500		700			300
	med	500		700			300
	N	*2*		*1*			*1*
C-Manufacturing	avg	26.1 k	21.9 k	28.9 k	32.3 k	17.5 k	27.9 k
	med	1.2 k	750	1.7 k	1 k	1.9 k	4.5 k
	n	*222*	*30*	*52*	*62*	*54*	*24*
D-Energy	avg	6.8 k	875	7 k		5 k	21 k
	med	1.3 k	850	7 k		3 k	21 k
	n	*10*	*4*	*1*		*3*	*2*
E-Water Supply	avg	33.4 k	60.7 k	65.3 k	5.3 k	2 k	
	med	3.5 k	5.5 k	2.5 k	4 k	1.3 k	
	n	*14*	*3*	*4*	*3*	*4*	
F-Construction	avg	44.4 k	5.2 k	1.5 k	17.4 k	205.2 k	75.8 k
	med	1 k	800	1 k	2 k	1.3 k	75.8 k
	n	*57*	*23*	*11*	*11*	*10*	*2*
G-Trade	avg	19.8 k	30.9 k	19.5 k	3.6 k	15.7 k	6.7 k
	med	1.3 k	1.3 k	1 k	1 k	1.5 k	2.3 k
	n	*104*	*33*	*35*	*13*	*17*	*6*
H-Transport	avg	29.3 k	22.8 k	8.7 k	9.8 k	2.1 k	203.9 k
	med	1.9 k	500	2 k	3.5 k	1.8 k	7.5 k
	n	*46*	*15*	*13*	*6*	*8*	*4*
I-Accommodation	avg	13.3 k	4.4 k	7.8 k	38.2 k	4.4 k	
	med	3.6 k	2.9 k	1.3 k	10 k	4.4 k	
	n	*22*	*8*	*8*	*5*	*1*	
J-Information	avg	13.3 k	31.7 k	4.5 k	8 k	5 k	1 k
	med	1 k	1.6 k	2 k	675	2.5 k	1 k
	n	*31*	*9*	*9*	*8*	*4*	*1*

Table A4.
Secured total costs (€) by industry and employee class

		Total	10–49	50–99	100–249	250–499	>500
K-Finance	avg	3 k	1.9 k	1.8 k	8 k	1.5 k	1.8 k
	med	1.1 k	1.5 k	1.8 k	6.1 k	500	1 k
	n	*21*	*4*	*2*	*4*	*4*	*7*
L-Real Estate	avg	2.9 k	3.7 k	1 k		1.5 k	2.6 k
	med	1 k	1 k	1 k		1.5 k	2.6 k
	n	*11*	*7*	*2*		*1*	*1*
M-Professional Activities	avg	13.1 k	9.4 k	4.7 k	28.4 k	12.3 k	13.4 k
	med	3 k	2 k	2.1 k	2 k	7.5 k	3 k
	n	*86*	*20*	*17*	*15*	*17*	*17*
N-Support Services	avg	10.8 k	1 k	6.2 k	1.5 k	6.1 k	45.4 k
	med	900	500	800	1 k	500	3 k
	n	*35*	*9*	*7*	*6*	*7*	*6*
O-Public Administration	avg	125	125				
	med	125	125				
	n	*2*	*2*				
P-Education	avg	16.6 k	2.6 k	63.4 k	4 k	600	300
	med	1 k	1 k	900	1.4 k	600	300
	n	*35*	*17*	*8*	*7*	*2*	*1*
Q-Health	avg	15 k	6.8 k	13.4 k	3.7 k	24.9 k	11.1 k
	med	1 k	5 k	2 k	2 k	550	1 k
	n	*72*	*5*	*11*	*11*	*26*	*19*
R-Entertainment	avg	3.2 k	1 k	4.3 k	3 k	1 k	
	med	2.1 k	1 k	4.3 k	3 k	1 k	
	n	*7*	*1*	*4*	*1*	*1*	
S-Other Services	avg	5.9 k	4.3 k	2.5 k	2.3 k	9.8 k	60
	med	2 k	4.4 k	400	1.5 k	2 k	60
	n	*23*	*1*	*7*	*3*	*11*	*1*
Total	avg	20.3 k	15.3 k	18.2 k	19.9 k	25.6 k	26.6 k
	med	1.4 k	1 k	1.3 k	1.5 k	1.7 k	2 k
	n	*805*	*193*	*193*	*157*	*170*	*92*

Table A5. Secured total costs (€) by industry and employee class (continued)

		Total	IT and IT-Sec	Mgt. Board	Other
10–49	avg	15.3 k	18 k	14.8 k	9.1 k
	med	*1k*	*1.1k*	*1k*	*500*
	n	193	67	107	19
50–99	avg	18.2 k	22.5 k	12 k	6.6 k
	med	*1.3k*	*2k*	*1k*	*900*
	n	193	123	52	18
100–249	avg	19.9 k	24.1 k	11.7 k	3.8 k
	med	*1.5k*	*1.2k*	*2.5k*	*1k*
	n	157	112	32	13
250–499	avg	25.6 k	25.5 k	11.8 k	42.5 k
	med	*1.7k*	*1.7k*	*2.2k*	*1.4k*
	n	170	142	15	13
>500	avg	26.6 k	28.9 k	9.9 k	3.6 k
	med	*2k*	*2k*	*775*	*1.9k*
	n	92	82	6	4
Total	avg	20.3 k	24.1 k	13.3 k	13.5 k
	med	*1.4k*	*1.6k*	*1.2k*	*1k*
	n	805	526	212	67

Table A6. Secured total costs (€) by employee class and interviewee position

Appendix 3
Questionnaire

In the following, an extract of the CATI-questionnaire, with items specifically relevant to this article, can be found. Please note that the sequences of questions, using complex filter questions, are not illustrated. The complete questionnaire and further information is available in Dreissigacker *et al.* (2020).

A01: In which area are you active in your company?

(Management/Board of Directors; IT and Information Security; Data Protection; Plant. Safety; Revision/Audit; External Service Provider; Other [with free text]; I do not know; Not specified [multiple answers possible])

B05: Which cyber-attack of the last 12 months was the most severe?

(Ransomware attack; Spyware attack; Other attack with malware; Manual hacking; (D)DoS attack; Defacing attack; CEO fraud; Phishing; Other attack [multiple answers possible; only if B01 at least once number > 0]), response options: (Yes; No; Don't know; Not specified)

B08: Was there a ransom demand during this attack? How much was it?

(Yes [with numerical value in EUR]; No; Do not know; Not specified [only the most severe cyber-attack of the last 12 months])

B08a: Did your company comply with the ransom demand?

(Yes; No; Do not know; Not specified [only on the most severe cyber-attack of the last 12 months])

B12 Did the company incurs direct costs from the attack? If yes, what was the approximate amount?

(External consultation (e.g. legal advice, emergency management); Immediate measures for defense and clarification; Damages/penalties; Outflow of funds; Business interruption; Restoration/replacement [multiple answers possible; only for the most severe cyber-attack of the last 12 months], response options: (Yes [with numerical indication in EUR]; No; Not specified)

Corresponding author
Bennet Simon von Skarczinski can be contacted at: bennet.simon.von.skarczinski@pwc.com