More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM

Bennet Simon von Skarczinski
PricewaterhouseCoopers (PwC) Germany, Germany, bennet.simon.von.skarczinski@pwc.com

Arne Dreissigacker
Criminological Research Institute of Lower Saxony (KFN), Germany, arne.dreissigacker@kfn.de

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

More Security, less Harm? Exploring the Link between Security Measures and Direct Costs of Cyber Incidents within Firms using PLS-PM

Bennet Simon von Skarczinski[1], Arne Dreissigacker[2], and Frank Teuteberg[3]

[1] PricewaterhouseCoopers (PwC), Hanover, Germany
bennet.simon.von.skarczinski@pwc.com
[2] Criminological Research Institute of Lower Saxony (KFN), Hanover, Germany
arne.dreissigacker@kfn.de
[3] University of Osnabrueck, Osnabrueck, Germany
frank.teuteberg@uni-osnabrueck.de

Abstract. As one of the first articles to empirically explore the direct costs of cyber incidents, our research provides novel and significant insights into the structural links between cyber incidents, exposure, and security within firms, as well as the related technical consequences. We employ an explorative approach, which is based on the causal information/cyber risk models proposed by Cohen et al. and Woods & Böhme, as well as PLS-modeling to analyze data from 493 firms that have incurred direct costs from their most severe cyber incident in the last 12 months. These data are part of a larger dataset, based on a representative and stratified random sample of 5,000 organizations that participated in a survey in 2018/19. Based on our model, we discuss the results and derive implications that are highly relevant to the alignment of IT (security) strategy and management. Furthermore, we identify gaps to be assessed in future research.

Keywords: IT-security investment, cybercrime losses, impact of data breaches

1 Introduction

Reports of severe repercussions resulting from cyber attacks against firms, such as the shutdown of the US colonial pipeline in May 2021 [1] or a ransomware attack forcing 800 Swedish Coop grocery stores to close in July 2021 [2], are regularly discussed within the media. However, research has thus far produced little or conflicting evidence on how firm-based interventions, such as IT-security investments, can reduce cyber risks [3]. In fact, a recent literature review came to the conclusion that even after ten years of cyber analyses, we have learned little about cyber incidents and their financial costs, which could lead to 'perceptions that cyber risk is more art than science' [3].
Although there is a growing body of information security (IS) research, such research has mostly been limited to either conceptual papers, analytical modeling, or purely economic perspectives, while empirical analyses in this domain have predominantly focused on individuals, staff, and compliance behavior [4]. Empirical IS research

17th International Conference on Wirtschaftsinformatik,
February 2022, Nürnberg, Germany

focusing on security interventions and harm on an organizational level, however, is rare [3, 5, 6]. Regarding the negative consequences of cyber incidents, such as financial costs and the causal relationships behind them, the literature cites a particularly great need for research [3, 7–9]. Very few researchers have directly linked security attempts to harm outcomes, included potential confounding variables in their research designs, or controlled for firm characteristics [3]. Of the studies that have done this [7, 10–17], none have focused on the financial costs of cyber incidents for individual organizations. Studies that, on the other hand, have focused on the costs of cyber incidents within firms have produced evidence on the distribution, magnitude, and frequency of costs, but have neglected explanations for the mechanisms behind them [18–28]. Policy-makers, insurance companies, and firms ultimately have a great interest in models that can explain the cost of cyber incidents [17]. The importance of determining the costs of cyber incidents is based on the assumption that corporate information security management (ISM) is subject to the principle of economic efficiency, which demands a balance between the costs and benefits of IS [29–33]. Without knowing which drivers determine the costs of cyber incidents, it is difficult for organizations to operate an efficient ISM. Against this background, we pose our research question **(RQ):**

How can the direct costs of a cyber incident be explained with regard to existing firm characteristics and implemented security measures?

Challenges relating to research on cyber risk and harm repeatedly refer to a) the difficulty of accessing reliable data [9, 34–37], and b) the lack of a consistent theoretical foundation for the phenomenon [8, 35, 38].

In the context of a government-funded research project to improve IS within German firms, we conducted a large-scale interview study with 5,000 firms across all industries in 2018/2019. Due to our ability to access this data, which included questions on firm characteristics, victimization experiences, and negative outcomes of incidents, we are able overcome difficulty a). Our choice to employ an explorative approach, which is based on the cyber risk cause and effect models proposed by Cohen's et al. (1998) [39] and Woods & Böhme (2021) [3], is based on our use of secondary data, as well as the lack of guidance provided by distinct cyber theories. The aim of our paper is to use an explorative approach to uncover initial relationships between firm characteristics, security measures, and the costs of cyber incidents, which can then, by future research, be examined in more detail using suitable theories and specially collected data.

A suitable statistical technique for exploratory research relating to artifacts in design science is partial least squares path modelling (PLS-PM) [40–43]. PLS-PM is a method used to analyze “high-dimensional data in a low-structure environment” [40], which is already established in IS research and has developed into a "full-fledged" analysis method in recent years [40, 44, 45]. Furthermore, PLS-PM is an appropriate tool in cases where the structural model is complex and includes many constructs, the research includes financial ratios or similar types of data artifacts, and/or the research is based on secondary data that lacks comprehensive measurement theory [42].

To answer our research question, our paper is structured as follows. Section 2 describes the terminological and conceptual foundations used within our article. Our research model, including the data used and the operationalization of our measurement and

structural model, is presented in section 3. Section 4 reports our results and addresses the quality criteria and the model fit. A discussion of what the exploratory findings imply, and the requirements of future research can be found in section 5. Finally, we outline limitations in section 6 and conclude our article in section 7.

2 Conceptual foundations

In this section, we describe our terminological and conceptual foundations.

Information security (IS) Our basic assumption is that an internal or external threat initiates a cyber attack, which is either stopped by a security measure/control (in this case, remaining an IS/cyber event) or leads to an IS/cyber incident by exploiting a vulnerability, which thus causes consequences for an organization. We define cyber attacks, which lead to cyber incidents, as intentional attacks against firms that disrupt, disable, destroy, or maliciously control a computing environment/ infrastructure; destroy the integrity of the data, or steal controlled information [46]. The objectives of information security, confidentiality, integrity and availability, for systems, data, and processes are thus no longer guaranteed [47].

Search for related literature & theory To structure the analysis of our secondary data, we used existing literature reviews (i.e., Eling (2020) [35], Eling & Schnell (2016) [48], Anderson et al. (2019) [49], Dreissigacker et al. (2020) [50], and Woods & Böhme 2021 [3]) to scan for articles that empirically or theoretically explained 'direct costs', 'losses', or more generally 'harm of cyber incidents' and 'data breaches' in relation to organizations. In addition to a backward and forward search, we conducted a Google Scholar search using the above search terms to identify additional literature. Since the articles that our search identified did not include cyber theories that suited our research field, which confirms the theory gap that has already been identified by others [8, 35, 38], we screened all theories provided in the information systems research wiki [51]. However, we did not find any holistic approaches that explained cyber harm, costs, or risk on an organizational level. Instead, the recently introduced causal model by Woods & Böhme [3], which explains cyber risk outcomes, seems to be the best available approach to conceptually support our research question.

IS cause-effect model Cohen et al.'s (1998) cause-and-effect model of attacks on information systems asserts that "causes (also called threats) use mechanisms (also called attacks) to produce effects (also called consequences)", while "protective mechanisms (also called defenses) are used to mitigate harm by acting to limit the causes, mechanisms, or effects" [39]. Cohen et al. specify potential individual threats, attacks, consequences, and defenses, but fail to articulate possible latent variables and discuss these in relation to existing literature. More than 20 years later, Woods & Böhme introduced a causal model that also follows this logic, but additionally includes the concept of security exposure and discusses latent variables.[1] Within their high-level

[1] In their more detailed causal model, Woods & Böhme also differentiate between preventative and reactive security, as well as surface and asset exposure, embracing the construct compromise. Given that our secondary dataset is unable to differentiate between these constructs, we do not explain the concept in more detail.

causal model of cyber risks, they assume that 'threats' to the IS of organizations, expressed by different threat levels, is the only condition required for 'harm' to occur [3]. As a third construct, 'security' moderates the relationship between threat and harm, insofar that more security leads to less expected harm. The fourth construct 'exposure' indicates that more vectors can be used to intrude systems and more assets can be compromised, leading to exposure amplifying the effect that threat has on harm [3]. To analyze the harm resulting from cyber incidents, the authors describe several indicators to operationalize these four latent constructs and describe additional relevant variables, which should be included in regression models to minimize effects of confounding factors. In the next section, we derive these, as well as other indicators and variables from the literature to the extent that our secondary data permits.

3 Research approach and model

This section describes our research approach, including the data used, as well as the description and derivation of our measurement and structural model.

Survey data We use data based on a representative and stratified random sample of 5,000 firms, which was conducted within the context of a government-funded initiative to improve IS in German firms. The stratified sample included 1,190 firms with 10-49 employees, 1,181 firms with 50-99 employees, 1,120 firms with 100-249 employees, 1,005 firms with 250-499 employees, and 504 large firms with more than 500 employees. Our sample thereby indicates a focus on small and medium enterprises (SME). The dataset accounts for the 18 official German WZ08 industry classifications, which allows for international comparison.

From August 2018 to January 2019, computer-assisted telephone interviews (CATI) were carried out with mainly IT/IS managers (69.8%) and board members (23.5%) working for firms with more than nine employees. Participants were asked about risk perceptions, detected cyber-incidents within the last 12 months, existing organizational and technical IS measures, as well as demographic characteristics of the firms. Further descriptions of the sample, the survey procedure, data quality and pretesting measures, as well as the questionnaire used can be found in the official research report [50, 52].

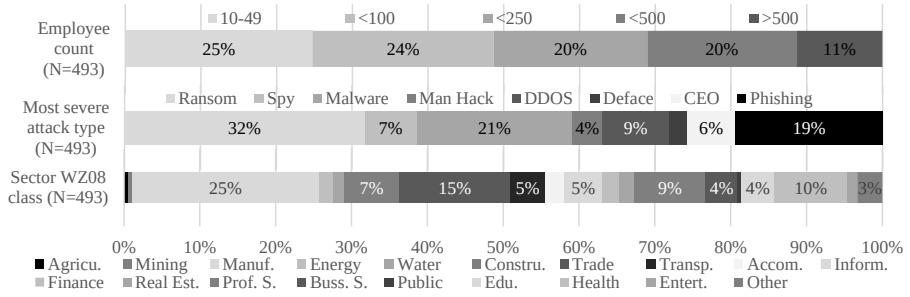

Figure 1. Characteristics of sub-sample

A detailed section of the questionnaire referred to the most severe incident experienced by firms within the last 12 months. Firms that reported a most severe incident were

particularly asked about system downtimes and direct costs. This fact, combined with the decision to not impute missing data, led to a strong reduction in the number of observations due to the listwise-deletion approach employed within the PLS regression. Of the 5,000 firms that were surveyed, 2,004 (40%) reported experiencing a most severe cyber incident in the last 12 months. Of those, 996 firms reported actual costs in EUR. The observations remaining in the main model, following the listwise deletion of missing values, were reduced to 493 (Figure 1).

PLS-PM As stated in our introduction, PLS-PM is an appropriate tool to explore complex empirical models. Such structural equation modeling can simultaneously estimate and test causal relationships between multiple independent and dependent variables [53]. PLS-PM models consist of two main components: i) the measurement model (also referred to as the outer model), which defines the relationships between a construct and its observed indicators (also referred to as manifest variables or single indicators), and ii) the structural model (also referred to as the inner model), which defines the relationships between the constructs [44]. Since our research design accounts for both emergent and latent variables, PLS-PM is well suited and can leverage its full capacities [40].

Constructs within the structural model Following Occam's Razor, the high-level causal model described is lean and reduced to the bare minimum but has relatively little explanatory power at this level. Therefore, it is important to operationalize the constructs at a lower level of abstraction, whilst also ensuring that the model remains streamlined. Since IS is a highly complex subject area, which does not only depend on technology but also strongly on organizational aspects and human behavior [4, 54], these aspects should be considered within the research design. Despite the challenge of operationalizing IS, self-reported indicators have successfully shown to explain IS outcomes [3, 10, 55]. However, in order to eliminate potential confounding variables, it is important to include relevant independent variables within the research design [3, 40], which of course entails a certain number of variables and their relationships.

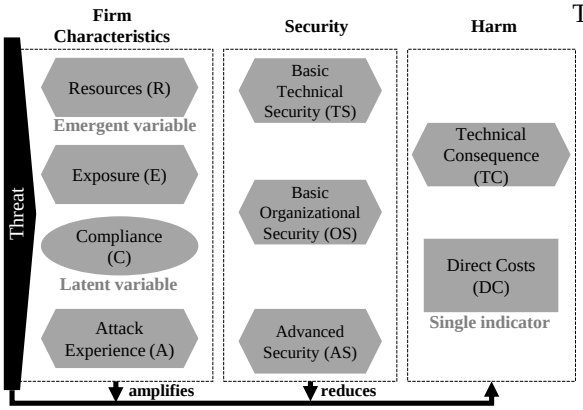

Figure 2. Structural model

The corresponding items and constructs from the secondary dataset were assigned in line with the threat-exposure-security-harm causal chain, outlined in section 2. This mapping was based on two rounds of feedback from relevant industry and academia experts, who accompanied our associated research project [50], and the integration of available literature. Figure 2 illustrates our structural model, whose

constructs we derive below. The corresponding indicators are summarized in the results section (Table 1).

Threats Since the dataset cannot provide sufficient exogenous threat level items, we rely on the threat level being implicit in the firm characteristics. **Resources (R)** The availability of technological, financial, and human resources constitutes an important aspect within the implementation of security solutions [4, 56]. Human resources are required for the adoption and maintenance of technical and organizational IS measures, while financial resources determine whether an organization can afford such IS measures [57]. Besides the 'IT-budget', we therefore consider the amount of 'IT staff' as a relevant indicator for the emergent 'resources' variable. Moreover, we regard the size of a firm, measured in 'employee classes', as a relevant determinant for their 'resources' (Table 1), since an organization's size has previously been shown to affect their IS and is commonly used as a control variable in similar research [7, 18, 34, 58]. Thus, we associate 'resources' with all security and harm constructs included within the model. **Exposure (E)** Controlling for other variables, firms baring more complexity (more locations in Germany and abroad, as well as export activity, see indicators E1-E3, Table 1) and thus more surface exposure in terms of higher interconnectedness of systems, processes, and infrastructure, are more vulnerable to cyber attacks [3]. Moreover, firms with more asset exposure (firms providing special products/services or having a special reputation or customer base, E4-E5) are also more prone to the attention of cyber attackers. Furthermore, we assume that rational acting firms with a higher exposure also demonstrate greater protection motivation and thus favor advanced security measures that go beyond basic technical and organizational IS measures [17]. **Compliance (C)** Human behavior is the primary source of IS risk [35]. We consider 'compliance' to be the only latent variable in our model given that it addresses behavior-oriented ratings of individuals, covering the indicators relating to risk awareness and compliance behavior of staff/management, as well as the firms' general IS efforts (Table 1). In this context, management awareness was found to be an significant factor within the adoption of IS measures [59, 60]. Greater compliance and managerial support both indicate that organizations more actively engage in raising IS and are therefore more likely to implement security measures [61]. **Attack Experience (A)** Prior IS research on organizational adoption factors of technology has investigated the experience of firms with IT systems [62]. Details of previous experiences of cyber attacks on IT systems could thus reveal a firm's current process and system deficits, and encourage managers to take additional IS measures to reduce the cyber risk [61], which also relates to organizational learning [37]. In this context, previous IS incidents could raise a firm's perception of protection [63] and thus cause firms to favor advanced IS measures. In the absence of scales to measure organizational IS [3], we use the self-reported existence of IS measures to operationalize the construct "security". **Basic Technical Security (TS)** is an emergent variable that includes the IT security measures used within our dataset, while **Basic Organizational Security (OS)** includes all security measures, which are mostly concerned with people, processes, and procedures [64]. We label them as basic since the majority of firms have already implemented such measures [27]. In contrast, we combine indicators that, particularly with regard to SMEs, have shown to go beyond fundamental IS measures [65] to **Advanced Security**

(AS). All security constructs in our model are related to harm. A **Technical Consequence (TC)** refers to the amount of eight possible system types (email & communication, order and customer management, accounting and controlling, web presence, banking & trading, warehousing and logistics, production control, other) that were affected by the most severe incident, as well as the total downtime of these system types (in hours). To better manage the very skewed data relating to downtime and direct costs, we used the natural logarithm of the downtime in hours and the estimated direct costs in EUR [40, 66]. The final dependent variable in our model is **Direct Costs (DC)**, which consists of the sum (EUR) of six underlying cost items that are either direct or opportunity costs (1. costs for external advice & support; 2. fines & compensation payments; 3. drain of financial means; 4. costs for replacement & recovery; 5. defense & investigation / personnel costs; 6. revenue loss / business interruption), estimated by the respondents. The cost types were primarily derived from the established Commercial Victimization Survey of the UK Home Office [67]. Since costs are "unsecured" insofar that this variable includes data from firms that reported at least one cost item, even when another item is reported to be 'unknown' or 'not specified', we cannot prevent an underestimation of costs. The data does not include general operating costs of IS, but incident costs only, and thus focuses on costs occurring as a consequence and costs occurring in response to cybercrime [67]. Costs that are not covered in our research include social, individual, and macroeconomic costs, as well as anticipation and indirect costs (i.e., reputation loss) of incidents.

4 Results

This section reports on our results and model fit, and is mainly based on the recent PLS guidelines proposed by Benitez et al. 2020 [40]. To calculate our model and to ensure an adequate model fit, we used Adanco 2.2.1. and its broad reporting functionality.

Statistical power refers to the probability of correctly rejecting the false null hypothesis and thus finding an effect in the sample that is indeed present in the population [68]. According to Cohen's regression power tables, our model requires at least 102 observations, when assuming statistical power of .8, a medium effect size (f2 = .150), and significance level of 5% [40, 69]. Our sample containing 493 observations thus seems more than appropriate. **Estimation** We used Mode B (regression weights) to estimate emergent constructs and Mode A to estimate latent constructs. Moreover, we set a dominant indicator to dictate the orientation of each construct (Table 1). For statistical inferences, we used bootstrapping with 999 runs. We checked whether the PLS-PM algorithm had properly converged (after 16 iterations) to prevent the occurrence of Heywood cases [70] or a technically invalid estimation [40].

Assessment of measurement model To assess the validity of our construct measurement, we report the overall model fit of the saturated model. All recommended discrepancy measures (SRMR (Value: .0452; HI95: .0453); least squares discrepancy d_{ULS} (Value: 1.078; HI95 1.085); geodesic discrepancy d_G (Value: .259; HI95 .306)) were below the 95% quantile of their reference distribution (HI95), which thereby provided empirical evidence for the emergent/latent variables included in our model.

Dijkstra-Henseler's rho (ρ_A: .881), which is used to assess the construct reliability for reflective measurement models, and in our case solely the latent variable "Compliance", is above the recommended threshold of .707 [71]. With reference to the latent variable, convergent validity can be assumed because the extracted measure of the average variance (AVE: .612) is greater than .5 [40, 72]. In terms of indicator reliability for latent variables, it is advisable to have significant (at 5% alpha level) factor loadings that are greater than .707, although slightly lower values are seldom problematic [40]. Except for indicator C2, in which the loading is very slightly below .707, we meet these requirements (Table 1). VIF values [40] for our indicators range from 1.000 to 1.673 and are thus far below the threshold of 5 [73, 74], which indicates that multicollinearity does not pose an issue within our model.

Table 1. Indicators of measurement model

#	Indicator	Span	Portion or mean (SD)	Loading	Weight
R1	Employee class (10-49; <100; <250; <500; >500)	1 - 5	2.8 (1.3)	.924***	.831***
R2	IT-Sec budget last 12 month (in EUR)	0 - 6m	96k (343k)	.591***	.393**
R3	Count IT-Sec staff	0 - 150	2.3 (8.3)	.265	.001
E1	Export activity (1=yes)	0 - 1	39.8%	.210°	.183
E2	Count of locations in Germany	1 - 200	5.5 (16,8)	.598***	.622***
E3	Count of locations abroad	0 - 280	1.4 (14.0)	.289	-.081
E4	Special products / processes / services (1=yes)	0 - 1	39.8%	.691***	.481**
E5	Special reputation / customer base (1=yes)	0 - 1	53.8%	.671***	.419*
A1	Count of experienced attacks last 12 months	1 - 3,041	106.3 (348.9)	.636°	.317
A2	Count of experienced attack types last 12 months	0 - 7	2.6 (1.4)	.956	.835
C1	Risk awareness & compliance of Mgt. (low; rather low; rather high; high)	1 - 4	3.3 (0.7)	.748***	.307***
C2	Risk awareness & compliance of staff (low; rather low; rather high; high)	1 - 4	3.0 (0.7)	.678***	.293***
C3	General IS effort	1 - 4	3.2 (0.7)	.904***	.633***
TS1	Password requirements (1=yes)	0 - 1	84.8%	.514***	.365**
TS2	Individual user rights (1=yes)	0 - 1	92.3%	.716***	.594***
TS3	Regular backups (1=yes)	0 - 1	98.4%	.455***	.216
TS4	Separate storage of backups (1=yes)	0 - 1	93.5%	.397***	.232*
TS5	Antivirus software (1=yes)	0 - 1	98.8%	.141	.033
TS6	Regular patching (1=yes)	0 - 1	94.3%	.552***	.333*
TS7	Firewall (1=yes)	0 - 1	98.6%	.122°	.070
OS1	Written IS policy (1=yes)	0 - 1	70.6%	.753***	.292*
OS2	Written emergency plan (1=yes)	0 - 1	60.9%	.845***	.493**
OS3	Regular compliance checks (1=yes)	0 - 1	56.4%	.691**	.130
OS4	IS training (1=yes)	0 - 1	49.9%	.686***	.399*
AS1	IT security certification (1=yes)	0 - 1	25.4%	.394***	.099
AS2	Regular risk assessments/pentests (1=yes)	0 - 1	51.7%	.707***	.428***
AS3	IS failure simulations (1=yes)	0 - 1	30.8%	.746***	.534***
AS4	Advanced firewall (1=yes)	0 - 1	71.0%	.629***	.414***
TC1	Logarhytmized downtime of systems in hours	0 - 9.4	3.0 (1.93)	.989***	.914***
TC2	Count of failed system types	0 - 7	2.1 (1.2)	.582***	.165*
DC	Logarhytmized direct costs of incident in EUR	2.9 - 14.5	7.8 (1.9)	-	-
IN	Control variable: IT interviewee (1=yes)	0 - 1	67.1%	-	-

*bold = dominant indicator; °p<.10, *p < .05, **p < .01, ***p < .001, one -tailed*

Not all loading and weight estimates relating to the latent variables are statistically significant (Table 1), yet we decided to keep these indicators in our model to maintain content validity [40] and prevent, in view of missing appropriate theoretical measurement concepts relating to our emergent variables, a design-to-fit approach.

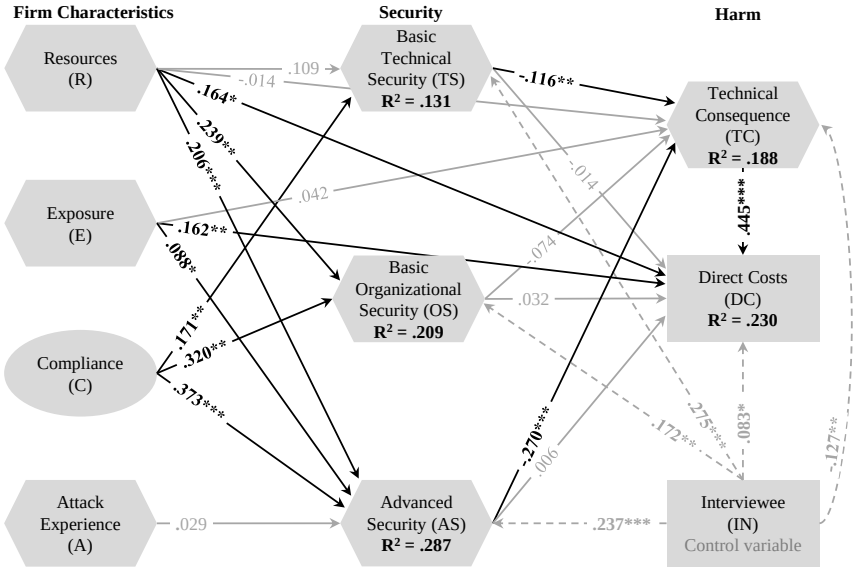

Figure 3. Structural model (N=493); °p<.10, *p < .05, **p < .01, ***p < .001, one-tailed

Assessment of the structural model Regarding the test of overall fit for the estimated model, which for PLS-PM was only introduced recently [40], the SRMR of .061 was above the HI95 but still below the recommended threshold of .080. The geodesic discrepancy ($d_{G:}$:.322) was above the HI95 (.303) but below the HI99 (.365). The path coefficients and corresponding significance levels are shown in Figure 3. The coefficients can be interpreted as "the change in the dependent construct, measured by standard deviations, if an independent construct is increased by one standard deviation while keeping all other explanatory constructs constant (ceteris paribus consideration)" [40]. For instance, whilst controlling for all other variables, increasing the basic technical measures by one standard deviation will increase the technical outcome by .116 standard deviations. Not all paths are significant and three paths, in contrast to the underlying cause-and-effect-model, even show unexpected, though not significant, signs (R→TC; OS→DC; AS→DC). Due to our exploratory research design, we, again, decided to leave the non-significant paths in the model [40]. Possible implications of the path coefficients will be discussed in the next section.[2] Cohen's f^2 effect sizes between the constructs range from 0 to .209, in which only Technical consequences → Direct costs (f^2=.209) and Compliance → AdvRes (f^2=.195) show medium effects,

[2] To control for industry and attack type, we analyzed the same model, using the two subsamples including solely manufacturing (N=122) and ransomware (N=162) incidents. While the goodness of fit measures have not deteriorated for the subsamples, both seem to explain more variance, compared to the main model.

whereas all others show either weak or no effects [69]. Benitez et al. explicitly note that it is unusual and unlikely that most constructs will have large effect sizes [40].
As the final measure used for goodness of fit in regression analysis, we report on the coefficient of determination (R^2)(Figure 3), which lies between 0 and 1, and indicates the proportion of the explained variance in a dependent variable and thus provides an insight into a model's predictive power [40, 75, 76]. The R^2 values of our dependent variables range from .131 to .287. Although this could be considered weak, according to more recent PLS-PM guidelines, the expected magnitude of R^2 depends on how well a phenomenon has been investigated. Since, in our case, the phenomenon has not been investigated particularly well [3], lower values are acceptable [40, 42].

5 Discussion

Based on our research question of how the direct costs of cyber incidents can be explained with regard to existing firm characteristics and security measures, we discuss our key findings and point out implications for academia and practice below.
Initially, the model coefficients show that greater size and resources of a firm are related to more security measures, although the effect for basic technical measures is not significant. This may be due to the fact that the indicators underlying the emergent variable technical consequences show an overall low variance (see Table 1), meaning that many firms have already adopted basis technical measures. Controlling for all other variables in the model, greater size and resources indicate higher direct costs (coeff. .164), a finding which has also been reported by previous research [26, 27].
This perceived contradiction between size, security, and cost may result from the costs of an incident increasing disproportionately with the size of a firm and the accompanying complexity of the IS ecosystem, even though larger firms take increased measures. Moreover, it is possible that either the security constructs need to be measured more accurately (i.e., more accurate maturity and dissemination) or that the security constructs can generally only explain a proportion of the variance, meaning that there may be other potential variables that influence the harm of incidents.
The **first main finding** of our research is that greater resources and greater exposure are independently associated with higher costs of the most severe cyber incident (coefficients .164 and .162, respectively) reported by firms. Surprisingly, no corresponding effects are found with respect to technical consequences, suggesting that firms with greater resources or greater exposure are not more affected by system failures than firms that are less exposed or have fewer resources; merely the subsequent costs of an incident are higher. This is explained, at least in part, by the fact that these firms rely more heavily on advanced measures that are significantly negatively related to technical consequences. For firms with greater resources or exposure, this means that advanced measures are at least able to help reduce the risk of technical consequences and associated costs. However, a greater risk of higher direct costs for these firms remains. Future research should therefore examine the effectiveness and complex interplay of security measures, as well as further differentiate the type of exposure and direct costs, to allow for more detailed conclusions.

The **second finding** shows that greater compliance (i.e., greater risk awareness, more compliant behavior by staff and management, and greater management role modeling) is crucial in relation to the more technical (coeff. .171), organizational (coeff. .320), and advanced security measures (coeff. .373). This points to the importance of binding rules and commitment to IS in the digitally connected world. Interestingly, experience of previous attacks has no independent effect on more advanced security measures. The questions of what higher compliance depends on and whether incidents experienced in the past also play a decisive role in raising IS remain open to future research.

The **third finding** relates to the influence of IS measures on the consequences of cyber incidents. All three latent security variables have a negative effect on technical consequences (technical measures -.116; advanced measures -.270), although the effect of the organizational measures (coeff. -.074) is not significant. Independent effects on the direct costs, on the other hand, are not observable. In practice, this means that particularly the technical and advanced measures can mitigate technical consequences for firms and, and thus, also direct costs. However, questions relating to which individual technical and organizational measures have specific preventative or mitigating effects on particular organizations' systems and processes, as well as the associated costs, remain open to future research.

Direct costs, and this is the **fourth key finding**, are significantly influenced by technical consequences (coeff. .445) within the model. As expected, the greater these are, the higher the direct costs of a cyber incident. A total of 23% of the variance in direct costs (R^2=.230) could be explained by the model. This also means that there are other variables, which are not included in the model, that influence direct costs. The comparison of different subsamples provided initial indications as to other relevant variables. The group comparison shows that there are sector-specific differences. Despite less observations relating to the subsample manufacturing (N=122), advanced security is unexpectedly affected by previously experienced attacks. In addition, the explained variance for direct costs clearly increases from R^2=.230 to R^2=.346. If we only consider ransomware attacks (subsample N=162), the model shows a stronger influence of basic technical security on technical consequences. Future research should distinguish between different types of attacks in this regard. It is conceivable, for example, that certain types of social engineering attacks cause costs, but no technical consequences, and simply could not have been prevented by certain IS measures, which is suggested by the direct positive effect of exposure to direct costs discussed above.

The **fifth and final finding** relates to the control variable "interviewee," which has a significant effect on all dependent variables within the explanatory model. For example, IT employees rated both the direct costs of an incident and the technical, organizational, and advanced security higher, but the technical consequences lower than non-IT employees. It is unclear whether IT employees tend to report more positively on their own area of responsibility (social desirability), whether they are worse at estimating financial costs, or whether they are simply better informed than non-IT employees because of their thematic proximity. In any case, this means that in future survey studies, the personal characteristics of the interviewees should at least be controlled for.

6 Limitations

Given that our study only refers to firms with 10 or more employees in Germany, the results cannot be generalized to firms in other countries. The sample was drawn on the basis of contact data from two commercial databases and not directly from the population. Although we found no evidence of systematic bias, firms not included in these databases were thereby also not included in our sample (coverage problem). As with other survey studies, the possibility of self-report bias should be noted. In addition, we retrospectively interviewed only one individual from each firm and the interviews were also limited in terms of complexity due to time constraints. The data was collected in 2018/2019. The events that have occurred in the meantime, such as the COVID-19 pandemic and the associated developments, have possibly led to a changed IS situation. However, since we do not focus on the analysis of specific amounts of costs nor on specific behavioral aspects of individuals, but instead on structural links of latent variables on an organizational level, we assume that even in a pandemic, the fundamental causal relationships of IS have not changed entirely. In addition, no other representative data of comparable scope and detail is available. Given the lack of a consistent theoretical basis for this research subject, we also note that our study is exploratory in nature. The lack of consistent theoretical guidance [35], as well as hardly any comparable empirical literature on this topic [3], can be cited as reasons why our model shows primarily low to medium R^2 and path coefficient measures [40, 42].

7 Conclusion

In this paper, we empirically analyzed how the direct costs of cyber incidents can be explained when considering firm characteristics and existing IS measures. We followed an explorative approach based on the causal IS risk models proposed by Cohen et al. [39] and Woods & Böhme [3], as well as partial least squares path modeling to analyze our survey dataset of 5,000 German firms and to identify structural links between attacks, exposure, security, and harm. Our analysis demonstrated that the direct costs resulting from cyber incidents depend on both the resources and exposure of the firms, as well as on the technical consequences related to the incident. The technical consequences, in turn, depend on and can be reduced by the existing basic technical and advanced security measures. We found that firms with greater compliance were more likely to protect themselves with basic technical and advanced measures compared to others and were thus able to minimize the technical consequences and associated costs of incidents.

Although our research has provided novel and significant insights into the direct costs of cyber incidents, we encourage validation of our findings based on other empirical data. As our research has shown that IS is a highly complex field of research, with numerous variables interacting at the technical, organizational, and human levels, further research is needed to develop and test comprehensive cyber theories explaining the costs of cyber incidents and to identify effective means of protection.

References

1. Stracqualursi, V., Sands, G. and Saenz, A.: Cyberattack forces major US fuel pipeline to shut down, https://edition.cnn.com/2021/05/08/politics/colonial-pipeline-cybersecurity-attack/index.html (Assessed: 28.08.2021)
2. Ahlander, J. and Menn, J.: Major ransomware attack against U.S. tech provider forces Swedish store closures, https://www.reuters.com/technology/cyber-attack-against-us-it-provider-forces-swedish-chain-close-800-stores-2021-07-03/ (Assessed: 28.08.2021)
3. Woods, D.W., Böhme, R.: Systematization of Knowledge: Quantifying Cyber Risk. 42nd IEEE Symposium on Security and Privacy (2021)
4. Herath, T.C., Herath, H.S.B., D'Arcy, J.: Organizational Adoption of Information Security Solutions. ACM SIGMIS Database for Advances in Information Systems 51, 12–35 (2020)
5. Hameed, M.A., Arachchilage, N.A.G.: A Model for the Adoption Process of Information System Security Innovations in Organisations: A Theoretical Perspective. Australasian Conference on Information Systems (2016)
6. Herley, C., van Oorschot, P.C.: SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit. In: 2017 IEEE Symposium on Security and Privacy (SP), pp. 99–120. IEEE (2017)
7. Sen, R., Borle, S.: Estimating the Contextual Risk of Data Breach. An Empirical Approach. J Manag Inf Syst 32, 314–341 (2015)
8. Cavusoglu, H., Cavusoglu, H., Son, J.-Y., Benbasat, I.: Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Inf Manag 52, 385–400 (2015)
9. Wolff, J. and Lehr, W.: Degrees of Ignorance About the Costs of Data Breaches: What Policymakers Can and Can't Do About the Lack of Good Empirical Data, https://ssrn.com/abstract=2943867
10. Straub, D.W.: Effective IS Security: An Empirical Study. Inf Sys Res 1, 255–276 (1990)
11. Tajalizadehkhoob, S., van Goethem, T., Korczyński, M., Noroozian, A., Böhme, R., Moore, T., Joosen, W., van Eeten, M.: Herding Vulnerable Cats. In: Thuraisingham, B., Evans, D., Malkin, T., Xu, D. (eds.) Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 553–567. ACM, New York, NY, USA (2017)
12. Edwards, B., Jacobs, J. and Forrest, S.: Risky Business: Assessing Security with External Measurements, http://arxiv.org/pdf/1904.11052v3
13. Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M., Liu, M.: Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents. In: Proceedings of the 24th USENIX Conference on Security Symposium, pp. 1009–1024. USENIX Association, USA (2015)
14. Biswas, B., Pal, S., Mukhopadhyay, A.: AVICS-Eco Framework: An Approach to Attack Prediction and Vulnerability Assessment in a Cyber Ecosystem. SSRN Journal (2016)

15. Hall, J.H., Sarkani, S., Mazzuchi, T.A.: Impacts of organizational capabilities in information security. Inf Comput Secur 19, 155–176 (2011)
16. McLeod, A., Dolezel, D.: Cyber-analytics: Modeling factors associated with healthcare data breaches. Decis Support Syst 108, 57–68 (2018)
17. Aldasoro, I., Gambacorta, L., Giudici, P., Leach, T.: The drivers of cyber risk. BIS Working Papers No 865 (2020)
18. Romanosky, S.: Examining the costs and causes of cyber incidents. J Cybersecur 2, 121-135 (2016)
19. Paoli, L., Visschers, J., Verstraete, C.: The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. Crime Law Soc Chang 70, 397–420 (2018)
20. Eling, M., Wirfs, J.: What are the actual costs of cyber risk events? Eur J Oper Res 272, 1109–1119 (2019)
21. Riek, M., Böhme, R., Ciere, M., Ganan, C., van Eeten, M.: Estimating the Costs of Consumer-facing Cybercrime. A Tailored Instrument and Representative Data for Six EU Countries. Workshop on the Economics of Information Security (WEIS) (2016)
22. Edwards, B., Hofmeyr, S., Forrest, S.: Hype and heavy tails: A closer look at data breaches. J Cybersecur 2, 3–14 (2016)
23. Wheatley, S., Maillart, T., Sornette, D.: The extreme risk of personal data breaches and the erosion of privacy. Eur Phys J B 89 (2016)
24. Strupczewski, G.: What Is the Worst Scenario? Modeling Extreme Cyber Losses. In: Linsley, P., Shrives, P., Wieczorek-Kosmala, M. (eds.) Multiple Perspectives in Risk and Risk Management, pp. 211–230. Springer International Publishing, Cham (2019)
25. Rantala, R.: Cybercrime against Businesses, 2005. Washington DC, USA (2008)
26. Richards, K.: Australian business assessment of computer user security. A national survey. Australian Institute of Criminology, Canberra, A.C.T. (2009)
27. UK Department for Culture, Media and Sport (DCMS): Cyber Security Breaches Survey 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf (Assessed: 30.08.2021)
28. Heitzenrater, C.D., Simpson, A.C.: Policy, statistics and questions: Reflections on UK cyber security disclosures. J Cybersecur 2, 43–56 (2016)
29. Gordon, L.A., Loeb, M.P.: Economic aspects of information security: An emerging field of research. Inf Syst Front 8, 335–337 (2006)
30. Gordon, L.A., Loeb, M.P.: Budgeting process for information security expenditures. Commun ACM 49, 121–125 (2006)
31. Brecht, M., Nowey, T.: A Closer Look at Information Security Costs. In: Böhme, R. (ed.) The Economics of Information Security and Privacy, pp. 3–24. Springer, Berlin (2013)
32. Iannacone, M.D., Bridges, R.A.: Quantifiable & comparable evaluations of cyber defensive capabilities: A survey & novel, unified approach. Comput Secur 96, 101907 (2020)

33. Connolly, L.Y., Borrion, H.: Your Money or Your Business: Decision-Making Processes in Ransomware Attacks. ICIS Proceedings (2020)
34. Buil-Gil, D., Lord, N., Barrett, E.: The Dynamics of Business, Cybersecurity and Cyber-victimization: Foregrounding the Internal Guardian in Prevention (Preprint). Preprint; accepted for publication in Victims & Offenders, published by Taylor & Francis. Vict Offender (2020)
35. Eling, M.: Cyber risk research in business and actuarial science. Eur. Actuar. J. 10, 303–333 (2020)
36. Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D.: A taxonomy of cyber-harms. Defining the impacts of cyber-attacks and understanding how they propagate. J Cybersecur 4, 1–15 (2018)
37. Kwon, J., Johnson, M.E.: Proactive Versus Reactive Security Investments in the Healthcare Sector. MIS Q 38, 451–471 (2014)
38. Hameed, M.A., Arachchilage, N.A.G.: A Conceptual Model for the Organizational Adoption of Information System Security Innovations. In: Security, Privacy, and Forensics Issues in Big Data, pp. 317–339. IGI Global (2020)
39. Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F., Isler, R.: A cause and effect model of attacks on information systems. Comput Secur 17, 211–221 (1998)
40. Benitez, J., Henseler, J., Castillo, A., Schuberth, F.: How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. Inf Manag 57 (2020)
41. Henseler, J.: Bridging Design and Behavioral Research With Variance-Based Structural Equation Modeling. Journal of Advertising 46, 178–192 (2017)
42. Hair, J.F., Risher, J.J., Sarstedt, M., Ringle, C.M.: When to use and how to report the results of PLS-SEM. EBR 31, 2–24 (2019)
43. Nitzl, C.: The use of partial least squares structural equation modelling (PLS-SEM) in management accounting research: Directions for future theory development. Journal of Accounting Literature 37, 19–35 (2016)
44. Henseler, J., Hubona, G., Ray, P.A.: Using PLS path modeling in new technology research: updated guidelines. Industr Mngmnt & Data Systems 116, 2–20 (2016)
45. Ringle, C.M., Sarstedt, M., Straub, D.: A Critical Look at the Use of PLS-SEM in MIS Quarterly. MIS Q 36 (2012)
46. National Institute of Standards and Technology (NIST): Computer Security Resource Center Glossary, https://csrc.nist.gov/glossary/term/Cyber_Attack
47. European Union Agency for Cybersecurity (ENISA): ENISA overview of cybersecurity and related terminology, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology
48. Eling, M., Schnell, W.: What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance 17, 474–491 (2016)
49. Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganan, C., Grasso, T., Levi, M., Moore, T., Vasek, M.: Measuring the Changing Cost of Cybercrime. The 18th Annual Workshop on the Economics of Information Security (2019)

50. Dreissigacker, A., Skarczinski, B. von, Wollinger, G.R.: Cyber-attacks against companies in Germany. Results of a representative company survey 2018/2019. Hanover (2020)
51. Larsen, K. R., Eargle, D. (Eds.): Theories Used in IS Research Wiki, http://IS.TheorizeIt.org
52. Dreißigacker, A., Skarczinski, B. von, Wollinger, G.R.: Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Hannover (2020)
53. Urbach, N., Ahlemann, F.: Structural Equation Modeling in Information Systems Research Using Partial Least Squares. Journal of Information Technology Theory and Application (JITTA)) 11 (2010)
54. Whitman, M., Mattord, H.: Management of Information Security. Cengage Learning, Boston, MA (2013)
55. Egelman, S., Harbach, M., Peer, E.: Behavior Ever Follows Intention? In: Kaye, J., Druin, A., Lampe, C., Morris, D., Hourcade, J.P. (eds.) Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 5257–5261. ACM, New York, NY, USA (2016)
56. Straub, D.W., Goodman, S.E., Baskerville, R.: Framing the information security process in modern society. In: Straub, D.W., Goodman, S.E., Baskerville, R. (eds.) Information security. Policy, processes, and practices, pp. 5–12. M. E. Sharpe, Armonk, NY (2008)
57. Rosner, M.M.: Economic Determinants of Organizational Innovation. Administrative Science Quarterly 12, 614–625 (1968)
58. Choudhury, A.S., Kwon, J.: A study of the effect of regulations on different types of information security breaches across different business sectors. PACIS 2016 Proceedings 73 (2016)
59. Hsu, C., Lee, J.-N., Straub, D.W.: Institutional Influences on Information Systems Security Innovations. Inf Sys Res 23, 918–939 (2012)
60. Kankanhalli, A., Teo, H.-H., Tan, B.C., Wei, K.-K.: An integrative study of information systems security effectiveness. Int J Inf Manag Sci 23, 139–154 (2003)
61. Skarczinski, B.S. von, Boll, L., Teuteberg, F.: Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side. ECIS Proceedings (2021)
62. D'Costa-Alphonso, M.-M., Lane, M.: The Adoption of Single Sign-On and Multifactor Authentication in Organisations. A Critical Evaluation Using TOE Framework. Issues in Informing Science & Information Technology 7 (2010)
63. Shackelford, S.J.: Should your firm invest in cyber risk insurance? Business Horizons 55, 349–356 (2012)
64. Rountree, D.: Organizational and Operational Security. In: Security for Microsoft Windows System Administrators, pp. 135–159. Elsevier (2011)
65. Bilodeau, H., Lari, M., Uhrbach, M.: Cyber security and cybercrime challenges of Canadian businesses, 2017. The Canadian Centre for Justice Statistics, Ottawa (2019)

66. Royston, P.: Multiple imputation of missing values: further update of ice, with an emphasis on interval censoring. STATA Journal 7, 445–464 (2007)
67. UK Home Office (HO): Understanding the costs of cyber crime. A report of key findings from the Costs of Cyber Crime Working Group, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674046/understanding-costs-of-cyber-crime-horr96.pdf
68. Cohen, J.: A power primer. Psychol Bull 112, 155–159 (1992)
69. Cohen, J.: Statistical Power Analysis for the Behavioral Sciences. Erlbaum, Hillsdale, USA (1988)
70. Henseler, J.: Partial Least Squares Path Modeling. In: Leeflang, P.S.H., Wieringa, J.E., Bijmolt, T.H., Pauwels, K.H. (eds.) Advanced Methods for Modeling Markets, pp. 361–381. Springer International Publishing, Cham (2017)
71. Nunnally, J., Bernstein I.: Psychometric Theory. McGraw-Hill, New York, USA (1994)
72. Fornell, C., Larcker, D.F.: Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research 18, 39–50 (1981)
73. Hair, J.F., Ringle, C.M., Sarstedt, M.: PLS-SEM: Indeed a Silver Bullet. Journal of Marketing Theory and Practice 19, 139–152 (2011)
74. Hair, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M.: A primer on partial least squares structural equation modeling (PLS-SEM). SAGE, Thousand Oaks, USA (2017)
75. Wooldridge, J.M.: Introductory Econometrics: A Modern Approach. Cengage Learning, Mason, USA (2013)
76. Becker, J.-M., Rai, A., Rigdon, E.: Predictive validity and formative measurement in structural equation modeling: embracing practical relevance. ICIS Proceedings, 1–19 (2013)