A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises

Nicolas Huaman[*C] Bennet von Skarczinski[†] Christian Stransky[*] Dominik Wermke[*]
Yasemin Acar[*#] Arne Dreißigacker[×] Sascha Fahl[*C]

[C]*CISPA Helmholtz Center for Information Security*
[*]*Leibniz University Hannover* [#]*Max Planck Institute for Security and Privacy*
[†]*PwC Germany* [×]*Criminological Research Institute of Lower Saxony*

Abstract

Cybercrime is on the rise. Attacks by hackers, organized crime and nation-state adversaries are an economic threat for companies world-wide. Small and medium-sized enterprises (SMEs) have increasingly become victims of cyberattacks in recent years. SMEs often lack the awareness and resources to deploy extensive information security measures. However, the health of SMEs is critical for society: For example, in Germany, 38.8% of all employees work in SMEs, which contributed 31.9% of the German annual gross domestic product in 2018. Many guidelines and recommendations encourage companies to invest more into their information security measures. However, there is a lack of understanding of the adoption of security measures in SMEs, their risk perception with regards to cybercrime and their experiences with cyberattacks. To address this gap in research, we performed 5,000 computer-assisted telephone-interviews (CATIs) with representatives of SMEs in Germany. We report on their experiences with cybercrime, management of information security and risk perception. We present and discuss empirical results of the adoption of both technical and organizational security measures and risk awareness in SMEs. We find that many technical security measures and basic awareness have been deployed in the majority of companies. We uncover differences in reporting cybercrime incidences for SMEs based on their industry sector, company size and security awareness. We conclude our work with a discussion of recommendations for future research, industry and policy makers.

1 Introduction

The consequences of cybercrime are felt world-wide. In 2018 a study by the Center for Strategic and International Studies (CSIS) and McAfee estimates that each year 0.8% of global GDP, close to $600 billion, is lost to cybercrime [25]. The global impact of cybercrime will only increase further as more and more potential targets gain online access in developing markets, and digital currencies simplify the extortion of money.

With many potential victims and easy automation, cyberattacks can be operated at scale. In 2019 alone, the FBI's Internet Crime Complaint Center received 467,361 complaints concerning cyberattacks, resulting in estimated losses of more than $3.5 billion [21]. Especially businesses are high-priority targets due to low risk to payoff ratio and their often large attack surfaces. The UK Department for Digital, Culture, Media & Sport reports in their "Cyber Security Breaches Survey 2019" that a third (32%) of the participating businesses experienced a cybersecurity breach or attack in the last 12 months [14].

While large enterprises often have considerable budgets and dedicated security teams available to protect themselves from attacks, SMEs often lack the expertise and assets to properly defend themselves from such attacks. The "Cyber Security Breaches Survey 2019" reports that SMEs were especially at risk, with up to 40% experiencing breaches [14]. According to the "Second Annual State of Ransomware Report: Survey Results for Australia", 32% of SMEs were hit by ransomware in 2017, and one fifth had to completely stop operations immediately [30]. A recent Public Service Announcement by the FBI further highlights the rise and danger of ransomware attacks [17].

SMEs[1] make up a large percentage of the economy in European countries and the U.S. In Germany, they are responsible for 31.9% of the gross domestic product, and they employ 38.8% of all employees in Germany. With such a large share of turnover but noticeably lower resources for information security, SMEs require special support to defend against cybercrime and the resulting casualties [39].

In this work, we investigate the perception, handling, problems, and experiences of SMEs in Germany with information security. Using the results, we uncover areas of high risk and provide recommendations for SMEs in Germany and internationally. To guide our research, we follow this set of research questions:

[1] In our study we exclude micro-enterprises - defined as <10 employees in Germany and <20 employees in the U.S.

RQ1: "*How do company employees perceive the risk of cyberattacks?*"

RQ2: "*Which and how frequent are information security measures deployed in SMEs?*"

RQ3: "*Which types and frequencies of attacks have our participating companies detected within the last 12 months?*"

RQ4: "*How are deployed security measures and company characteristics related to reported incidents and what are the emerging victimization factors?*"

Based on these research questions, we conducted computer-assisted telephone-interviews (CATI) with representatives of SMEs in Germany ($n = 5,000$). We were interested in their experiences and problems with cybercrime, as well as their perception of risks and handling of information security. We find that basic technical security measures and a certain security awareness have arrived in company mindsets, but not for all employees. Security measures such as information security training, regular risk analysis and emergency drills that involve all company staff still only happen within half of all SMEs in our dataset. We also identify aspects contributing to the likelihood of encountering certain cybercrime attacks, including company characteristics such as industry sector, internationality, and company size but also smaller factors such as the technical and organization security measures and their effects on certain attack types.

Our work is different from previous research in multiple ways:

- To the best of our knowledge, the scale of our interview study with 5,000 companies is unmatched by previous academic publications and on-par with the largest government surveys (e. g., 7,818 by the U.S. Department of Justice in 2008 [32]).
- Our interview study covers not only interactions with cybercrime and cyberattacks but also company characteristics, risk awareness and deployed security measures.
- Our data analysis includes empirical results for company characteristics as well as their relation to deployed security measures, risk perception of those companies, and experienced cyberattacks.

By using internationally assignable categories, we aim to make our results more comparable with studies and official statistics in other countries.

The remaining paper is organized as follows: We discuss related work (Section 2), describe our methodology (Section 3), and present our results (Section 4). Finally, we discuss our findings (Section 5) and conclude our work (Section 6).

2 Related Work

We discuss related work in two key areas: measurement of cybercrime in small and medium companies and the effects and costs of cybercrime.

Measurement of Cybercrime in Small and Medium Companies. Previous research focuses on surveys and statistics covered by official authorities, as well as surveys conducted by commercial organizations without the direct involvement of academic institutions. Even though there is a major need for well-founded research in literature covering cyberattacks against organizations [2,27,28,35], commercial author groups clearly dominate the publicly available literature [18] and, therefore, significantly influence our society's perception of the phenomenon [31].

Rantala conducted one of the first large-scale surveys investigating cyberattacks using social science approaches to enable the transfer of findings to the underlying population. Surveying 8,000 U.S. enterprises, she constituted the prevalence of cyberattacks in 2005 by several structural characteristics and security measures as well as damages and costs. She finds that companies are not affected equally by cyberattacks (e. g., some sectors are targeted more frequently, and companies that outsourced all or part of their computer security had a higher prevalence) [32]. Rantala's findings provide a good overview, but might be outdated compared to the dynamic field of cybersecurity, lack inferential analysis, and are not valid for most European organizations. More recently, Klahr et al. and Osbourne et al. conducted similar research to Rantala with a focus on UK businesses. Both surveys also found evidence for varying impacts of cyberattacks against businesses (e. g., large businesses are more likely to be struck more often, have a higher incident of breaches among those taking action to protect themselves [24], and certain sectors suffer more online crime incidents than others [29]) but also omit to exceed descriptive analytics.

Alluding to the lack of proper research, Romanosky's findings based on publicly available data suggest "*that public concerns regarding the increasing rates of breaches and legal actions may be excessive*", compared to the actual impact of events. However, putting the focus on financial impacts by industries, they find that actual damages are comparatively low, leaving out explanatory approaches how certain events lead to particular impacts and why these impacts might differ between individual enterprises (e. g., due to security measures) [34]. Kjaerland also uses secondary data collected by CERTs in the early 2000s, finding "*commercial and government sectors experience different types of attacks, with different types of impact, stemming from different sources*". Although their data set provides some attack-specific variables, they also face limitations of lacking structural characteristics of the targeted businesses, established security measures, as well as a representative sample [23]. The same limitations can be applied to Paoli et al. who attempt to assess the im-

pact of cybercrime by surveying 300 Belgian businesses in 2016, suffering a non-participation rate of 95%. Also, having a less-technical focus, they find evidence that most affected businesses do not report major harm or costs, and only a fifth of the affected businesses rate harm to operational activities as serious or higher [31].

In the U.S., the Internet Crime Complaint Center (I3C) releases a yearly "Internet Crime Report" [21]. This report covers international and national complaints directed to the I3C. The report provides a good overview of the types of breaches and incidents occurring in the U.S. and provides recommendations, but does not cover company demographics or root-cause analysis. In the UK, the Department for Digital, Culture Media and Sport (DCMS) releases a yearly "Cyber Security Breaches Survey" [14]. The report covers security incidents in companies, security measures they deploy, and risk factors within company demographics. It is a continuation of the survey from Klahr et al. [24]. While it focuses on providing descriptives, statistics, and trends, we attempt to relate risk factors and security measures to security incidents to provide in-depth insights into why companies with certain characteristics are attacked and at risk of what type of attack.

Effects and Costs of Cybercrime. Smith et al. conducted case studies with ten companies concerning the marketing activity and shareholder value after a cybercrime attack [36]. They demonstrate a decline in stock value, high recovery costs, and other consequences for these companies. Other event studies also found evidence for the negative impacts of cybersecurity breaches on stock prices [1, 12, 41]. Anderson et al. analyzed the cost of cybercrime in 2012 [4] and again in 2019 [3]. They report findings in terms of direct losses, the cost of defense and the indirect cost, and factors like lost revenue, but without an explicit focus on companies. In 2019, Demjaha et al. conducted a qualitative case study in semi-structured interviews with employees at a company that recently faced a data breach [13]. Stevens et al. introduced formalized threat modeling in a field study ($n = 25$), finding that the designed threat mitigation strategies provided tangible security benefits [40].

As indicated, research in the field of cyberattacks against businesses based on social science approaches is still underrepresented, compared to the expanse and relevance of this phenomenon. Tackling the critique of Anderson et al. stating available statistics on cybercrime are insufficient and fragmented and suffer under- and over-reporting [4], we believe our large-scale surveys is among the soundest and most comprehensive studies in continental Europe.

3 Methodology

In this section, we describe the interview methodology, details of our data analysis, and discuss limitations of our work. For our study, a professional computer-assisted telephone interview (CATI) service provider conducted 5,000 interviews with German company representatives from August 2018 to January 2019. We provide an overview of the overall methodology in Figure 1.

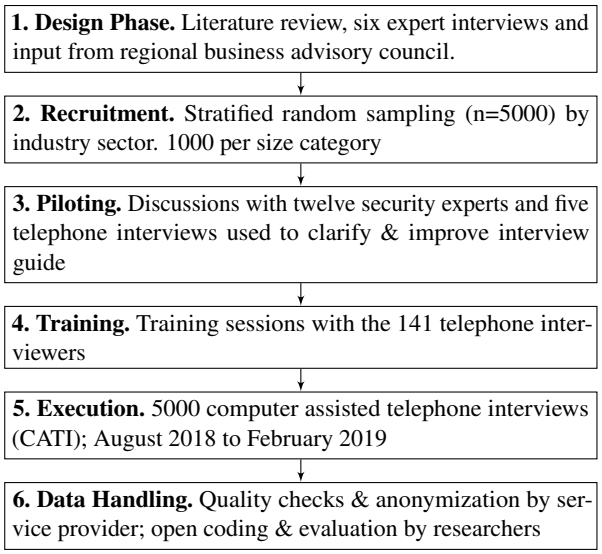

Figure 1: Illustration of our methodology, including research question identification, interview guide development, pretesting, data collection, and data analysis.

3.1 Interview Guide Development

Our research questions (cf. Section 1) served as the foundation for the CAT-interview guide. Additionally, we conducted interviews with both cybercrime experts and non-experts to establish further areas of interest and improve clarity for the final interview guide.

Interview Structure. We collected interview data in the form of computer-assisted telephone (CAT-) interviews with the help of a professional survey institute with experienced and trained interviewers. Telephone interviews allow queries from the interviewees. To allow for a representative sample of interview partners in German SMEs and a higher response rate, we utilized contacts provided by the survey institute for the interviews.

We developed the final interview questions based on a literature review [6, 7, 10, 20, 22, 24, 31, 32] with the help of six expert interviews and multiple feedback rounds with information security and privacy experts from industry and academia. We did not compensate the experts and the interviews lasted on average 88 minutes. We evaluated the interviews following Mayring's qualitative content analysis approach with two researchers [26].

The CAT-interview guide had the following structure:

1. **Introduction**. The interview started with a brief introduction of the interviewer and interviewee and the pur-

pose of the study. We asked questions about the interviewee's job role in the company and their estimation of sensitivity to information security and cybercrime risks in the company. We report findings of this part of the interview in Sections 4.1 and 4.2 and discuss them in Section 5.

2. **Cyberattacks**. This section includes questions about detected cyberattacks within the last 12 months and covers different types of attacks, e. g., phishing or CEO-fraud.

3. **Security Measures**. This section includes questions about the deployment of technical and organizational security measures in the interviewees' companies.

4. **Demographics**. This section includes demographic questions about the company, e. g., annual turnover, number of locations, and export activity.

Types of attacks. In the interview guide, we divided attacks into the eight categories: ransomware, spyware, attacks using other malware (e. g., viruses, worms, botnets, exploits), manual hacking (e. g., hardware manipulation, unauthorized configuration), (D)DoS attacks, defacing of web content, CEO fraud and phishing. We chose this less technical and relatively broad classification for two reasons. First, to be independent of specific attack vectors, techniques, and tools. We also did not want to include specific domains, systems, or data (e. g. XSS), which could change over time. Second, in order to promote comprehensibility and acceptance among the participants as well as to reduce the complexity of the resulting telephone interview. The types of attacks can be combined with each other. For example, information from a phishing or spyware attack can be used to prepare and execute a CEO fraud attack. The impact on systems and data does not represent a type of attack, but rather the consequence of an attack. For example, "identity theft" does not represent a type of attack, but the result of a successful attack, e. g., with the help of spyware.

Pre-Testing. We pre-tested the interview guide in two phases: First, we invited twelve security experts from industry and academic partners, including information technology and management representatives of multiple regional medium-sized companies, to discuss content- and comprehension-related aspects of the interview guide. We aimed to identify questions companies could not answer (e. g., general problems of comprehension or distinction of certain attacks and security measures), would not answer (e. g., due to discretion or missing approvals) or are not relevant or applicable for specific industries or business models. Second, we piloted the guide by performing telephone interviews with six employees responsible for the information security in small and medium companies. Three of these worked in companies providing IT-as-a-service to multiple small and medium enterprises and offered anonymous insights on their clients. With these pilots, we aimed to identify comprehension difficulties and further thoughts on possible responses to interview questions.

Based on the pre-testing, we revised the interview guide: Besides adding two more questions and some more answer options (e. g., "partially applicable"), we added explanations and rephrased the wording of a few existing questions.

During pre-testing, the telephone interview took 20 minutes on average, and all pilots felt comfortable answering the interview questions. Hence, we did not expect fatigue effects and did not randomize questions to make the interview process easier for the interviewers.

Interviewer Training. In preparation of the interviews, we performed interview training sessions with the 141 interviewers in two on-site call centers of the CATI service provider. The interviewer training illustrated the purpose of our study, discussed each question of the interview guide in detail, encouraged interviewers to point to questions that required further clarification, and provided a list of potential queries interviewees might ask during the interviews.

3.2 Recruitment

We based our research on a stratified random sample of 5,000 organizations. Stratified sampling is a method to sample from a population by partitioning the population into subpopulations. The population of companies in Germany is partitioned based on industry sectors and company sizes.

Industry Sectors. In order to ease international comparability and connectivity to other official studies, we use the official German Industry Classification WZ08 system [38]. WZ08 is based on the European NACE Revision 2 classification [16], which in turn is based on ISIC Rev 4 classification [43] of the United Nations. To obtain a representative sample, we aimed for a sample to be proportional to the distribution of industry sectors by the WZ08-Classification.

Company Size. We built the following subgroups for company size: 10–49, 50–99, 100–249, 250–499, and more than 500 employees. These clusters are based on the Commission Recommendation (2003/361/EC) [42]. This definition is standard across statistics related to European and German SMEs, which allows comparison between our results and those of similar studies. Since we focus on recommendations for tech departments of companies outside of the technology sector, we excluded micro-enterprises (< 9 employees). These micro-enterprises usually either have a strong technological focus or need to rely on external providers for their IT due to their small size. To compare company size categories, we instructed the CATI service provider to obtain 1,000 companies of each subgroup and companies in each company size subgroup for SMEs as well as 500 companies with 500 or more employees (cf. Table 1).

Large organizations and organizations providing services of general interest, in particular, are thus more strongly rep-

Table 1: Sample distribution and selection criteria for the different categories ($n = 5{,}000$).

Category	Selection Criteria	Sample Size		Percent	
		Target	After Filtering	Dataset	Real World
10–49 employees	Proportional to the selection population by company size and industry; Industry by WZ08-Classification A to S[†]	1,000	1,190	23.8%	79.1%
50–99 employees		1,000	1,181	23.6%	10.5%
100–249 employees		1,000	1,120	22.4%	6.5%
250–499 employees	Best Effort Base by company size and industry; industry by WZ08-Classification A to S[†]	1,000	1,005	20.1%	2.2%
500+ employees		500	504	10.1%	1.8%
Enterprises providing services of general interest [8]	Best Effort Base by industry; Selected industries (Subindustries of WZ08-D, E, H, J, K, L, O, P, Q)	500	*	*	*
Total			5,000	100%	100%

Overview of WZ08-classes (shortened, full names in [38]): **A: Agriculture & Fishing, B: Mining & Quarrying, C: Manufacturing, D: Energy & Gas, E: Water & Waste, F: Construction, G: Retail, H: Transportation, I: Accommodation & Food, J: Communication, K: Finances & Insurance, L: Real Estate, M: Prof. & Scientific, N: Administrative & Sup., O: Public Administration, P: Education, Q: Health & Social Work, R: Arts & Entertainment, S: Other Services, T: Households, U: Extraterritorial Organisations**

[*] Included in categories above. Not further analyzed due to being out of context for this publication.

[†] Excluding WZ08-O, T, U

resented in the sample than in the population and selection totality (oversampling).

The CATI service provider drew the sample from two commercial company databases [5, 19]. The databases, according to their self-declaration, combined contain all small, medium-sized, and large companies in Germany and include contact and meta information, including industry sector and company size.

We aimed to interview employees responsible for information security. In companies without dedicated information security staff, e. g., because information security was outsourced to external service providers or taken over by employees of other areas, we invited a representative of the board or other job roles (cf. Table 2 for further details).

3.3 Data Handling

Data Quality. We took the following measures to improve overall data quality. Since we relied on CAT-interviews, we designed the interview questions with a focus on comprehension. Interviewers were supported by a computer program that led them through the interview guide so they could focus on the interviewees' answers and enter data electronically. The computer program enforced validation rules, including the correct sequence of filter questions and checks for invalid answers. In addition, all interviewers were experienced and completed our interviewer training sessions. Concerning the questions about company headcount, annual turnover, and encountered security incidents, self-reporting on exact numbers proved to be difficult for participants. In the case of employees and annual turnover, we used the buckets available in the company database we used for sampling. In the case of employees, these buckets match the categories in Table 1. For incident numbers, however, the numbers strongly clustered and likely varied in quality. Therefore, we changed our analysis approach for the relevant regressions, only investigating whether a company did or did not need to actively react to a certain attack type within the last 12 months (Section 4.4).

The interview guide included only closed questions. Number questions like number of locations included a free-text option (See Appendix A) to enter these numbers, but only the interviewee position included actual free-text. For these positions, three authors developed a codebook, coded all answers independently and resolved all conflicts.

Data Analysis. As our regression analyses are intended to be exploratory, we consider a set of candidate models for each regression and select the final model based on the lowest Akaike Information Criterion (AIC) [11]. To analyze binary outcomes (e. g., deployment of a security measure), we rely on logistic regression, and to analyze numeric outcomes (e. g., information security sensitivity), we rely on linear regression. We consider candidate models consisting of every possible combination of the independent factors. Possible independent factors and corresponding baseline values are described in the appendix A. In general, sections included all factors of the previous section and the demographics as optional factors, but none of the later sections i. e. security measures (4.3) have demographics (4.1) and risk awareness (4.2) as factors but not incidents (4.4) or company sensitivity (4.2). This way we prevent having to describe the same correlations multiple times and we can keep a clear red line throughout our analysis. For some regressions, we added factors as non-optional, where it helped comparison or allowed for some more detail. The respective result sections explain which factors were added and why, and the results generally did not increase the AIC by more than 30 points. We present the outcome of our regressions in tables where each row contains a factor and the corresponding change of the analyzed outcome in relation to the baseline of the given factor. Our logistic regression models measure change from baseline factors with an odds ratio

(O.R.), in the case of our linear regression a coefficient (Coef.). For each factor of a model, we also list a 95% confidence interval (C.I.) and a p-value indicating statistical significance. For our analysis, we focus on factors with significant p-values, which we mark with a "*" and bold font. Due to the many regression analyses we performed, we moved most of them to Appendix B, keeping only representative regressions in the paper itself.

Ethical Considerations. To conduct the large scale telephone interview study in this paper, our institutions did not require a formal IRB process. Nonetheless, we modeled our interview guide after an IRB approved interview study, adhered to the strict German and U.S. data and privacy protection laws and the General Data Protection Regulation in the E.U., and structured our study following the ethical principals of the Menlo report for research involving information and communications technologies [15].

All participants were informed about the study purpose, the data we collected and stored, and contact details to contact the principal investigators or the CATI company in case of questions or concerns. Interviewees were briefed and debriefed on the phone before and after data collection. The CATI provider collected written consent prior to interviews.

Replication Package. To support the replicability of our work, we provide a replication package including the following material: (i) the recruitment email, (ii) the written consent form, (iii) the briefing for interviewers, (iv) the interview questions, and (v) a summary of the dropout and recall report[2]. We translated the original documents from German to English. We also provide the analyzed interview questions in the Appendix A.

Due to the sensitive nature of the collected data, our consent form states that only aggregated, anonymized data will be published. Therefore, we cannot make the raw data available.

We hope this replication package helps future studies to better compare and position themselves to our work.

3.4 Limitations

Like every research study, our work comes with several limitations, which we address below.

Our study is focused on SMEs in Germany. Hence, our results are likely not generalizable to SMEs in other countries. It may also be likely that micro-enterprises and very large enterprises show different results. However, small and medium-sized businesses make up 38.8% of all employees and 17.6% of enterprises, generating 31.9% of the gross domestic product [39]. We used two commercial company databases [5, 19]. They include company name, address, contact information, and the branch of the company. According to their self-declaration, the databases should include all registered companies in Germany [37]. If this is not the case, certain organizations from the population might not have had the chance to be included in the sample. Concerning our interview methodology, the sensitive questions we asked in our security survey might have introduced a desirability bias. Interviewees might have had concerns to answer questions truthfully [33] or participate at all. To combat this bias, we asked for facts about existing and past company policy and history instead of asking for desires and plans. Furthermore, our recruitment-email, briefing and consent form clarified that results will be handled anonymously and only reported in aggregated form, and that we are not rating company security, but investigating the prevalence of cybercrime across companies. We found that companies with fewer than 50 employees more often declined participation in the CAT-Interview. Similarly, companies in certain industries tend to deviate from average participation rates by at most 6%, which we deemed negligible for our results.

Furthermore like all surveys and interviews, we have to expect a self-reporting bias. Since we interviewed only one representative for each company, the data we collected is subjective and informed by individual knowledge, motivation, and attitudes. While we preferred tech staff responsible for information security (e.g., chief information officers, security engineers, or DevOps) as interviewees, not all companies had such staff available. Hence, the interviewees' job roles were diverse (cf. Table 2) and impacted the responses we collected. However, we took this into consideration in our regression analyses (cf. Section 3.3).

Finally, due to time and complexity restrictions of CAT-Interviews [33], our study can only provide limited insights into the maturity level and implementation details of security measures and attacks. For example, two participants confirmed the existence of password policies in their companies without being able to provide detailed information about the policies.

4 Study Results

Overall, the CATI service provider contacted 43,219 small and medium-sized companies in Germany to interview 5,000 companies (11.57% response rate)[3].

In this section we report and discuss results of all 5,000 CAT-interviews. We report and discuss company demographics, risk perceptions of employees, deployed security measures, and detected attacks.

4.1 Company Demographics

A total of 5,000 companies participated in the interview study (cf. Table 1). We interviewed employees in charge of their company's information technology (IT) or security (69.7%;

[2] cf. https://publications.teamusec.de/cybercrime

[3] 5,165 participants started the interviews; 165 (3.2%) dropped out during the interview.

Table 2: Demographics ($n = 5{,}000$).

	Question	Ratio	Companies
General			
Company Age > 10 Years	A.4.1	83.8%	4,192
Export Activity	A.4.3	39.9%	1,997
Enterprises of special interest (Table 1)	A.4.7	16.9%	847
Interviewee Position †			
Tech & Information Security	A.1.1	69.7%	3,484
Management	A.1.1	23.4%	1,171
Audit	A.1.1	2.1%	104
Data Protection	A.1.1	6.8%	342
Factory Safety	A.1.1	1.1%	56
Other	A.1.1	8.0%	402
Distribution †			
Multiple National Locations	A.4.4	41.5%	2,077
International Locations	A.4.4	14.0%	699
IT-Department †			
Inhouse	A.4.5	85.2%	4,262
Outsourced	A.4.6	82.3%	4,116
Information Security Staff †			
Inhouse	A.4.5	73.6%	3,682
Outsourced	A.4.6	37.4%	1,872
Headcount	*		See Table 1

† Multiple answers allowed
* Taken from the recruitment database

3,484), as well as employees in management board positions (23.4%; 1,171). Additionally, we interviewed representatives responsible for company audits (2.1%; 104), data protection (6.8%; 342) and factory safety (1.1%; 56) as well as representatives that did not fit in one of the above categories (8.0%; 402). With increasing company size, our interview was more likely to be with dedicated information technology staff. In smaller companies, we mostly interviewed executive management.

The average company age was 56 years (median = 39); the majority (83.8%; 4,192) is older than ten years (SQ: A.4.1). In our sample, older companies tended to employ more people. Approximately half (58.9%) of the interviewees reported that their company had only one business location in Germany (SQ: A.4.4). About 40% of the companies exported products or services. Companies with fewer employees were less likely to export (SQ: A.4.3). About 85.2% (4,262) of the participants stated that their company employed dedicated information technology (IT) staff (SQ: A.4.5), and 82.3% of companies had purchased IT services from external providers (SQ: A.4.6). Hence, 3,511 (70.2%) run both their own IT department and purchase external IT services. The majority (73.6%; 3,682) of companies has dedicated information security staff, while 37.4% (1,872) relied on external information security service providers. 24.4%(1,220) exclusively rely on external information security services. Table 2 provides an overview of all demographic information we collected. For most demographic questions we allowed multiple answers (cf. Appendix A)

Table 3: Linear regression for sensitivity score.

Factor	Coef.	C.I.	*p*-value
Industry Sector (Only levels with significance shown)			
J: Communication	**0.77**	**[0.35, 1.19]**	**<0.01***
K: Finances & Insurance	**1.23**	**[0.85, 1.61]**	**<0.01***
L: Real Estate	**0.53**	**[0.05, 1.01]**	**0.03***
M: Prof. & Scientific	**0.43**	**[0.11, 0.75]**	**<0.01***
N: Administrative & Sup.	**0.52**	**[0.15, 0.89]**	**<0.01***
Interviewee Position			
Management	-0.18	[-0.38, 0.02]	0.07
Tech	**-0.32**	**[-0.50, -0.13]**	**<0.01***
Employees (Per 100)	**-0.05**	**[-0.09, -0.00]**	**0.03***

4.2 Sensitivity and Risk Perceptions

We asked interviewees questions about information security sensitivity in their companies, and distinguished between management and regular employees. Additionally, we collected risk assessment for their company becoming a victim of a cyberattack with a distinction between targeted and mass attacks.

Information Security Sensitivity. To assess information security sensitivity, we asked interviewees three questions (SQ: A.3.2): We focused on the awareness of information security risks of (i) the management board and (ii) regular employees and their compliance with information security policies, and asked (iii) if the company actively advanced its information security, e. g., by investing in new information security technologies. Figure 2 summarizes the findings. The responses illustrate that most interviewees gave their company a positive assessment for information security sensitivity. Based on the three questions, we built an information security sensitivity score ranging from -6 to 6[4]. According to the regression model in Table 3, the sensitivity scores differed between industry sectors. The regression model indicates that interviewees working in communication, finances & insurance, real estate, professional, scientific, and technical activities and administrative and support service activities were significantly more likely than the baseline construction sector to report higher sensitivity scores. Interestingly, interviewees working in larger companies were significantly more likely to report lower sensitivity scores than interviewees working for smaller companies. Finally, the regression model indicates that interviewees working in a tech job were significantly more likely to report lower information security sensitivity scores.

> *Summary: Information Security Sensitivity.* Interviewees rated their organization's security sensitivity as generally high. While management made up a smaller portion of the interviewee sample, they reported higher sensitivity scores than regular employees. Finance and communication

[4]For this score, we mapped the three 4 point Likert items to $\{-2;-1;1;2\}$. Based on the sum of these scales, an integer between $[-6;6]$, we built a "sensitivity score" that we used for a regression analysis.

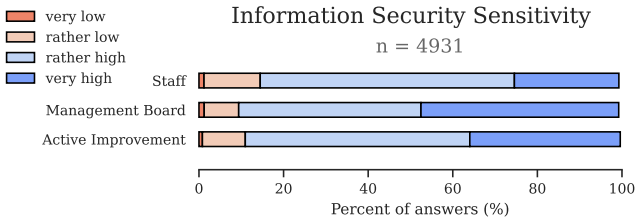

Figure 2: Sensitivity of company towards information security.

Table 4: Linear regressions for risk assessment.

Assessment for mass attacks	**Coef.**	**C.I.**	***p*-value**
Interviewee Position			
Management	**0.13**	**[0.00, 0.25]**	**0.05***
Tech	**0.23**	**[0.12, 0.35]**	**<0.01***
Export Activity	**0.12**	**[0.04, 0.20]**	**<0.01***
Multiple National Branches	0.07	[-0.01, 0.15]	0.09
International Branches	**0.15**	**[0.03, 0.26]**	**0.01***
Information Security Sensitivity Employees	**-0.10**	**[-0.14, -0.06]**	**<0.01***
Per 1 Mio Annual Turnover	0.00	[-0.00, 0.00]	0.27
Employees (Per 100)	0.03	[-0.00, 0.06]	0.07
Assessment for targeted attacks	**Coef.**	**C.I.**	***p*-value**
Interviewee Position			
Management	-0.02	[-0.13, 0.08]	0.66
Tech	0.07	[-0.04, 0.17]	0.23
Data Protection Officer	**-0.11**	**[-0.22, -0.01]**	**0.04***
Other	**-0.13**	**[-0.26, -0.00]**	**0.05***
Export Activity	**0.14**	**[0.09, 0.20]**	**<0.01***
Multiple National Branches	**0.06**	**[0.00, 0.12]**	**0.03***
International Branches	**0.11**	**[0.03, 0.20]**	**<0.01***
Information Security Sensitivity Management	**-0.04**	**[-0.07, -0.02]**	**<0.01***
Per 1 Mio Annual Turnover	0.00	[-0.00, 0.00]	0.11
Employees Tech (Per 100)	0.00	[-0.00, 0.00]	0.09
Employees (Per 100)	**0.03**	**[0.01, 0.05]**	**<0.01***

industries received higher scores in general, while staff in tech positions tended to report lower scores across all areas.

Perceived Risk. We asked the interviewees to assess the risk for their company to become a victim of any cyberattack within the next 12 months. We distinguished between targeted attacks, i. e., attacks that would only threaten their company specifically and mass attacks, i. e., attacks that would threaten other companies as well (SQ: A.1.2).

We included the company demographics and sensitivity from the previous section as optional factors in the regression analysis. Surprisingly, the industry sector was dropped out as a factor in both models, indicating that a company's industry sector was not correlated with risk awareness.

In general, interviewees reported significantly lower risks for a targeted attack (8.7%) than for a mass attack (34.9%).

Similar to the information security sensitivity score, the interviewee's job role correlated with their risk perception. Our regression analysis indicates that employees working in information technology or the management board positions perceived a higher risk for mass attacks and data protection

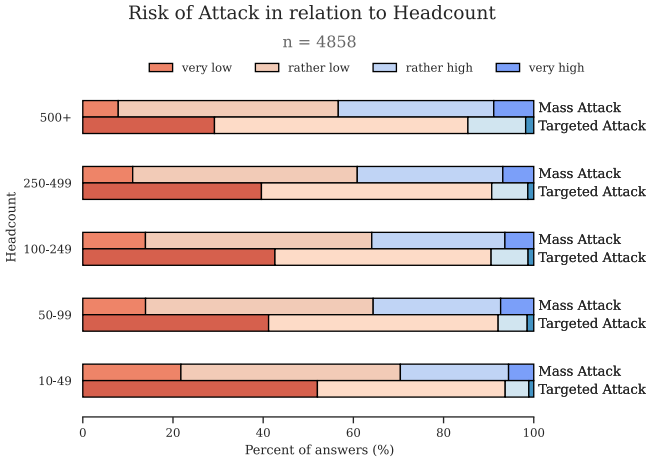

Figure 3: Risk assessment in relation to company size (headcount).

officers and others were significantly more likely to report a lower risk for targeted attacks. Companies that reported export activity and international locations also reported higher risk assessments for mass (Coef. 0.12 and 0.15) and targeted attacks (Coef. 0.14 and 0.11). Furthermore, risk perception varies with company size. Interviewees working for small companies (< 50 employees) reported a lower perceived risk than interviewees working for larger companies (≥ 500 employees) for targeted attacks (6.6% vs. 12.4%; 30.3% vs. 41.7%).

Interestingly, the impact of information security sensitivity differs between mass and targeted attacks based on the sensitivity type: in the regression model for mass attacks, risk assessment negatively tracks with an increase of perceived employee sensitivity (O.R. $= -0.10$), while in the model for targeted attacks, negative effects are seen with perceived manager sensitivity (O.R. $= -0.04$).

Summary: Perceived Risks. Most interviewees assess the risk for their company of being hit by a targeted attack as relatively low, compared to the risk of being hit by a mass attack. In general, interviewees working for small companies report a lower perceived risk of being attacked than interviewees working for larger companies.

4.3 Deployed Security Measures

We asked interviewees to report deployed security measures in their companies and distinguished between technical, e. g., firewall, and organizational measures, e. g., incident response plans (SQ: A.3.1). Figure 4 provides an overview of the reported security measures.

The majority of the interviewees reported that their companies deployed technical security measures. More than 90% reported that they use firewalls, regularly patch and update

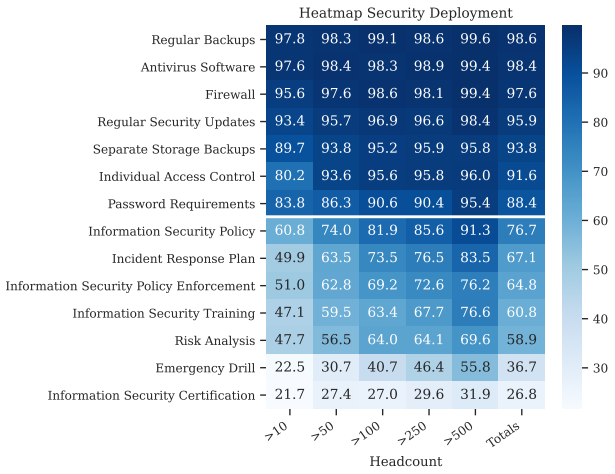

Figure 4: Technical (top half) and organizational (bottom half) security measures reported by our interviewees.

their systems, use up-to-date anti-virus software, deploy effective access control mechanisms, and secure backup strategies. While we cannot provide an in-depth analysis of respective technologies and deployment quality or maturity, our results indicate that many common technical security measures find widespread adoption in companies.

In contrast, the adoption of organizational measures is lower in general and more diverse. While most interviewees reported written security and privacy policies (78.7%) in their companies and that they get regularly reviewed and revised if necessary (79.4%), only 29.9% report security certifications or exercises or simulated the failures of computer systems in their companies (37.4%). Again, we cannot provide more in-depth details of the quality or maturity of policies or the type of security certification.

Figure 4 illustrates the deployment likelihood of both technical and organizational security measures varies with company size.

Technical Security Measures. While technical security measures seem to find widespread adoption in general, we report individual measures in more detail below. We ran a logistic regression for every technical security measure, including demographics and risk awareness as optional factors.

We consider the following technical measures: regular backups, up-to-date antivirus software, use of firewalls, regular security updates, use of individual access control, and password requirements. Our regression models indicate that for all technical measures other than access control, technical staff was significantly more likely to report the deployment of the security measure than other employees. A potential explanation is that technical staff is well-informed about deployed measures.

Table 5 shows the regression analysis outcome for individual access control and regular security updates. Tables 13–16

Table 5: Logistic regressions for technical measures.

Individual Access Control	**O.R.**	**C.I.**	***p*-value**
Company Age	1.32	[0.78, 2.25]	0.30
Export Activity	1.34	[0.99, 1.82]	0.06
International Branches	1.63	[0.92, 2.87]	0.09
IT-Sec External	**1.99**	**[1.54, 2.57]**	**<0.01***
Industry Sector (only levels with significance displayed)			
C: Manufacturing	**1.57**	**[1.00, 2.47]**	**0.05***
E: Water & Waste	**2.98**	**[1.01, 8.78]**	**0.05***
J: Communication	**5.93**	**[1.76, 19.91]**	**<0.01***
L: Real Estate	**6.56**	**[1.94, 22.15]**	**<0.01***
M: Prof. & Scientific	**5.86**	**[2.55, 13.48]**	**<0.01***
P: Education	**3.47**	**[1.71, 7.02]**	**<0.01***
Q: Health & Social Work	**3.29**	**[1.74, 6.22]**	**<0.01***
R: Arts & Entertainment	**3.96**	**[1.15, 13.63]**	**0.03***
S: Other Services	**2.96**	**[1.26, 6.97]**	**0.01***
Interviewee Position			
Management	**0.39**	**[0.25, 0.62]**	**<0.01***
Tech	**1.60**	**[1.04, 2.48]**	**0.03***
Other	**0.49**	**[0.29, 0.82]**	**<0.01***
Risk Assessment Mass	**1.16**	**[1.05, 1.29]**	**<0.01***
Employees Tech (Per 100)	**6.76**	**[1.28, 35.83]**	**0.02***
Employees (Per 100)	**1.25**	**[1.09, 1.43]**	**<0.01***
Regular Security Updates	**O.R.**	**C.I.**	***p*-value**
Export Activity	1.38	[0.94, 2.03]	0.10
Multiple National Branches	1.21	[0.86, 1.71]	0.27
IT-Sec External	**1.53**	**[1.10, 2.11]**	**0.01***
Industry Sector (only levels with significance displayed)			
H: Transportation	**0.51**	**[0.26, 0.97]**	**0.04***
Interviewee Position			
Tech	**2.60**	**[1.84, 3.67]**	**<0.01***
Employees (Per 100)	1.11	[0.96, 1.28]	0.17

in the Appendix summarize the remaining regression models. The reporting of deployed technical measures varied by interviewee job role. Technical staff was more likely to report the deployment of individual access control (O.R. = 1.6), regular backups in a separate location (O.R. = 2.74), antivirus software (O.R. = 3.33) and regular security updates (O.R. = 2.60). Interviewees in management roles were significantly less likely to report the deployment of password requirements (O.R. = 0.64), individual access control (O.R. = 0.39) and firewalls (O.R. = 0.37).

We find that the likelihood of deploying technical security measures varies by industry sector: Compared to the construction baseline, companies in the manufacturing (O.R. = 0.67), transportation (O.R. = 0.59), and finance and insurance (O.R. = 3.80) sectors were more likely to deploy password requirement policies. We found similar effects for the deployment of access control mechanisms. Considering the odds ratio, companies in the communication (O.R. = 5.93), real estate (O.R. = 6.56), and professional, scientific, and technical activities (O.R. = 5.86) sectors were most likely to deploy access control. Companies in the transportation (O.R. = 0.51) sector were also more likely to perform regular security updates compared to the construction baseline. The deployment of firewalls, antivirus software and the adoption of backup strategies did not vary significantly by industry sector.

The deployment of password requirement policies (O.R. = 1.23) and access control (O.R. = 1.25) varies by company headcount. Larger companies were more likely to deploy

both security measures. In contrast, the use of antivirus software, regular security updates, or firewalls do not track with company headcount.

The use of antivirus software (O.R. = 4.18), firewalls (O.R. = 3.77), and a company's backup strategy (O.R. = 2.47) varied with company age. Similarly, company age positively correlated with the deployment of the previous measures - more mature companies were more likely to deploy them. However, we could not find a correlation between company age and other technical security measures.

We identified a correlation of the use of external information security expertise with the deployment of access control (O.R. = 1.99), antivirus software (O.R. = 2.87), regular security updates (O.R. = 1.53) and firewalls (O.R. = 2.18).

> *Summary: Technical Security Measures.* We find that basic technical security measures are widely deployed, even in small companies. However, we also find that aspects such as industry sector, company headcount, company age and the use of external information security expertise correlated with a diverging deployment of technical security measures.

Organizational Security Measures. We report results for the following deployed organizational security measures: incident response plans, risk and vulnerability analyses, emergency management and drills, information security certification, information security training for employees, written information security policies and regular compliance checks. Table 6 illustrates the regression analysis for security certifications. We list the remaining regression analyses for organizational measures in tables 8–12 in the Appendix.

Similar to technical security measures, the regression analyses suggest that the interviewees' job role correlated with the reporting of organizational security measures. Interviewees working in tech were more likely to report all organizational security measures, while interviewees working in management more often reported the implementation of information security policies, incident response plans (O.R. = 0.68), and emergency drills (O.R. = 0.60). However, data protection officers were more likely to report on information security policies (O.R. = 1.69) and their enforcement (O.R. = 1.56).

Figure 4 suggests that organizational measures are less common than technical measures, especially in smaller companies (cf. Table 6,8–12). Similarly, larger companies are more likely to deploy written information security policies and incident response plans (O.R. = 1.36), regular enforcement of information security policies (O.R. = 1.08), information security training for their staff (O.R. = 1.14), and practicing emergency drills (O.R. = 1.17). Interestingly, the reported prevalence of risk analyses and information security certifications did not vary by company size. An explanation could be that information security certifications are required by law for companies in certain industry sectors like finances and health, which typically have fewer staff.

The use of external information security providers correlated with the deployment of two organizational information security measures. Companies that relied on external information security providers were more likely to deploy information security policies or incident response plans (O.R. = 1.31), and regular emergency drills (O.R. = 0.80).

Companies with international locations were more likely to deploy written security policies or incident response (O.R. = 1.38), security certification (O.R. = 1.27), security policy enforcement (O.R. = 1.29) and security training (O.R. = 1.49). Similarly, companies with more than one national branch, were more likely to deploy regular risk analyses (O.R. = 1.19), written security policies or incident response plans (O.R. = 1.58) and enforcement of these policies (O.R. = 1.34).

We included the risk perception (cf. Section 4.2) as an optional factor in the regression analysis. We find that risk perception in the context of targeted attacks correlated with the reporting of a written information security policy or incident response plan (O.R. = 1.17), for information security certification (O.R. = 1.16), risk analysis (O.R. = 1.12), information security training (O.R. = 1.11) and the execution of emergency simulations or drills (O.R. = 1.18). On the other hand, risk perception in the context of mass attacks correlated with a lower likelihood for that company to have information security certification or perform risk analysis.

We also found that the number of tech staff in companies correlated with the reporting of policy enforcement and compliance (O.R. = 1.37) as well as emergency drills (O.R. = 1.20).

Similar to technical security measures, the industry sector correlated with the reporting of organizational measures. A potential explanation can be law requirements for as well as requirements and technological affinity of different sectors. For example, companies in the finances & insurance sector have strong security requirements [8]. This sector holds the highest odds ratio in five of six organizational measures, including for information security policies and incident response plans (O.R. = 6.43), for the enforcement of these plans (O.R. = 7.20), in regular risk analyses (O.R. = 7.27), in security training (O.R. = 13.85), and for the deployment of emergency drills (O.R. = 16.09).

> *Summary: Organisational Security Measures.* Organizational measures have lower adoption rates in SMEs. However, we find that company size correlates with all organizational security measures we included in our analysis. Companies in the finance and energy sector are most likely to employ organizational security measures.

4.4 Reported Incidents

We asked participants to report the security incidents their company detected and reacted to in the last 12 months. We explicitly asked participants not to report incidents that could

Table 6: Logistic regression for information security certification.

Factor	O.R.	C.I.	*p*-value
Company Age	1.05	[0.71, 1.54]	0.81
Multiple National Branches	**1.20**	**[1.02, 1.40]**	**0.03***
International Branches	**1.27**	**[1.02, 1.58]**	**0.04***
IT-Sec External	**1.48**	**[1.26, 1.73]**	**<0.01***
Industry Sector (only levels with significance displayed)			
D: Energy & Gas	**7.82**	**[3.88, 15.76]**	**<0.01***
G: Retail	**1.80**	**[1.20, 2.71]**	**<0.01***
I: Accommodation & Food	**2.67**	**[1.55, 4.61]**	**<0.01***
J: Communication	**3.35**	**[2.01, 5.58]**	**<0.01***
K: Finances & Insurance	**4.94**	**[2.96, 8.24]**	**<0.01***
L: Real Estate	**2.11**	**[1.09, 4.08]**	**0.03***
M: Prof. & Scientific	**2.22**	**[1.45, 3.39]**	**<0.01***
N: Administrative & Sup.	**2.34**	**[1.46, 3.75]**	**<0.01***
Q: Health & Social Work	**2.14**	**[1.38, 3.32]**	**<0.01***
R: Arts & Entertainment	**3.30**	**[1.65, 6.62]**	**<0.01***
Interviewee Position			
Management	**0.70**	**[0.58, 0.85]**	**<0.01***
Factory Safety	**2.58**	**[1.36, 4.91]**	**<0.01***
Risk Assessment Mass Attack	**0.86**	**[0.81, 0.93]**	**<0.01***
Risk Assessment Targeted Attack	**1.16**	**[1.06, 1.28]**	**<0.01***
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.10
Employees Tech (Per 100)	1.07	[0.95, 1.21]	0.24

Table 7: Logistic regressions for reported security incidents.

Ransomware	O.R.	C.I.	*p*-value
Interviewee Position			
Audit	1.73	[0.95, 3.16]	0.07
Regular Backups and Separate Backup Location	1.36	[0.73, 2.55]	0.34
Regular Security Updates	0.68	[0.34, 1.38]	0.28
Information Security Policies or Incident Response Plan	**2.02**	**[1.39, 2.94]**	**<0.01***
Information Security Certification	0.97	[0.78, 1.21]	0.80
Information Security Policy Enforcement	**0.72**	**[0.56, 0.93]**	**0.01***
Risk Analysis	1.05	[0.84, 1.30]	0.67
Emergency Drill	0.99	[0.81, 1.22]	0.95
Password Requirements	1.02	[0.72, 1.43]	0.93
Individual Access Control	1.02	[0.65, 1.59]	0.93
Company Age	0.98	[0.60, 1.60]	0.92
Export Activity	1.15	[0.90, 1.45]	0.26
Multiple National Branches	**1.58**	**[1.29, 1.92]**	**<0.01***
International Branches	1.06	[0.81, 1.40]	0.66
Industry Sector (only levels with significance displayed)			
H: Transportation	**0.52**	**[0.28, 1.00]**	**0.05***
Information Security Training	1.17	[0.94, 1.46]	0.15
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.17
Employees Tech (Per 100)	**1.00**	**[1.00, 1.00]**	**0.03***
Employees (Per 100)	1.07	[1.00, 1.14]	0.07
CEO-Fraud	**O.R.**	**C.I.**	***p*-value**
Interviewee Position			
Tech	**1.42**	**[1.09, 1.85]**	**<0.01***
Information Security Policies or Incident Response Plan	**1.68**	**[1.14, 2.47]**	**<0.01***
Information Security Certification	1.01	[0.81, 1.27]	0.91
Information Security Policy Enforcement	0.95	[0.73, 1.24]	0.71
Risk Analysis	1.15	[0.93, 1.43]	0.20
Company Age	1.10	[0.66, 1.84]	0.71
Export Activity	1.11	[0.87, 1.42]	0.40
Multiple National Branches	**1.29**	**[1.06, 1.58]**	**0.01***
International Branches	**1.52**	**[1.17, 1.97]**	**<0.01***
Industry Sector (only levels with significance displayed)			
D: Energy & Gas	**2.34**	**[1.02, 5.34]**	**0.04***
S: Other Services	**2.34**	**[1.18, 4.63]**	**0.01***
Per 1 Mio Annual Turnover	**1.00**	**[1.00, 1.00]**	**<0.01***
Employees Tech (Per 100)	1.00	[1.00, 1.00]	0.27
Employees (Per 100)	**1.20**	**[1.12, 1.28]**	**<0.01***

be dealt with automatically, e. g., spam e-mails that were automatically blocked using anti-virus software or spam filters. 45.1% of the participants reported that their company had to actively react to at least one incident in the last 12 months. More than half of them (1,842) were attacked multiple times. Figure 5 illustrates the reported incidents. We find that while some attack-types are evenly distributed across industry sectors, some types of attacks were more frequently reported for certain industry sectors.

We specifically asked interviewees to report on CEO-Fraud, DDoS, defacing, manual hacking, phishing, ransomware, and spyware & other malware (cf. Table 7 for ransomware and CEO-Fraud). The remaining regression analyses are listed in the Appendix (cf. Table 17–21).

We find that multiple national company locations correlated with the reporting of incidents including ransomware (O.R. = 1.58), spyware & other malware (O.R. = 1.21), manual hacking/advanced persistent threat (O.R. = 2.03), DDoS (O.R. = 1.36), CEO-fraud (O.R. = 1.29) and phishing (O.R. = 1.24).

Furthermore, companies that report information security policies or incident response plans (O.R. 1.21–2.98) correlated with the reporting of phishing, CEO-fraud, defacing, or ransomware attack. Participants who reported active enforcement of these plans were less likely to report attacks in all categories except for DDoS (O.R. 0.57–0.91).

Reporting export activity was positively correlated with reporting spyware and other malware (O.R. 1.27).

To further explore trends in Figure 5, we included the industry sector as a non-optional factor in the regression analyses which increased the AIC by no more than 4% across all incident models, which we deemed acceptable for the analysis. We find that the industry sector only map to some reported incident types. This included ransomware, that was less frequently reported in the transportation sector (O.R. 0.52) compared to the baseline and DDoS, that was more frequently reported in the communication sector than in the baseline (O.R. 4.34). Defacing incidents were more frequently reported both in the water & waste and communication sectors (O.R. 5.73 and 4.34), CEO-Fraud, was more frequently reported in the energy & gas and "other services" sectors (O.R. 2.34 both) and finally phishing, was more frequently reported for the vehicle retail sector (O.R. 1.60).

> *Summary: Detected Incidents.* We found that organizational measures more frequently map to the reporting of security incidents than reported technical security measurements. We find that larger companies, especially with tech departments reported more incidents. Finally, our findings suggest that the industry sector correlated with the reporting of security incidents.

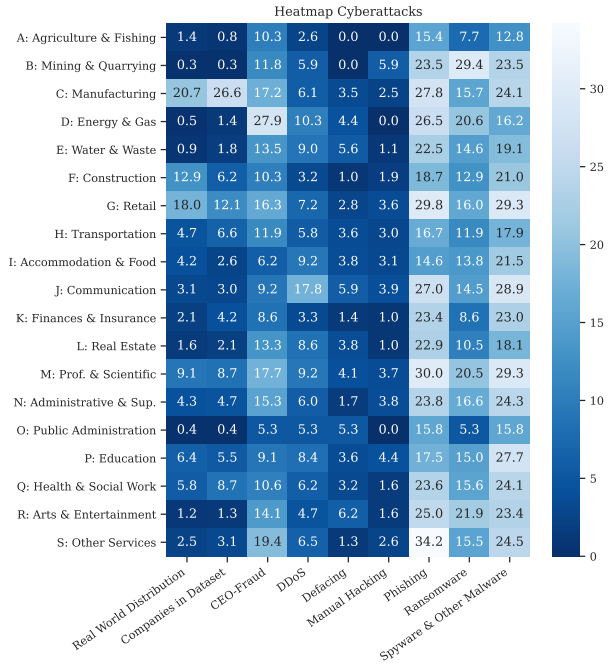

Figure 5: Heatmap; percentage of companies per sector that have experienced this attack.

5 Discussion

Below, we discuss our findings and, based on the findings, outline recommendations for industry, governments and legislators, as well as future research.

5.1 Key Findings

In relation to our research questions, we summarize the following key findings:

RQ1. "*How do company employees perceive the risk of cyberattacks?*" In general, our interviewees did not perceive a high risk of cyberattacks for their companies. Notably, however, they generally perceived the risk of mass attacks higher than the risk of targeted attacks – especially interviewees working for smaller companies. The lower perceived risk of targeted attacks might make them more susceptible to attacks such CEO-Fraud, or targeted ransom ware attacks,e. g. Emotet [9], as well as insider threats.

RQ2. "*Which and how frequent are information security measures deployed in SMEs?*" Most of our interviewees reported the deployment of technical measures such as firewalls and antivirus software compared to less frequently reported organizational measures such as certifications for information security. Furthermore, we found a high variance within reported organizational measures, with measures that require regular active engagement such information security training, risk analysis, or emergency drills being less frequently reported. Together with the previously discussed low perceived risk of targeted cyberattacks, this might make companies particularly vulnerable to attacks like CEO-Fraud and insider-threats.

RQ3. "*Which types and frequencies of attacks have our participating companies detected within the last 12 months?*" Most companies reported incidents such as phishing and malware. CEO-Fraud and (D)DoS attacks also appeared to be more common problems. Defacing and manual hacking, on the other hand, were rarely reported. However, the reporting of our interviewees does not allow us to clearly distinguish between mass and targeted attacks.

RQ4. "*How are deployed security measures and company characteristics related to reported incidents and what are the emerging victimization factors?*" We found that interviewees working in particular industry sectors more frequently reported certain types of incidents: CEO-Fraud (D: Energy and Gas), (D)DoS (J: Communication), and defacing (B: Mining). Hence, while more incidents could just be the result of better detection, we still think companies in those industry sectors might require stronger protection and security measures, and should receive special attention in relation to the specific threats they are facing. Similarly, interviewees working in Public administration and Agriculture & Fishing companies reported ransomware attacks less frequently. We find that interviewees working for companies with larger tech departments more frequently reported incidents. We also find that interviewees working in companies that more frequently deployed technical security measures did not report more security incidents. However, the reporting of organizational measures correlated with the reporting of certain types of incidents. Company demographics such as international activity and company size also contributed to more frequently reported incidents by interviewees. This also relates to the more frequent reporting of incidents by interviewees working for companies with multiple locations. Companies with multiple locations reported more manual hacking incidents. The distributed infrastructure of multiple location companies might increase the attack surface and attract manual hacking attempts. Insider threats and advanced persistent threats could exploit the distributed nature of these companies. Interviewees working for companies with information security policies or incident response plans more frequently reported certain types of incidents including ransomware, phishing and defacing. The deployment of security policies might contribute to detect incidents such as ransomware, phishing and defacing more frequently, but does not seem to prevent these types of incidents.

5.2 Future Work and Recommendations

As described in Section 4, we identified different characteristics that contributed to the reported sensitivity and risk perceptions, deployed security measures, and detected incidents in

companies in different ways. The interview results reflect the complexity of companies, and illustrate that information security is impacted by technological (e.g., maturity of measures), organizational (e.g., company size, corporate culture or sector specific security requirements) and individual (e.g., ability and willingness to provide, process and share information) characteristics of companies and their employees.

While our large-scale exploratory interview study illustrates of the impact of cybercrime on SMEs, it cannot provide in-depth causal analyses of the phenomena we identified and described in this work. Therefore, our study provides ground truth for exciting future work based on 5,000 interviews.

We provide the following ideas for future work and recommendations: (i) we outline ideas for future research in the context of cybercrime and SMEs based on our findings, (ii) based on our findings we discuss recommendations for companies to improve their information security, and (iii) provide recommendations for governments and legislators.

For Researchers. Concerning follow-up work should investigate specific aspects of cybercrime and security measures we detailed in Section 5.1. We strongly recommend to mind the correlations we found between interviewee position in the company and the reporting concerning both incidences and measures, which is hard to work around for smaller companies, where some roles might be missing entirely. The strong discrepancy between tech and management in both risk assessment 4.2 and deployed measures 4.3 should be investigated in future work. This extends to the low risk perception of participants in general. 40% of the companies in our dataset have experienced cybercrime that they had to actively counter in the last 12 months. We suspect this could be caused by misconceptions about what even qualifies as cybercrime, by low consequences resulting from most types of cybercrime or by issues tracking the consequences of cybercrime in SMEs. As a final finding, we noticed outliers in the correlation of industry sectors and incidents (cf. Figure 5). An in-depth investigation could reveal how to improve security for these sectors or adapt their approaches to other industry sectors. Finally, future research could assess the maturity and internal spread of technical security measures within organizations, since technical measures had very high reporting rates (c.f. Figure 4), but we suspect that the security impact of measures like access control and firewall setup can vary widely based on the implementation quality and maturity.

For Companies. While we do not have concrete recommendations for security measurements, our results indicate a strong correlation of organisational measures compared to technical measures and low adoption as seen in Figure 4. For companies, this indicates that they should look at organisational measures like information security policies and employee training and evaluate which of these make sense for their business model. Especially measures like a security incidence policy strongly correlate with reported incidences, as seen in section 4.4. Another interesting tendency in our analysis is that the risk sensitivity of the management generally was rated higher than the sensitivity of company staff. This can in part be attributed to bias when our interview partners held management positions. Even with that in mind, the management should spread this self-reported awareness to company staff and provide opportunities to raise information security awareness and participate in security training, especially for staff not directly involved in tech.

For Governments/Legislators. Seeing how industry sectors that tend to have high security requirements to upload by the law (K: Finances & Insurance and D: Energy & Gas) have a higher tendency to report fewer incidents despite strong detection mechanisms, the government can play a strong role in the security of small and medium enterprises. Legislators could improve cybersecurity by focusing on the areas of industries with high incidence counts for certain attacks as seen in Figure 5. For example requirements for industry sectors like J:Communication to implement security measures against (D)Dos attacks. Furthermore, our descriptive results in Section 4.2 show that risk awareness and assessment is still low and legislators should actively work on increasing awareness for information security and the risks of cybercrime. In Germany, we are already working to integrate results of the survey into a platform that provides information security guidelines and serves to raise risk awareness for German companies in cooperation with a federal ministry.

6 Conclusion

In this work we investigated effects, mitigations, and risk assessments of cybercrime in small and medium-sized companies in Germany. We contributed what is to our knowledge the first analysis of German SMEs on this scale. Our findings uncover that security awareness has arrived in all SMEs, but this awareness is not yet spread to all staff, mostly left to management and tech departments, which opens SMEs up to phishing, insider attacks and advanced persistent threats. We also discover positive effects likely related to legislation for information security and use our results to formulate recommendations for employers, governments and future areas of research. In conclusion, cybersecurity awareness in Germany has arrived in SMEs, but the resulting measures and assessment of risks are sub optimal and open enterprises up to unnecessary attack surfaces.

7 Acknowledgements

This research has been partly funded by the Federal Ministry for Economic Affairs and Energy Germany with the project “Cyberangriffe gegen Unternehmen” (BMWi-VID5-090168623-01-1/2017).

References

[1] Alessandro Acquisti, Allan Friedman, and Rahul Telang. Is There a Cost to Privacy Breaches? An Event Study. In *ICIS Proceedings*, volume 94, 2006.

[2] Ioannis Agrafiotis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1):1–15, 2018.

[3] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Gañán Carols, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. Measuring the Changing Cost of Cybercrime. In *The 2019 Workshop on the Economics of Information Security*, 2019.

[4] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. *Measuring the Cost of Cybercrime*, pages 265–300. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[5] Bisnode Deutschland GmbH. Data & Analytics - B2B und B2C. https://www.bisnode.de/.

[6] Bitkom e.V. Wirtschaftsschutz in der digitalen welt. https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf, 2017.

[7] Angela Bollhöfer, Esther; Jäger. Wirtschaftsspionage und Konkurrenzausspähung. Technical report, Max-Planck-Institut für ausländisches und internationales Strafrecht, 2018.

[8] Bundesamt für Justiz (Federal Office of Justice). (German) Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV). https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html.

[9] Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security). The State of IT Security in Germany in 2019. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.pdf?__blob=publicationFile.

[10] Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security). Cyber-Sicherheits-Umfrage 2017. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/cyber-sicherheits-umfrage_2017.html, 2018.

[11] K. P. Burnham. Multimodel Inference: Understanding AIC and BIC in Model Selection. *Sociological Methods & Research*, 33(2):261–304, 2004. Publisher: SAGE Publications.

[12] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1):69–104, 2004.

[13] Albesë Demjaha, Tristan Caulfield, M. Angela Sasse, and David Pym. 2 Fast 2 Secure:A Case Study of Post-Breach Security Changes. In *Proc. 4th European Workshop on Usable Security (EuroUSEC'19)*. IEEE, 2019.

[14] Department for Digital, Culture, Media and Sport, UK. Cyber Security Breaches Survey 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf, March 2019.

[15] D. Dittrich and E. Kenneally. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. Technical report, U.S. Department of Homeland Security, August 2012.

[16] eurostat. NACE Rev. 2 - Statistical classification of economic activities in the European Community. https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF.

[17] Federal Bureau of Investigation. High-impact ransomware attacks threaten u.s. businesses and organizations. https://www.ic3.gov/media/2019/191002.aspx, October 2019.

[18] Maarthen Gehem, Artur Usanov, Erik Frinking, and Michel Rademaker. Assessing Cyber Security: A Meta-analysis of Threats, Trends, and Responses to Cyber Attacks. Technical report, Hague Centre for Strategic Studies, 2015.

[19] Heins & Partner GmbH. Heins & Partner. http://www.heinsundpartner.de/.

[20] Annette Hillebrand, Antonia Niederprüm, Saskja Schäfer, and Iris Thiele, Sonja; Henseler-Ungar. Aktuelle Lage der IT-Sicherheit in KMU. Technical report, Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK), 2017.

[21] Internet Crime Complaint Center. 2019 Internet Crime Report. https://pdf.ic3.gov/2019_IC3Report.pdf, 2020.

[22] <kes> Zeitschrift für Informationssicherheit. Checkliste zur informations-sicherheit. https://www.kes.info/aktuelles/microsoft-studie-2018/, 2018.

[23] Maria Kjaerland. A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, 25(7):552–538, 2006.

[24] Rebecca Klahr, N. Jayesh Shah, Paul Sheriffs, Tom Rossington, Gemma Pestell, Mark Button, and Victoria Wang. Cyber Security Breaches Survey 2017. Technical report, The UK Statistics Authority, 2017.

[25] James Lewis. Economic Impact of Cybercrime - No Slowing Down. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf, February 2018.

[26] Philipp Mayring. *Qualitative content analysis: theoretical foundation, basic procedures and software solution*. SSOAR: Open Access Repository, Klagenfurt, 2014.

[27] Mike McGuire and Samantha Dowling. Cyber crime: A review of the evidence. Technical report, United Kingdom Home Office, 2013.

[28] OECD. *Digital Security Risk Management for Economic and Social Prosperity*. OECD Publishing, 2015.

[29] Sarah Osborne, Rosanna Currenti, Maria Calem, and Hannah Husband. Crime against businesses: findings from the 2017 commercial victimisation survey. Technical report, United Kingdom Home Office, 2018.

[30] Osterman Research, Inc. High-impact ransomware attacks threaten u.s. businesses and organizations. https://go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Australia.pdf, July 2017.

[31] Letizia Paoli, Jonas Visschers, and Cedric Verstraete. The impact of cybercrime on businesses: a novel conceptual framework and its application. *Crime, Law and Social Change*, 70(4):397–420, 2018.

[32] Ramona Rantala. Cybercrime against Businesses, 2005. Technical report, U.S. Department of Justice, 2008.

[33] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. In *Proc. 40th IEEE Symposium on Security and Privacy (SP'19)*. IEEE, 2019.

[34] Sasha Romanosky. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2):121–135, 2016.

[35] Ravi Sen and Sharad Borle. Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, 32(2):314–341, 2015.

[36] Katherine Smith, Murphy Smith, and Jacob Smith. Case Studies of Cybercrime and its Impact on Marketing Activity and Shareholder Value. *Academy of Marketing Studies Journal*, 15, December 2010.

[37] Statistisches Bundesamt (Federal Statistical Office). Business-Register. https://www.destatis.de/EN/Themes/Economic-Sectors-Enterprises/Enterprises/Business-Register/Tables/business-register.html.

[38] Statistisches Bundesamt (Federal Statistical Office). Classification of Economic Activities, issue 2008 (WZ 2008). https://www.klassifikationsserver.de/klassService/jsp/common/url.jsf?variant=wz2008&lang=EN.

[39] Statistisches Bundesamt (Federal Statistical Office). (German) Anteile kleiner und mittlerer Unternehmen an ausgewählten Merkmalen 2017 nach Größenklassen in %. https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/Tabellen/wirtschaftsabschnitte-insgesamt.html?nn=208440.

[40] Rock Stevens, Daniel Votipka, Elissa M Redmiles, Colin Ahern, Patrick Sweeney, and Michelle L Mazurek. The Battle for New York: A Case Study of Applied Digital Threat Modeling at the Enterprise Level. In *Proc. 27th Usenix Security Symposium (SEC'18)*. USENIX Association, 2018.

[41] Rahul Telang and Sunil Wattal. Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - An Empirical Investigation. *IEEE Transactions on Software Engineering*, 33(8):544–557, 2007.

[42] The commission of the European communities. Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003H0361&from=DE, 2013.

[43] United Nations. Statistical Division and others. *International Standard Industrial Classification of All Economic Activities (ISIC)*. Number 4 in M. United Nations Publications, 2008.

A CATI Questionnaire

We provide a translation of the interview guide for our CATIs. It contains the questions in the form of "Question? (Choices→ **Factor in Regression [B:Baseline]**), (Scale)". The response options "not specified" and "I do not know" are given for any question, but not listed below. WZ08-Classification of the industries → **Industry Sector [B:Construction]** and headcount bins → **Headcount** were adopted from the underlying commercial sampling databases. For the full questions and supplementary material of the survey, please refer to Section 3.3.

A.1 "Company" - Introduction

1. In which area do you work in your company [multiple answers possible]? → **Interviewee Position**
   (Multiple Choice: Executive/Management Board, IT & Information Security, Data Protection, Plant Security, Audit, External Service Provider, Other [free text])
2. How high do you estimate the risk for your company to be harmed by a cyber-attack in the next 12 months…
   (…that also hits many other companies at the same time? [e.g. mass sent malware], → **Risk Assessment Untargeted**;
   …that exclusively affects your company? [e.g. targeted espionage attack]); → **Risk Assessment Targeted** (Scale: Very low, Rather low, Rather high, Very high)

A.2 "Incidence" - Detected cyber-attacks

1. Always related to the last 12 months: How often has your organization been affected by and had to actively respond to the following types of attacks?
   (Ransomware - which was intended to encrypt company data, → **Ransomware**;
   Spyware - which was intended to spy on user activities or other data, Other malicious software e.g. viruses/worms/trojans → **Spyware & Other Malicious Software**;
   Manual hacking - i.e. mis-configuration and manipulation of hardware and software without the use of special malware → **Manual Hacking**;
   Denial of Service ((D)DoS) - attacks aimed at overloading web or e-mail servers, defacing attacks aimed at unauthorised alteration of company web content → **(D)DOS**;
   CEO fraud - in which a company leader was faked in order to effect certain actions by employees → **CEO-Fraud**:
   Phishing - in which employees were deceived with genuine-looking e-mails or websites e.g. in order to obtain sensitive company data) → **Phishing**
   (Scale: Amount [...])

A.3 "Measures" - Information security measures

1. Which of the following measures are currently in place in your company?
   (Written information security guidelines, written guidelines for emergency management → **Information Security Policy/Incident Response Plan**;
   Compliance with the guidelines is checked regularly and violations are punished if necessary → **Information Security Policy Enforcement**;
   Regular risk and vulnerability analyses (incl. pen-test) → **Risk Analysis**;
   Certification of information security [e.g. in accordance with ISO 27001 or VdS 3473] → **Information Security Certification**;
   Information security training for employees → **Information Security Training**;
   Exercises or simulations for the failure of important IT systems → **Emergency Drills**;
   Minimum requirements for passwords → **Password Requirements**;
   Individual assignment of access and user rights depending on the task → **Individual Access Control**;
   Regular data backups, Physically separate storage of backups → **Regular Data Backups/Seperate Backup Location**;
   Up-to-date antivirus software → **Antivirus Software**;
   Regular and prompt installation of available security updates and patches → **Regular Security Updates**;
   Protection of IT systems with a firewall) → **Firewall**;
   (Scale: Yes, no)
2. What is your impression? Would you say..:
   (a) The management is aware of the IT risks consciously and adheres to the specifications → **Information Security Sensitivity Management**;
   (b) The staff is aware of the IT risks consciously and adheres to the specifications → **Information Security Sensitivity Employees**;
   (c) In the company a lot is done for information security [INT.: more than classical protective measures] → **Information Security Investment**;

A.4 "Demographics" - Company characteristics

1. When was your company founded? → **Company Age [B:< 10 years]**; (year [free text], ≤ 2 years, < 10 years, < 25 years, < 100 years, ≥ 100 years)
2. How high was the total turnover of your company in the last financial year? → **Annual Turnover**;
   (Total sales [free text], ≤ 500,000 €, < 1 million €, < 2 million €, < 10 million €, < 50 million €, < 500 million €, ≥ 500 million €)
3. Does your company export products or services? → **Export Activity**; (Yes, no)
4. How many locations with their own IT infrastructure does your company have...?
   (Locations in Germany → **Multiple National Locations**one;[free text], Locations abroad → **International Locations** [free text])
5. How many employees of your company invest the majority of their working time in …
   (... the operation of IT in general? → **Employees Tech** (Scale: Number [free text])
6. Has your company outsourced IT functions [Multiple answers possible]
   (Email & Communication, Network Administration & Maintenance, Web Presence (e.g. Online Marketplaces, Shops, Customer Portals), Cloud Software & Cloud Storage, Information Security (e.g. Incident Detection, SIEM, Threat Intelligence) → **Outsourced IT Security**, Other [Free text], No IT Functions outsourced)
7. Which of the following measures are currently in place in your company?
   (Scale: Yes, no)

B Regressions for the Dataset

Table 8: Logistic regression: Information security policy enforcement

Factor	O.R.	C.I.	*p*-value
Export Activity	1.14	[0.96, 1.34]	0.13
Multiple National Locations	**1.34**	**[1.16, 1.54]**	**<0.01***
International Locations	**1.29**	**[1.04, 1.59]**	**0.02***
Industry Sector (only levels with significance displayed)			
D: Energy & Gas	**5.03**	**[2.17, 11.67]**	**<0.01***
G: Retail	**1.50**	**[1.11, 2.03]**	**<0.01***
I: Accommodation & Food	**1.60**	**[1.03, 2.49]**	**0.04***
J: Communication	**1.83**	**[1.17, 2.86]**	**<0.01***
K: Finances & Insurance	**7.20**	**[3.76, 13.79]**	**<0.01***
M: Prof. & Scientific	**1.54**	**[1.11, 2.14]**	**0.01***
N: Administrative & Sup.	**1.68**	**[1.15, 2.45]**	**<0.01***
P: Education	**1.70**	**[1.11, 2.58]**	**0.01***
Q: Health & Social Work	**2.06**	**[1.46, 2.90]**	**<0.01***
Interviewee Position			
Tech	**1.51**	**[1.30, 1.77]**	**<0.01***
Data Protection Officer	**1.56**	**[1.17, 2.09]**	**<0.01***
Factory Safety	0.56	[0.29, 1.09]	0.09
Risk Assessment Targeted	1.03	[0.95, 1.11]	0.46
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.17
Employees Tech (Per 100)	**1.37**	**[1.07, 1.74]**	**0.01***
Employees (Per 100)	**1.08**	**[1.02, 1.15]**	**<0.01***

Table 9: Logistic regression: Incidence response plan

Factor	O.R.	C.I.	*p*-value
Export Activity	1.07	[0.88, 1.31]	0.50
Multiple National Locations	**1.58**	**[1.32, 1.90]**	**<0.01***
International Locations	**1.38**	**[1.01, 1.87]**	**0.04***
IT-Sec External	**1.31**	**[1.11, 1.54]**	**<0.01***
Industry Sector (only levels with significance displayed)			
C: Manufacturing	**1.60**	**[1.16, 2.20]**	**<0.01***
D: Energy & Gas	**6.33**	**[2.18, 18.36]**	**<0.01***
G: Retail	**1.86**	**[1.32, 2.62]**	**<0.01***
I: Accommodation & Food	**2.66**	**[1.59, 4.46]**	**<0.01***
J: Communication	**3.52**	**[1.91, 6.46]**	**<0.01***
K: Finances & Insurance	**6.43**	**[3.10, 13.31]**	**<0.01***
L: Real Estate	**2.09**	**[1.19, 3.67]**	**0.01***
M: Prof. & Scientific	**2.65**	**[1.74, 4.03]**	**<0.01***
N: Administrative & Sup.	**1.58**	**[1.02, 2.44]**	**0.04***
P: Education	**1.68**	**[1.12, 2.52]**	**0.01***
Q: Health & Social Work	**3.06**	**[2.00, 4.69]**	**<0.01***
S: Other Services	**1.70**	**[1.03, 2.83]**	**0.04***
Interviewee Position			
Management	**0.68**	**[0.50, 0.93]**	**0.02***
Tech	**1.57**	**[1.16, 2.13]**	**<0.01***
Data Protection Officer	**1.69**	**[1.17, 2.45]**	**<0.01***
Factory Safety	**0.45**	**[0.22, 0.89]**	**0.02***
Other	**0.62**	**[0.43, 0.88]**	**<0.01***
Risk Assessment Targeted	**1.17**	**[1.06, 1.29]**	**<0.01***
Employees (Per 100)	**1.36**	**[1.25, 1.48]**	**<0.01***

Table 10: Logistic regression: Risk analysis

Factor	O.R.	C.I.	*p*-value
Company Age	**1.51**	**[1.08, 2.12]**	**0.02***
Export Activity	1.10	[0.93, 1.30]	0.28
Multiple National Locations	**1.19**	**[1.03, 1.37]**	**0.02***
International Location	1.17	[0.95, 1.45]	0.15
Industry Sector (only levels with significance displayed)			
D: Energy & Gas	**3.50**	**[1.63, 7.48]**	**<0.01***
I: Accommodation & Food	**1.63**	**[1.03, 2.57]**	**0.04***
J: Communication	**2.32**	**[1.46, 3.68]**	**<0.01***
K: Finances & Insurance	**7.27**	**[3.84, 13.77]**	**<0.01***
M: Prof. & Scientific	**1.57**	**[1.11, 2.21]**	**<0.01***
N: Administrative & Sup.	**1.69**	**[1.15, 2.50]**	**<0.01***
Interviewee Position			
Management	0.84	[0.68, 1.05]	0.12
Tech	**1.24**	**[1.01, 1.52]**	**0.04***
Risk Assessment Mass	**0.92**	**[0.87, 0.98]**	**<0.01***
Risk Assessment Targeted	**1.12**	**[1.03, 1.22]**	**0.01***
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.12
Employees Tech (Per 100)	1.07	[0.93, 1.24]	0.32
Employees (Per 100)	1.05	[0.99, 1.11]	0.08

Table 11: Logistic regression: Information security training

Factor	O.R.	C.I.	*p*-value
Company Age	**1.49**	**[1.07, 2.07]**	**0.02***
Export Activity	1.13	[0.96, 1.34]	0.14
International Locations	**1.49**	**[1.20, 1.86]**	**<0.01***
Industry Sector (only levels with significance displayed)			
C: Manufacturing	**1.40**	**[1.04, 1.87]**	**0.03***
D: Energy & Gas	**3.36**	**[1.73, 6.55]**	**<0.01***
E: Water & Waste	**1.84**	**[1.08, 3.13]**	**0.03***
G: Retail	**1.44**	**[1.06, 1.96]**	**0.02***
J: Communication	**3.30**	**[2.05, 5.32]**	**<0.01***
K: Finances & Insurance	**13.85**	**[7.12, 26.92]**	**<0.01***
L: Real Estate	**1.72**	**[1.04, 2.85]**	**0.03***
M: Prof. & Scientific	**1.56**	**[1.12, 2.18]**	**<0.01***
N: Administrative & Sup.	**1.67**	**[1.14, 2.44]**	**<0.01***
Q: Health & Social Work	**1.91**	**[1.36, 2.68]**	**<0.01***
Interviewee Position			
Tech	**1.58**	**[1.37, 1.84]**	**<0.01***
Risk Assessment Targeted	**1.11**	**[1.03, 1.20]**	**<0.01***
Employees Tech (Per 100)	1.16	[0.99, 1.36]	0.06
Employees (Per 100)	**1.14**	**[1.08, 1.20]**	**<0.01***

Table 12: Logistic regression: Emergency drill

Factor	O.R.	C.I.	*p*-value
Company Age	**1.57**	**[1.07, 2.30]**	**0.02***
Export Activity	1.13	[0.95, 1.35]	0.18
Multiple National Location	1.10	[0.95, 1.28]	0.19
International Location	1.17	[0.95, 1.44]	0.14
IT-Sec External	**0.80**	**[0.69, 0.93]**	**<0.01***
Industry Sector (only levels with significance displayed)			
C: Manufacturing	**1.64**	**[1.15, 2.34]**	**<0.01***
D: Energy & Gas	**2.95**	**[1.55, 5.62]**	**<0.01***
G: Retail	**1.57**	**[1.08, 2.28]**	**0.02***
H: Transportation	**1.72**	**[1.13, 2.61]**	**0.01***
I: Accommodation & Food	**2.61**	**[1.54, 4.41]**	**<0.01***
J: Communication	**3.13**	**[1.95, 5.03]**	**<0.01***
K: Finances & Insurance	**16.09**	**[9.39, 27.56]**	**<0.01***
L: Real Estate	**2.09**	**[1.17, 3.73]**	**0.01***
M: Prof. & Scientific	**1.52**	**[1.03, 2.25]**	**0.04***
N: Administrative & Sup.	**1.70**	**[1.09, 2.64]**	**0.02***
Interviewee Position			
Management	**0.60**	**[0.44, 0.81]**	**<0.01***
Tech	**1.58**	**[1.18, 2.12]**	**<0.01***
Other	**0.64**	**[0.45, 0.92]**	**0.02***
Risk Assessment Mass	0.95	[0.90, 1.02]	0.14
Risk Assessment Targeted	**1.18**	**[1.09, 1.29]**	**<0.01***
Employees Tech (Per 100)	**1.20**	**[1.05, 1.36]**	**<0.01***
Employees (Per 100)	**1.17**	**[1.12, 1.24]**	**<0.01***

Table 13: Logistic regression: Password requirements

Factor	O.R.	C.I.	*p*-value
Multiple National Location	1.21	[0.99, 1.48]	0.07
International Locations	**1.41**	**[1.01, 1.97]**	**0.04***
Industry Sector (only levels with significance displayed)			
C: Manufacturing	**0.67**	**[0.45, 0.99]**	**0.05***
H: Transportation	**0.59**	**[0.38, 0.93]**	**0.02***
K: Finances & Insurance	**3.80**	**[1.45, 9.92]**	**<0.01***
Interviewee Position			
Management	**0.64**	**[0.52, 0.80]**	**<0.01***
Other	**0.64**	**[0.47, 0.87]**	**<0.01***
Employees Tech (Per 100)	1.18	[0.88, 1.59]	0.27
Employees (Per 100)	**1.23**	**[1.12, 1.35]**	**<0.01***

Table 14: Logistic regression: Regular backups in separate backup locations

Factor	O.R.	C.I.	*p*-value
Company Age	**2.47**	**[1.53, 3.99]**	**<0.01***
Export Activity	1.05	[0.78, 1.41]	0.73
Interviewee Position			
Tech	**2.74**	**[2.00, 3.75]**	**<0.01***
Other	0.71	[0.48, 1.05]	0.08
Risk Assessment Targeted	1.13	[0.95, 1.34]	0.17
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.06
Employees (Per 100)	1.07	[0.95, 1.21]	0.25

Table 15: Logistic regression: Antivirus software

Factor	O.R.	C.I.	*p*-value
Company Age	**4.18**	**[1.81, 9.65]**	**<0.01***
IT-Sec External	**2.87**	**[1.40, 5.88]**	**<0.01***
Interviewee Position			
Tech	**3.33**	**[1.71, 6.51]**	**<0.01***
Risk Assessment Mass	1.15	[0.89, 1.49]	0.27
Per 1 Mio Annual Turnover	1.00	[0.99, 1.00]	0.25
Employees (Per 100)	1.39	[0.98, 1.96]	0.06

Table 16: Logistic regression: Firewall

Factor	O.R.	C.I.	*p*-value
Company Age	**3.77**	**[1.86, 7.65]**	**<0.01***
Export Activity	1.49	[0.85, 2.63]	0.17
IT-Sec External	**2.18**	**[1.29, 3.67]**	**<0.01***
Interviewee Position			
Management	**0.37**	**[0.14, 0.96]**	**0.04***
Tech	2.18	[0.87, 5.45]	0.10
Other	**0.31**	**[0.11, 0.86]**	**0.03***
Risk Assessment Targeted	1.23	[0.89, 1.70]	0.22
Employees Tech (Per 100)	0.83	[0.65, 1.07]	0.15
Employees (Per 100)	1.22	[0.94, 1.58]	0.14

Table 17: Logistic regression: Spyware & other malware

Factor	O.R.	C.I.	*p*-value
Interviewee Position			
Audit	**2.05**	**[1.23, 3.41]**	**<0.01***
Regular Backups and Separate Backup Location	1.47	[0.88, 2.44]	0.14
Antivirus Software	1.58	[0.44, 5.68]	0.48
Regular Security Updates	1.15	[0.60, 2.21]	0.66
Firewall	2.01	[0.59, 6.92]	0.27
Information Security Policies or Incidence Response Plan	1.30	[0.97, 1.75]	0.08
Information Security Certification	1.00	[0.82, 1.20]	0.97
Information Security Policy Enforcement	0.91	[0.73, 1.14]	0.41
Risk Analysis	1.16	[0.96, 1.39]	0.12
Emergency Drill	0.88	[0.74, 1.06]	0.18
Password Requirements	0.98	[0.74, 1.31]	0.91
Individual Access Control	1.15	[0.80, 1.65]	0.46
Company Age	1.11	[0.73, 1.69]	0.62
Export Activity	**1.27**	**[1.04, 1.55]**	**0.02***
Multiple National Locations	**1.21**	**[1.02, 1.43]**	**0.03***
International Locations	**1.29**	**[1.02, 1.64]**	**0.04***
Industry Sector (only levels with significance displayed)			
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.16
Employees Tech (Per 100)	**1.00**	**[1.00, 1.00]**	**0.05***
Employees (Per 100)	1.03	[0.96, 1.09]	0.42

Table 18: Logistic regression for Manual Hacking

Factor	O.R.	C.I.	*p*-value
Interviewee Position			
Management	1.45	[0.85, 2.46]	0.17
Regular Backups and Separate Backup Location	1.51	[0.35, 6.53]	0.58
Antivirus Software	0.38	[0.05, 3.21]	0.38
Regular Security Updates	0.44	[0.12, 1.64]	0.22
Information Security Policies or Incidence Response Plan	2.12	[0.85, 5.25]	0.10
Information Security Certification	0.74	[0.44, 1.23]	0.25
Information Security Policy Enforcement	0.88	[0.51, 1.52]	0.65
Risk Analysis	1.08	[0.68, 1.73]	0.74
Password Requirements	1.42	[0.59, 3.40]	0.43
Individual Access Control	2.03	[0.59, 6.97]	0.26
Company Age	1.86	[0.44, 7.78]	0.40
Export Activity	1.17	[0.70, 1.96]	0.55
Multiple National Locations	**2.03**	**[1.29, 3.20]**	**<0.01***
International Location	1.20	[0.68, 2.13]	0.53
Industry Sector (only levels with significance displayed)			
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.70
Employees Tech (Per 100)	1.00	[1.00, 1.00]	0.11
Employees (Per 100)	0.98	[0.84, 1.16]	0.85

Table 19: Logistic regression: DDoS

Factor	O.R.	C.I.	*p*-value
Interviewee Position			
Audit	**3.03**	**[1.53, 6.00]**	**<0.01***
Other	**0.34**	**[0.15, 0.78]**	**0.01***
Firewall	0.79	[0.18, 3.49]	0.75
Information Security Policies or Incidence Response Plan	1.21	[0.72, 2.06]	0.47
Information Security Certification	1.10	[0.82, 1.47]	0.54
Information Security Policy Enforcement	1.16	[0.79, 1.69]	0.45
Risk Analysis	**1.62**	**[1.18, 2.22]**	**<0.01***
Emergency Drill	0.87	[0.65, 1.15]	0.33
Company Age	0.66	[0.37, 1.18]	0.16
Export Activity	0.92	[0.66, 1.27]	0.60
Multiple National Locations	**1.36**	**[1.03, 1.79]**	**0.03***
International Locations	**1.80**	**[1.25, 2.59]**	**<0.01***
Industry Sector (only levels with significance displayed)			
J: Communication	**4.34**	**[1.95, 9.67]**	**<0.01***
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.50
Employees Tech (Per 100)	1.00	[1.00, 1.00]	0.06
Employees (Per 100)	0.99	[0.90, 1.10]	0.91

Table 20: Logistic regression: Defacing

Factor	O.R.	C.I.	*p*-value
Interviewee Position			
Data Protection Officer	1.75	[0.93, 3.29]	0.08
Regular Backups and Separate Backup Location	1.94	[0.45, 8.39]	0.38
Regular Security Updates	1.41	[0.30, 6.48]	0.66
Firewall	0.24	[0.05, 1.21]	0.08
Information Security Policies or Incidence Response Plan	**2.98**	**[1.34, 6.59]**	**<0.01***
Information Security Certification	1.07	[0.69, 1.65]	0.76
Information Security Policy Enforcement	**0.57**	**[0.36, 0.91]**	**0.02***
Risk Analysis	1.09	[0.71, 1.67]	0.69
Password Requirements	2.19	[0.92, 5.24]	0.08
Individual Access Control	0.71	[0.32, 1.57]	0.39
Company Age	1.18	[0.42, 3.31]	0.75
Export Activity	0.98	[0.60, 1.59]	0.93
Multiple National Location	1.12	[0.75, 1.67]	0.58
International Location	1.50	[0.89, 2.53]	0.13
Industry Sector (only levels with significance displayed)			
E: Water & Waste	**5.73**	**[1.22, 26.90]**	**0.03***
J: Communication	**4.34**	**[1.13, 16.69]**	**0.03***
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.53
Employees Tech (Per 100)	1.00	[1.00, 1.00]	0.25
Employees (Per 100)	1.06	[0.92, 1.22]	0.41

Table 21: Logistic regression: Phishing

Factor	O.R.	C.I.	*p*-value
Interviewee Position			
Tech	**1.28**	**[1.05, 1.57]**	**0.02***
Factory Safety	**3.60**	**[1.86, 6.97]**	**<0.01***
Antivirus Software	1.62	[0.46, 5.72]	0.45
Regular Security Updates	0.70	[0.40, 1.22]	0.21
Information Security Policies or Incidence Response Plan	**1.72**	**[1.27, 2.31]**	**<0.01***
Information Security Certification	0.91	[0.75, 1.10]	0.32
Information Security Policy Enforcement	0.86	[0.70, 1.07]	0.19
Risk Analysis	**1.25**	**[1.04, 1.49]**	**0.02***
Company Age	0.90	[0.60, 1.34]	0.60
Export Activity	1.19	[0.97, 1.45]	0.09
Multiple National Locations	**1.24**	**[1.04, 1.46]**	**0.01***
International Location	1.23	[0.98, 1.56]	0.08
Industry Sector (only levels with significance displayed)			
G: Retail	**1.60**	**[1.07, 2.40]**	**0.02***
Per 1 Mio Annual Turnover	1.00	[1.00, 1.00]	0.12
Employees Tech (Per 100)	1.00	[1.00, 1.00]	0.11
Employees (Per 100)	1.01	[0.95, 1.07]	0.81