KRIMINOLOGISCHES
FORSCHUNGSINSTITUT
NIEDERSACHSEN E.V.

Research Report No. 158

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

IT-Sicherheit
IN DER WIRTSCHAFT

Cyber-attacks against companies in Germany

Results of a representative company survey 2018/2019

Additional funding through: pwc VHV STIFTUNG

Arne Dreissigacker, Bennet von Skarczinski, Gina Rosa Wollinger

2020

RESEARCH REPORT No. 158

Cyber-attacks against companies in Germany

Results of a representative company survey 2018/2019

Arne Dreissigacker, Bennet von Skarczinski, Gina Rosa Wollinger

2020

Bibliographic Information of the German National Library
The German National Library lists this publication in the German National Bibliography; detailed bibliographic data is available on the Internet at http://dnb.de.

This publication was prepared by the Criminological Research Institute of Lower Saxony within the project "Cyber-attacks against Companies" which is part of the initiative "IT-Sicherheit in der Wirtschaft" of the Federal Ministry for Economic Affairs and Energy (BMWi). The publication is available at https://kfn.de/publikationen/kfn-forschungsberichte/

Funding code: BMWi-VID5-090168623-01-1/2017

Project duration: December 2017 - November 2020

Initiative "IT-Sicherheit in der Wirtschaft"

The initiative "IT-Sicherheit in der Wirtschaft" of the Federal Ministry for Economic Affairs and Energy aims to support in particular small and medium-sized companies in the secure use of ICT systems. Together with IT security experts from science, business and administration, the aim is to create a basis for raising awareness of IT security in SMEs in the digital economy. Through concrete support measures companies are supposed to be enabled to improve their IT security. Further information about the initiative and its services is available at www.it-sicherheit-in-der-wirtschaft.de.

ISBN: 978-3-948647-06-3

Printing: DruckTeam Druckgesellschaft mbH, Hannover, Germany.

Lützerodestraße 9, 30161 Hannover, Germany
Phone: +49 (0)511 34836-0, Fax: +49 (0)511 34836-10
Email: kfn@kfn.de, Website: www.kfn.de

Supported by:

Federal Ministry
for Economic Affairs
and Energy

on the basis of a decision
by the German Bundestag

IT-Sicherheit
IN DER WIRTSCHAFT

Additional funding through:

pwc

VHV STIFTUNG

PRELIMINARY REMARK

This research report is an English translation of the German language KFN Research Report No. 152.[1] It is not excluded that this English version may therefore contain deviations in explanations or meanings which are caused by the translation process.

ACKNOWLEDGEMENT

Such a project, and in particular such an extensive company survey on cyber-attacks against companies, cannot be carried out without the support of many people from different bodies and organisations. At this point, we would like to thank all involved actors for their support! Special thanks go to the Federal Ministry for Economic Affairs and Energy for the main financial support of the project within the initiative "IT-Sicherheit in der Wirtschaft". In addition, we would like to thank PricewaterhouseCoopers and the VHV Foundation for the additional funding in the form of personnel funds and resources. We would like to thank our cooperation partners from the L3S Research Centre and Leibniz University Hannover, all associated partner organisations and their representatives, as well as all those involved in the project advisory board and in the regional company round table at PwC in Hannover for stimulating discussions and feedback on the questionnaire and the results. We would also like to thank the survey institute Kantar EMNID for their support in finalising the questionnaire and for the professional execution of the survey. We would also like to express our special thanks to the companies and institutions and their representatives who took part in the expert interviews prior to the questionnaire design, in the pre-test of the questionnaire and in the company survey. Only in this way was it possible for us to gain secure and differentiated insights into the spread and consequences of cyber-attacks and to identify risk and protection factors that should help to assess the scope of the phenomenon and help prevent cyber-attacks.

Hanover, August 2020
The authors

[1] Dreißigacker, Arne; Skarczinski, Bennet von; Wollinger, Gina Rosa (2020): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Ed. by Kriminologisches Forschungsinstitut Niedersachsen e. V. Hannover (KFN-Forschungsbericht Nr. 152). Available online at: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_152.pdf, checked on 7/24/2020.

ABBREVIATIONS

2FA	Two-Factor Authentication
ADM	Working Group of German Market and Social Research Institutes
AG	Public limited company
Bitkom	Federal Association for Information Technology, Telecommunications and New Media
BMWi	Federal Ministry for Economic Affairs and Energy of Germany
BVMW	Federal Association of Small and Medium-sized Companies- Entrepreneurial Association of Germany
BYOD	Brind-your-own-device
BSI	Federal Office for Information Security of Germany
CATI	Computer Assisted Telephone Interview
CD	compact disc
DDos	Distributed Denial of Service
DoS	Denial of Service
eco	eco - Association of the Internet Industry
ENISA	European Network and Information Security Agency
GDV	General Association of the German Insurance Industry
GmbH	limited liability company
ICT	Information and communication technology
IfM	Institute for SME Research Bonn
IHK	Chamber of Industry and Commerce
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
KFN	Criminological Research Institute Lower Saxony
n.a.	not specified
KG	Limited partnership
CI	Confidence Interval
L3S	Research Centre L3S of Leibniz University of Hannover
n.r.	irrelevant
NIST	National Institute of Standards and Technology
OHG	General partnership
PKS	Police crime statistics

PwC	PricewaterhouseCoopers WPG mbH Germany
SD card	Secure Digital Memory Card
SME	Small and medium-sized enterprises
StGB	German Criminal Code
SVB	Employees subject to social insurance contributions
URS	Company register system
USB	Universal Serial Bus
WIK	Scientific Institute for Infrastructure and Communication Services
WZ	Economic sector
ZAC	Central contact point Cybercrime for the Economy at the Police

CONTENT

1 INTRODUCTION

Digitization can generally be described as the spread of digital technologies, which has an impact on many areas of life.[2] Organizations and companies are also confronted with this development in many ways. However, they are not only unilaterally exposed to digitization and a digitization discourse that generates pressure to act[3], but they themselves influence the process of digitization.[4] Taking into consideration the perceived potential for optimisation and value creation (e.g. simplification and acceleration of process flows, cross-border cooperation, development of data-based business models), companies make organisational decisions on the use of digital technologies/data/services and on their development/generation/marketing.[5]

Among the unintended side effects of these decisions are, for example, the growing risks of cybercrime and the associated damage to companies and their customers and business partners, which raise questions about the security of IT systems in more or less digitized companies.

From a criminal law perspective, cybercrime covers a wide range of offences. In the context of companies, this includes, for example, criminal offences such as fraud (§ 263 StGB), extortion (§ 253 StGB) or mobbing acts committed via the Internet. These are often[6] subsumed as "cyber-enabled crime"[7], as the Internet and IT systems connected via it serve merely as "means of committing crimes" and are not the actual target of the attack. As a rule, they are subsumed under long-standing criminal offences within the German Criminal Code (StGB). In contrast, "cyber-dependent crime" includes offences that only became possible with digital networking and are primarily directed against IT systems or digital data. For these offences, new offences have been created in the StGB. These include, for example, the spying or interception of data (§§ 202a, 202b and 202c StGB), data theft (§ 202d StGB), data alteration, computer sabotage (§§ 303a and 303b StGB) and the falsification of evidentially relevant data (§ 269 StGB).

Criminological research that deals with cybercrime focuses comparatively often on offences in the area of "cyber-enabled crime" that is directed against private individuals,[8] although in general there is still relatively little criminological research.[9] This is particularly true for cybercrime

[2] Cf. Büchner (2018b: 333f.).

[3] Cf. Büchner (2018a); Pfeiffer (2015).

[4] Cf. Büchner (2018b).

[5] The companies differ in terms of their "data literacy", which is measured according to Büchner (2018b: 339) is often in a "tension relationship" to the "possibilities of data generation used".

[6] E.g. insult according to § 185 StGB, slander according to § 186 StGB or defamation according to § 187 StGB

[7] On the distinction between cyber-enabled crime and cyber-dependent crime, see e.g. Council of Europe (2001); Eisele (2016: 255); Robertz, Oksanen and Räsänen (2016: 2); Seidl and Starnecker (2017: 338); Wall (2004: 20); Bundeskriminalamt (2018).

[8] E.g. Chen et al. (2016); Fansher & Randa (2018); Näsi et al. (2017); Tsitsika et al. (2015); Henson et al. (2016) or Wegge et al. (2016).

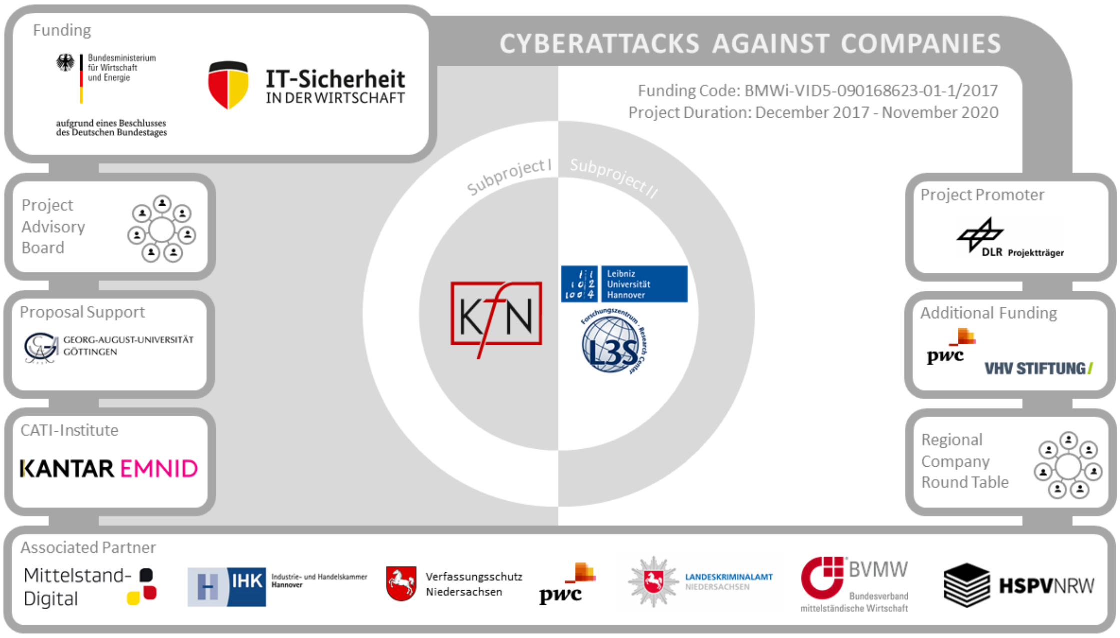
[9] Cf. Meier (2012). Reep-van den Bergh and Junger (2018) provide an overview of research on cybercrime against private individuals in Europe.

in the business sector. Above all, there is a lack of studies that go beyond a descriptive depirction of the spread of cybercrime and examine factors influencing the risk of victimisation.[10]

A survey commissioned by the German Federal Ministry for Economic Affairs and Energy (BMWi) from WIK-Consult on the IT security of SMEs in Germany has shown that there is a great need for action in the field of cyber security for small and medium-sized companies.[11] But also for larger companies and other areas of the economy, such as the financial sector, studies for the years 2015 and 2016 have shown that 40 to 50 % of companies were affected by cybercrime in the sense of industrial espionage, sabotage or data theft within two years (Bitkom 2015; KPMG 2015; PwC/University of Halle 2016).

In view of this initial situation, it must be a central concern both for criminological research and for the German economy to react appropriately to the threat posed by cybercrime and to deal with the issue of IT security in a more targeted manner. In order to be able to assess the risks, spread and extent of cybercrime in particular and to evaluate possible protective measures, e.g. with regard to the cost-benefit ratio, valid results of scientific research that is as independent as possible, is required.

Figure 1 **Project participants**


Funding
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
IT-Sicherheit IN DER WIRTSCHAFT
CYBERATTACKS AGAINST COMPANIES
Funding Code: BMWi-VID5-090168623-01-1/2017
Project Duration: December 2017 - November 2020
Subproject I
Subproject II
KfN
Leibniz Universität Hannover
Forschungszentrum L3S Research Center
Project Advisory Board
Proposal Support
GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN
CATI-Institute
KANTAR EMNID
Project Promoter
DLR Projektträger
Additional Funding
pwc
VHV STIFTUNG
Regional Company Round Table
Associated Partner
Mittelstand-Digital
IHK Industrie- und Handelskammer Hannover
Verfassungsschutz Niedersachsen
pwc
LANDESKRIMINALAMT NIEDERSACHSEN
BVMW Bundesverband mittelständische Wirtschaft
HSPVNRW

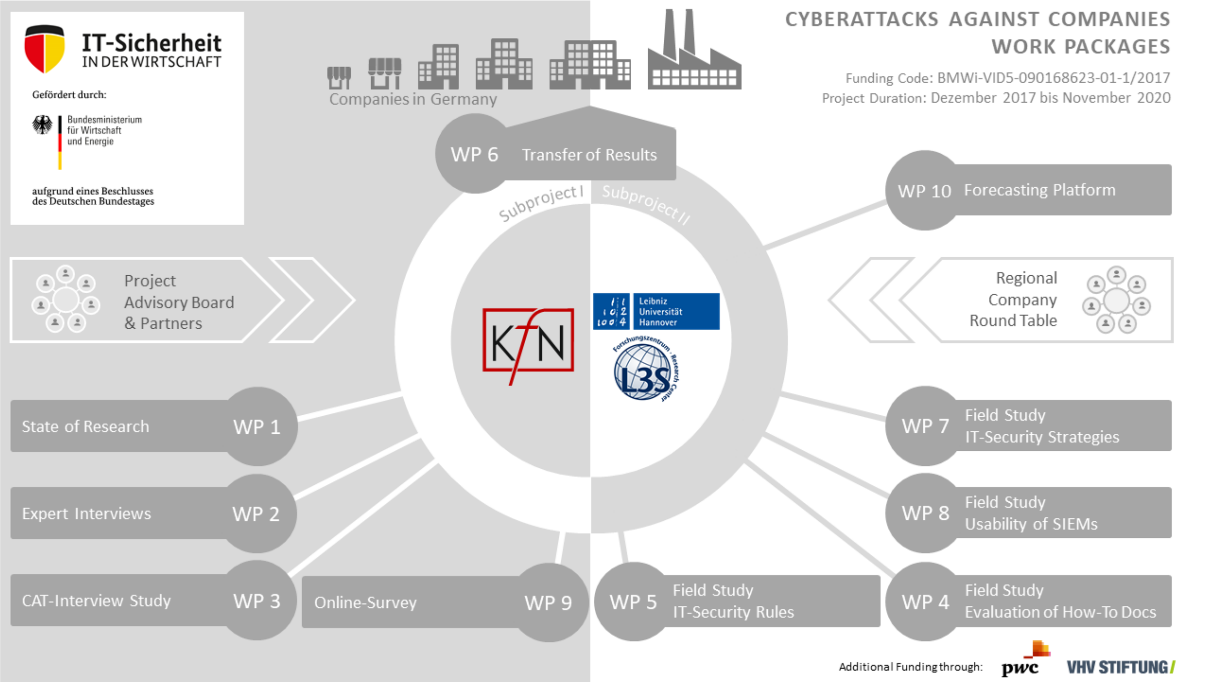
The Criminological Research Institute of Lower Saxony (KFN) together with the Research Center L3S of the Leibniz University Hannover has therefore decided to conduct a broad investigation which should provide differentiated knowledge about the types and frequency of cyber-attacks. It is also intended to determine the spread of prevention measures and IT security standards. Based on these results, the transfer of scientific findings into practice is also to be ensured. For this purpose, prevention strategies and concrete recommendations for action are to be developed.

[10] Cf. Meško (2018).

[11] Cf. Bundesministerium für Wirtschaft und Energie (2012).

The project "Cyber-attacks against companies" is funded as part of the initiative "IT security in the economy" of the Federal Ministry for Economic Affairs and Energy and it, receives additional funding from the VHV Foundation and PricewaterhouseCoopers and is supported by an advisory project advisory board[12] (Figure 1[13]). It has a modular structure and uses different survey methods to answer the respective research questions (Figure 2). To date, interviews have been conducted with IT managers in companies as well as with experts from law enforcement agencies, the Office for the Protection of the Constitution, the Federal Office for Information Security and the insurance industry,[14] followed by field studies with IT employees in companies on the topics "Evaluation of documentation in the context of small and medium-sized companies" and "IT security rules in everyday working life".

Figure 2 **Work packages**


IT-Sicherheit
IN DER WIRTSCHAFT
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Companies in Germany
CYBERATTACKS AGAINST COMPANIES
WORK PACKAGES
Funding Code: BMWi-VID5-090168623-01-1/2017
Project Duration: Dezember 2017 bis November 2020
WP 6 Transfer of Results
Subproject I
Subproject II
WP 10 Forecasting Platform
Project Advisory Board & Partners
Regional Company Round Table
KfN
Leibniz Universität Hannover
Forschungszentrum L3S Research Center
State of Research WP 1
Expert Interviews WP 2
CAT-Interview Study WP 3
Online-Survey WP 9
WP 5 Field Study IT-Security Rules
WP 7 Field Study IT-Security Strategies
WP 8 Field Study Usability of SIEMs
WP 4 Field Study Evaluation of How-To Docs
Additional Funding through:
pwc
VHV STIFTUNG

In addition, a survey of 5,000 companies in Germany with a special focus on small and medium-sized companies was conducted, which forms the basis for this report. The project is scheduled to run for three years from December 2017 to November 2020.

1.1 Object of research

1.1.1 Cyber-attacks

Compared to other criminological objects of investigation, such as classic property crime, research on "cyber-dependent crime" is associated with special characteristics: The variation and

[12] In addition to the sponsors of the project, the Federal Association of Medium-Sized Businesses, Mittelstand-Digital, the Chamber of Industry and Commerce Hanover, the State Criminal Police Office Lower Saxony, the Office for the Protection of the Constitution of Lower Saxony, the Chair of Corporate Accounting and Business Informatics at the University of Osnabrück, the Chair of Criminology and Sociology at the University of Police and Public Administration NRW in Cologne, VHV Insurance and the IT security company CIPHRON are represented in the project.

[13] Further information on the overall project and all those involved can be found at https://cybercrime-forschung.de.

[14] Results of the expert interviews can be found at Stiller et al. (2020).

combination possibilities of attack vectors[15], malware and perpetrators' procedures are hard to overlook due to rapid technological developments.[16] In addition, the absolute number of non-registered crimes[17] can be regarded as very large.[18] Certain attacks or individual steps of related attacks, such as the unauthorised copying and passing on of personal data, may not be recognised by those affected. It is possible that their consequences will only become apparent at a later point in time, when a tangible damage to the company (e.g. the lost competitive advantage due to a spyware attack) or third parties has occurred. A study of the consulting company Pascual & Marchinion indicates, for example, that people whose credit card data was stolen as a result of incidents at banks or retail companies in the previous year, are almost three times more likely to become victims of identity theft.[19] The intentions of the perpetrators, e.g. the purpose for which data is copied, manipulated or destroyed without authorisation, are in many cases also not immediately apparent to private users or companies. Even the question of whether it is a targeted attack or one that affects many companies can only be answered very vaguely. In this context, the study focuses on cyber-attacks, regardless of their criminal law assessment, that were, one the one hand, noticed and, on the other hand, required an active response from the company to prevent or limit damage. This response can range from manually moving malware-infected data to a quarantine area to system recovery of an entire network. A police report of an ongoing CEO fraud would also be a corresponding reaction. The survey differentiated between the following types of cyber-attack: Ransomware, spyware, other malware, manual hacking, (D)DoS attack, defacing, CEO fraud and phishing.[20]

1.1.2 Companies

As potentially affected by these cyber-attacks, companies are the focus of this study. According to the German Federal Statistical Office, companies are "defined as the smallest legally independent unit that keeps accounts for commercial or tax law reasons. In addition, the company must make an annual assessment of its assets or the success of its economic activity. This also includes facilities for carrying out a freelance activity".[21]

A particular focus is on small and medium-sized companies (SMEs). According to a common SME definition of the Institut für Mittelstandforschung Bonn (Institute for SME Research) of January 2016, companies are classified as follows, using the employee size class and the annual turnover. Companies with up to 9 employees and an annual turnover of up to EUR 2 million

[15] Attack vectors are combinations of attack paths and techniques with which attackers gain unauthorised access to IT systems (see Bundesamt für Sicherheit in der Informationstechnik, 2017: 78).

[16] The approaches and perspectives for differentiating and classifying cyber-attacks differ relatively widely in criminological research. Depending on the focus (approach or goals of the perpetrators, consequences for those affected, etc.), cyber-attacks are classified and investigated in categories that are more or less discriminatory (see Meško, 2018).

[17] The number of non-registered crimes includes all crimes of which the police have no knowledge, and which are therefore not included in official crime statistics. A distinction can be made between the *relative number of non-registered crimes,* which can be at least partially "illuminated" by research, and the *absolute number of non-registered crimes.* The *absolute number of non-registered crimes* includes criminally relevant acts that are not remembered or not recognized by the persons involved, for example (cf. Prätor 2014).

[18] Bayerl & Rüdiger (2018) point out that the police crime statistics (PKS) are hardly valid regarding cybercrime offences due to the presumably very large number of non-registered crimes.

[19] See Pascual & Marchini (2015).

[20] An explanation of the types of cyber-attacks and their operationalisation can be found in Chapter 7, where identity theft or credit card fraud, for example, were not considered as an attack type but as a consequence or purpose of a cyber-attack.

[21] Statistisches Bundesamt (2018: 5). See also Hartmann (2017: 188f.).

form the group of micro companies, up to 49 employees and a turnover of up to EUR 10 million/year belong to the group of small companies and up to 499 employees and an annual turnover of up to EUR 50 million belong to the group of medium-sized companies.[22] These SMEs are in turn distinguished from large companies with 500 or more employees and an annual turnover of more than EUR 50 million. This study deviates from this in so far as only the characteristic of the employment size class was used for stratification and drawing of the sample and for the presentation of the results. The data about the annual turnover was collected and considered separately. In addition, the group of micro companies (up to 9 persons employed) has been excluded as it is the company group that is poorly represented in the databases used for sampling and would have been difficult to reach. Their inclusion would therefore have exceeded the time and cost frame of this survey.

The respondents from companies included in this study were asked to represent their companies as legally independent entities. This means, for example, that several locations of the company were included, but no subsidiaries or parent companies, as these operate as their own legal form.

1.2 Research questions

The aim of the company survey is to obtain differentiated information on the prevalence of cyber-attacks to which companies have had to react to and to ascertain the consequences (system failures, costs etc.) and reactions (police reporting behaviour, involvement of IT security providers etc.). Furthermore, it will be analysed which factors increase the risk of a successful attack and which IT security measures are in place. Regarding the reaction to attacks, it is of interest what experiences have been made with law enforcement authorities and insurers, if applicable, and what reasons exist for not reporting incidents or not having insurance protection for information security violations. This should also lead to conclusions about how criminal prosecution should be structured so that companies can make greater use of it. Furthermore, the survey of specific company characteristics should help to make meaningful distinctions between companies that have been affected by certain types of attacks.

In the first company survey within the project "Cyber-attacks against Companies", the following research questions are central:

- What IT security measures against cyber-attacks have companies put in place?
    - Do the companies have written guidelines? Are they continuously adapted to the changes of cyber-attacks?
    - Does the company have specialized employees who are explicitly assigned to the task of fending off or preventing cyber-attacks? Are external specialists used instead or in addition?
    - How do companies control their own IT security? In particular, is a security check of the IT system carried out using methods that attackers could use to

[22] Source: https://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/ (accessed on 07.06.2019). The European Commission uses a definition of SMEs that differs in terms of the size class of employees: only those with up to 249 employees and annual turnover of EUR 50 million or annual balance sheet total of EUR 43 million are counted as medium-sized companies (source: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/ (accessed on 7th June 2019)).

    penetrate the system without authorisation (penetration testing)? Is there a formal certification of the IT security system?

- What types of cyber-attacks have companies had to respond to in the last twelve months?
    - What differences in the type and frequency of cyber-attacks can be seen when differentiating by employee size class and industry affiliation of the companies?
    - How long does it take the companies to replace the affected system or to bring it into an operational state?
    - Are there any suspicions about the perpetrators?
    - How have companies reacted to attacks?
    - In the case of attacks linked to extortion, have they provided all or part of the requested service?
    - How much damage has been caused by perceived cyber-attacks?
    - Are the companies surveyed insured against damage resulting from cyber-attacks? What benefits have insured companies received following a cyber-attack and how satisfied are they with them?
- What is the police reporting behaviour of affected companies?
    - What are the reasons for not reporting?
    - What experiences did the reporting companies have with the police?
    - In how many cases have perpetrators been identified?
- Is there a correlation between the frequency of cyber-attacks and the existence of certain IT security measures?
    - Can it be proven that investments in IT security reduce the probability of successful cyber-attacks?
    - Which IT security measures have a particularly strong effect, if any?

Before answering these questions with the results of the company survey in chapters 5 to 10, the progress of research on cyber-attacks against companies is presented in detail in chapter 2 and the method and selection procedure for data collection is explained in chapter 3. The sample is then described based on certain company characteristics and their distribution in the population, after which a transition to further company characteristics is made in Chapter 4.

After the results on the IT security structure of companies, their assessments of IT risks, the experienced cyber-attacks in the last twelve months, the details on the most severe attack and the effectiveness of IT security measures, Chapter 11 provides a summarizing conclusion with references to methodologically induced restrictions as well as an outlook on the following analyses and upcoming research modules within the project "Cyber-attacks against Companies".

2 STATE OF RESEARCH

2.1 Characterization of the state of research

The literature on the subject of "cyber-attacks against companies" is constantly growing due to the worldwide topicality and explosiveness of the phenomenon and is characterised by a high degree of heterogeneity both in terms of the respective research focus and the groups of authors and their motivations. For example, the research focuses vary in the victim perspective (organization or individual), the perpetrator perspective (external attacker, insider), a technical or non-technical focus on IT security measures, the treatment of related topics (digitization, industry 4.0, costs of cyber-attacks, cyber insurance, etc.), the underlying data (survey or analysis of secondary technical data, size and composition of the sample) or the validity of the results for the underlying population (international, national, regional). Regarding authors and editorships, it is possible to distinguish, for example, between the following three groups: a) governmental, policy-related and other non-commercial institutions, b) commercial or entrepreneurial organisations and c) academic research institutions. However, this distinction is not always possible due to the fluid boundaries between them.

Public authorities and other non-commercial bodies regularly publish information on case numbers of the phenomenon of "cyber-attacks against businesses". These author groups usually focus on the primary field of activity of the respective institution, mostly in a neutral manner, provide additional information or suggestions for action to affected companies, but usually focus less on the investigation of causes and in-depth analysis. Especially findings of official publications are often based on police crime statistics, and thus only include officially reported incidents, but not the non-registered crimes.

A second group of authors have a business or commercial background in publishing surveys and reports. This is, for example, the increase of their own reputation, the presentation of their own competences, representation of interests or contract research. Such literature is also very heterogeneous, partly using emotional content but also scientific methods and procedures. It may not be independent and sometimes contains subjective statements and results that are in harmony with the own business background. Reports, studies and surveys by this group of authors represent most of the publicly available literature on the subject of "cyber-attacks against companies"[23] and therefore significantly shape the public perception of the phenomenon.[24]

The third group has a research-specific or academic background. The aim of this literature usually is to gain knowledge based on scientific methods and to disseminate this knowledge as independently as possible to a wide range of addressees. Literature of these authors usually has an appropriate and transparent description of the sample, data and methods used and specifies

[23] Cf. Gehem et al. (2015).

[24] Cf. Paoli et al. (2018).

quality criteria and limitations that serve to evaluate the findings. Literature of this group, especially empirical research, is, although the phenomenon "cyber-attacks against companies" is not new, strongly underrepresented and needs a fact-based expansion.[25]

Despite the large number and diversity of publicly available literature on the topic of "cyber-attacks against companies", the fragmented, non-comparable, sometimes contradictory or missing foundation of the research database is repeatedly criticised.[26] This reaches all the way to the accusation that there is hardly any reliable data on the phenomenon of "cyber-attacks against companies", even that many actors are no longer able to distinguish reliable from unreliable data and therefore make poorly informed decisions.[27] The predominant literature therefore does not seem to fully satisfy the information needs of the actors, be they companies, public authorities, researchers or private individuals.

2.2 Procedure for selecting and processing the literature under consideration

At the beginning of the review related literature, a comprehensive online research was conducted with the aim of identifying relevant empirical studies and reports on the topic of "cyber-attacks against companies".[28] In the course of the review of the state of research, more than 350 titles were systematically recorded in a literature management program, categorized within more than 150 groups and provided with approx. 1,700 knowledge elements (comments, keywords, etc.). The documents come from a wide variety of authors from Germany and abroad and do not necessarily have a focus on small and medium-sized companies, as it can be assumed that the phenomenon of "cyber-attacks against companies" does not respect national borders[29] or size classes and therefore relevant findings can also be found outside this literature. Since it is not possible to reproduce this literature in its entirety, this literature status is limited to a selection of the most relevant sources, which are, for example, characterised by new, particularly surprising and contradictory findings or, in the opinion of the authors, represent a good reflection of the majority of the literature sifted. A focus is also on quantitative studies that collect and evaluate primary data.[30]

An example for a limited selection of literature for the benefit of a systematic and summarized presentation of the respective findings is the study "Current Situation of IT Security in SMEs" by the Scientific Institute for Infrastructure and Communication Services (WIK GmbH)[31], which forms the starting point for the literature status described below. Supplemented in content

[25] Organisation for Economic Co-operation and Development (2015); McGuire & Dowling (2013); Agrafiotis et al. (2018); Ngo & K. Jaishankar (2017); Gehem et al. (2015); Cobb (2015); Paoli et al. (2018).

[26] Gehem et al. (2015); Florencio & Herley (2012); McGuire & Dowling (2013); Hillebrand et al. (2017); Cobb (2015); Ryan & Jefferson (2003).

[27] Cf. Ryan & Jefferson (2003).

[28] The online research included various databases and search engines (e.g. DuckDuckGo, Google, Google Scholar, AISeLibrary, Springer, Elsevier, etc.) as well as forward and backward searches for keywords (e.g. cybercrime, online crime, cybercrime, cyber-attacks, etc.) with a focus on organizations and companies. German and English language sources were evaluated without restrictions on specific regions, business sectors or company sizes. The main focus was on literature that collects and analyses primary data. The online research was carried out from December 2017 to April 2019.

[29] Cf. Böhme (2013); Kigerl (2012).

[30] The following recently published studies could no longer be included in the presentation of the state of research: Verband der TÜV e.V. (2019); Berg & Niemeier (2019).

[31] Hillebrand et al. (2017).

and scope, the state of research now presents 32 studies or reports published between 2006 and 2019.

A tabular summary of the literature relevant for this research report is included[32] in Table 53. There, background information on sample sizes, sample compositions, methods used, etc. can be looked up, if indicated by the authors. This is urgently required in order to put alleged commonalities or contradictions of the literature under consideration into a larger context. An explanation of selected findings from the literature mentioned above follows in section 2.4.

2.3 Limitations of the considered literature

In the context of the review of the literature and the associated review of numerous different studies and reports on the subject of "cyber-attacks against companies", the most frequent limitations will be named and briefly discussed in this section. This is intended to sensitize the reader to a certain extent and help with the interpretation of the related literature. The limitations mentioned in the areas of a) sample type, sample size and sampling, b) operationalisation and c) presentation of results and transparency can lead to the fact that the results of the listed studies can be compared with each other and with this study only to a very limited extent.

(a) Sampling type, sample size and sampling procedure

The composition of the participating companies in some studies is highly biased with respect to the distribution of certain characteristics of the respective population, such as the employee size class or the sector. The findings of the sample under investigation can therefore not be transferred to the population, or only to a very limited extent. The weighting of answers according to suitable estimators for the population, for example data from the business register for surveys of German companies, can help to "re-proportionalise" statements from the sample in relation to the population. In comparison to a true random sample, the self-recruitment of participating companies in studies can also be problematic. Depending on how widespread the possibility of taking part in a survey is, it may be that only certain companies take part or only certain companies learn about a survey. This is the case, for example, if web links to the questionnaires are only sent to the company's own customers or to members of its own association who already have a certain level of awareness of the topic "IT security". Companies without these networks or relevant prior knowledge do not become aware of these surveys. Furthermore, self-recruitment in connection with anonymous surveys can hardly exclude multiple participation of a company.

A further limitation may result from the use of small sample sizes, which in studies are often justified by budget or time restrictions. The larger the sample size, the more precise the information on the population can be made. In particular filter questions and granular answer categories can reduce the respective sample cases of a group to such an extent that statistical significance is hardly possible.

In order to be able to transfer the findings of a study to a population, it is important to first define and transparently describe the basic and selection population. Some studies explicitly include or exclude participating companies of certain sectors or sizes, while other studies do

[32] p. 163ff. (Annex 1: Additional tables).

not. In addition, industry definitions are created by the participants themselves without allowing a transition to a common standard (e.g. WZ08, NACE, NAICS). Subsequently, it is left to the interviewee to classify himself in this industry scheme, which can lead to the proverbial comparison of *apples and pears* between two studies.

b) Operationalisation

During the implementation of a study, it is determined how the theoretical characteristics to be investigated are to be made measurable in concrete terms (so-called operationalisation). During the literature research, many inconsistent and sometimes non-transparent definitions on the topic of "cyber-attacks against companies" came to light, which greatly limit a direct comparison of the several studies. The term "cyber-attack", for example, was defined technically or legally, was already evaluated as a mere attempt or was used only after damage had occurred. In addition, a "company" was divided into independent legal entities, a group of companies or individual operating sites with locations in Germany or abroad. No distinction was made between risk perceptions according to the perception for one's own company or a peer group, as a general threat situation or concrete threats from certain types of attack or attackers. Heterogeneous definitions and operationalizations will always exist due to the numerous players in the "IT security market" but should be consciously taken into account when interpreting the results.

Further restrictions may result from the data collection. For example, although the object of investigation on cyber-attacks against companies is the organisation, data is in most cases provided in writing or verbally by individuals with limited knowledge and their own preferences, ideas and motivations (so-called self-reporting bias). The database thus contains a certain degree of subjectivity. In addition, to ignorance and difficulties in understanding, social desirability can also lead to respondents providing information that does not correspond to reality. In order to control this, it is possible to compare the response behaviour of different groups of respondents (e.g. do managing directors answer the question about the assessment of the working atmosphere differently than IT employees?) It goes without saying that respondents can only provide information about events that they themselves are aware of. Cyber-attacks unnoticed by the organisation or the person interviewed cannot be investigated by these forms of study.

c) Presentation of results and transparency

Further limitations within the reviewed literature result from missing information or lack of transparency. For example, in some answer options it is not determined whether companies do not know the facts, do not want to answer or the question does not apply to the situation of the company at all. Also, questions about IT security measures often do not specify whether they were already in place before or after a relevant cyber-attack. In addition, standard information on the selected population, the sample as well as the structure and functions of respondents is sometimes missing. Survey and observation periods (e.g. the year 2017 or the last 12 months) are also not clearly delimited and presented. There are even studies available that make statements on observation years, although these had not yet been completed at the time of data collection.[33] Last but not least, there is a general risk of misinterpretation by readers due to a lack of transparency about the underlying specific question, as some studies only publish their conclusions but not the question originally asked.

The limitations described here are intended to sensitize readers and help them to interpret the literature summarized in the following section more appropriately.

2.4 Central results of previous research

This section summarises and explains the studies listed in Table 53[34] (Annex 1). In order to make it easier for the reader to appreciate the content, the contents are summarised thematically[35] and not title by title. Direct comparisons of the findings available in the literature with the findings of this company survey will be discussed within chapters 5 to 10 where possible and meaningful.

2.4.1 Structural characteristics

Of the 32 selected studies, 18 were from commercial or entrepreneurial author groups, nine from government, policy and other non-commercial organisations and five from academic research institutions. They were published between 2006 and 2019, with around two-thirds of them dating from 2017 to 2019. The studies vary greatly in their scope (12 - 110 pages, median 33 pages) and in 16 cases concern exclusively German, in six cases exclusively another nation and in ten cases companies/organisations from several countries. If the underlying data were collected through interviews or questionnaires (26 cases), the sample sizes ranged between 254 and 9,500 respondents (median 679). Ten studies did not specify which persons or functions were interviewed.

No information on the population underlying to the sample was provided in about two thirds of the cases. Information on the type of sampling and sampling procedure was not provided in 17 cases. The structure of the sample was described by most of the companies, mostly by stating the sectors and sizes of companies surveyed.[36] A reflection on the possibility of generalising the results is often missing and in the worst case is tacitly assumed. Four of the studies go beyond a purely descriptive presentation of the results and apply instruments of conclusive statistics.

2.4.2 Risk assessment and threat situation

Studies to assess the risk and threat of cyber-attacks against oneself and one's own organisation or against other peer groups (e.g. other industries) are based on self-assessments. Information on this was identified in 17 of the 32 studies.

[33] Here, it appears that years have been used in graphs without indicating that the year does not refer to the distribution of the characteristic throughout the year, but that the characteristic was only surveyed in that year.

[34] ANNEX 1: Additional tables, p. 167ff.

[35] See "Content characteristics" in table 53.

[36] As a rule, separate groups were formed here, only a few referred to official classifications (e.g. WZ classes, ISIC, NACE, NAICS etc.).

According to a survey conducted by the German Federal Office for Information Security (BSI), 92 % of the companies surveyed in 2017 considered cyber-attacks to be a relevant threat to operational capability.[37] One year later, however, this figure falls by 14 % to 76 %, while the proportion of companies expecting an increasing threat situation[38] rose by 22 % from 66 % to 88 % over the same period.[39] In contrast, the German Insurance Association (GDV) found in a survey that only 32 % to 43 % of the companies surveyed perceive the risk of their own victimisation as high or very high.[40] A study conducted by the Northern Chamber of Industry and Commerce Germany (IHK Nord) in 2013 came to similar conclusions (38 % of those surveyed perceive the situation as threatening).[41] A study by PwC sees the threat level as increased or greatly increased, very similar to the BSI 2017 survey (66 %, even 85 % for Industry 4.0 companies), but also sees signs of a gap between the generally perceived threat level and awareness of one's own risk.[42] Another PwC study shows that the generally perceived threat is perceived more strongly than the own threat.[43] The GDV also notes this difference in their own perception: 72 % see the risk of cybercrime for SMEs, but only 34 % see their own risk of being affected by cybercrime.[44] The IHK Nord also states that companies that have already been attacked assess the situation as more threatening than others.[45] Further surveys report high perceived threats, but without distinguishing between the threat perception for the general public and the individual.[46] According to a survey by Hiscox, 66 % of respondents say that cyber threats are among the most severe threats to the company, along with fraud.[47]

In addition, only a few studies deal with what companies feel threatened by in concrete terms or how this is manifested. According to a study by the Max Planck Institute for Foreign and International Criminal Law, companies feel threatened above all by other IT attacks (44 %), physical espionage (34 %), data espionage (31 %) and social engineering (16 %).[48] Cisco cites Targeted Attacks (78 %), Advanced Persistent Threats (76 %) and the expansion of Bring your own device (BYOD) practices as the greatest concerns of IT security decision-makers.[49] PwC has found that the increased threat level is mainly reflected in the general existence of new types

[37] Cf. Bundesamt für Sicherheit in der Informationstechnik (2017).

[38] Cf. Bundesamt für Sicherheit in der Informationstechnik (2019a).

[39] In the first version of the report of Bundesamt für Sicherheit in der Informationstechnik (2019b) 87% of the respondents did not agree with this statement. After a note on this and other conspicuous results, a corrected version of the report was published on 18 April 2019, in which all results in the "Opinion" section were corrected. In a related press release ("BSI corrects results of the Cyber Security Survey" source: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Cyber-Sicherheitsumfrage-180419.html), it is stated that "a technical error in the analysis [...] led to a falsification of a few results of the survey".

[40] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[41] Cf. Industrie- und Handelskammer Nord e.V. (2013).

[42] Cf. PricewaterhouseCoopers AG WPG (2017).

[43] See PwC Strategy& GmbH (2016).

[44] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[45] Cf. Industrie- und Handelskammer Nord e.V. (2013).

[46] See for example eco - Verband der Internetwirtschaft e.V. (2017). 95% of companies see a (strongly) growing threat; see also techconsult (2017) The statements and results of the Techconsult survey leave many methodical and content-related questions. For example, it is stated that the perceived threat to IT and information security increased steadily between 2014 and 2017 and the threat index based on the own survey rose from 46 to 50 during this period, but without going into the underlying operationalization or giving any orientation for estimating the level

[47] Cf. Hiscox (2018).

[48] Cf. Bollhöfer & Jäger (2018).

[49] Cf. Cisco (2017).

of attacks, the rising number of cyber-attacks and additional legal requirements.[50] The Scientific Institute for Infrastructure and Communication Services (WIK), on the other hand, has described the perceived threat situation, among other things, by the increasing need to protect corporate data in 2012 and 2017. In this context, customer, invoice, personnel, and process data in 2017 in particular will have higher protection requirements than in 2012.[51]

Overall, the risk assessments revealed by studies cover a wide range. In addition to the limitations mentioned in Section 2.2, this may be due to differences in the respective observation periods, locality and non-representative sampling.

2.4.3 Prevalences

This section summarizes the frequencies of victimization identified in the literature. These prevalence rates always refer to a defined period of time (e.g. lifetime prevalence, annual prevalence, etc.) in which the respective companies or defined groups of companies (e.g. in sectors, in regions) were affected by various types of cyber-attacks to a relevant extent. Information on this was identified in 17 of the 31 studies[52] and in each case given as a percentage of the companies that were victims of cyber-attacks (%).

(a) Types of attack

One of the first and representative surveys in the United States in 2005 questioned nearly 8,000 companies about cyber-attacks. Across all industries and types of attacks, 67 % of companies surveyed said they had been the victim of cyber-attacks at least once in 2005, with a broad distinction made between cyber-dependent crimes (e.g. virus, denial of service, sabotage: 44 % of all companies), cyber-enabled crimes (e.g. fraud, personal data breach: 8 % of all companies) and other incidents (e.g. hacking, phishing, spyware: 15 % of all companies).[53] Similarly, high 12-month prevalence (66.5 %) is also found ten years later by Paoli et al., but for Belgian companies. They distinguish between the five non-technical types of cybercrime illegal access (50 %), data/system interference (44 %), cyber extortion (24 %), internet fraud (13 %) and cyber espionage (4 %).[54] Gehem et al. found very different results in their qualitative meta-analysis of 65 cybersecurity reports.[55] Depending on the author of the underlying study, the types of attacks occurring in 2013 and 2014 sometimes differed considerably: Malware, for example, was classified as the top threat by the European Network and Information Security Agency (ENISA), while the Russian software company Kaspersky puts the prevalence rate for malware at around 61 % (after spam at around 65 %), the Internet site Hackmageddon at around 21 % and the US communications group Verizon at around 12 %.[56]

[50] Cf. PricewaterhouseCoopers AG WPG (2017).

[51] Cf. Hillebrand et al. (2017).

[52] It is difficult to obtain official data on attacks against companies from police crime statistics because no distinction is made between the victim groups of companies and private individuals. For example, the Federal Criminal Police Office uses external data, e.g. Bitkom, to present the federal cybercrime situation picture; Cf. Bundeskriminalamt (2018).

[53] See Rantala (2008).

[54] Cf. Paoli et al. (2018).

[55] Cf. Gehem et al. (2015).

[56] Cf. ibid.

The consultancy and auditing firm PricewaterhouseCoopers (PwC) comes to the following conclusions in two German studies: in 2015, 56 % of the companies surveyed registered at least one cyber-attack[57], and in 10 % (2015) and 19 % (2016) of the cases the attacks were successful.[58] According to a study by Bitkom from 2018, 68 % of the companies stated that they had been affected by incidents in the area of Digital Business Protection in the last 24 months, with the theft of IT and telecommunications equipment (32 %), theft of sensitive digital data (23 %) and non-digital theft of data and machines (21 %) as well as digital sabotage of systems (19 %) being the most common types of attack. Other classic forms of cyber-attacks, such as digital social engineering or spying on digital communication, were represented by only 11 %.[59] For some response categories, the difficulty in distinguishing and delimiting the response categories provided is striking: for example, the theft of digital data can also be caused by the theft of physical devices. It also remains unclear in many studies what exactly is meant by an incident: Due to a lack of definitions, this could be a registered attack attempt without consequences, averted cyber-attack, an actual damage event or simply an IT malfunction.

The Bitkom study distinguishes between being affected and actually suffering damage: 47 % of industrial companies have suffered damage from digital attacks in the last two years. The three most common types of attack were malware (24 %), the exploitation of software vulnerabilities (16 %) and phishing (16 %).[60]

The GDV reports an overall victimisation rate of 30 %, with undefined attacks by e-mail (59 %) and hacker attacks (26 %) among the most common types of attack.[61] It should be noted here that the degree of victimisation was defined with the occurrence of damage and generally no time period was specified in which damage occurred. Furthermore, no explanation was given as to which types of attack are hidden behind the "e-mails" mentioned (e.g. spam, social engineering, etc.). According to the BSI, with 33 %, the impact of cyber security incidents on the companies surveyed is similarly low in 2018. Here again, the degree to which they were affected was not defined more precisely, although it was stated that in around half of the cases the attacks were successful, e.g. had access to IT systems or influenced functionalities.[62] The IHK Nord also reports unspecified 12-month prevalence of 33 %, but for the year 2013.[63] The Ponemon Institute cites strongly upwardly deviating prevalence for the fiscal year 2017. 98 % of the companies surveyed had experience with malware, 69 % with phishing/ social engineering, 63 % with botnets, 43 % with stolen devices, 53 % with denial of service attacks, 40 % with insider attacks and 27 % of the companies surveyed with ransomware attacks.[64]

The US communications group Verizon differentiates between "incident" and "Data Breaches",[65] but for the so-called incidents it names denial of service attacks (DoS) with over

[57] See PwC Strategy& GmbH (2016).

[58] See PricewaterhouseCoopers AG WPG (2017).; no definition of what constitutes a successful attack was given.

[59] Cf. Bitkom e.V. (2018).

[60] Cf. ibid.

[61] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[62] Cf. Bundesamt für Sicherheit in der Informationstechnik (2019a).

[63] Cf. Industrie- und Handelskammer Nord e.V. (2013).

[64] Cf. Ponemon Institute (2017b).

[65] Incident = A security event that compromises the integrity, availability or confidentiality of an information asset. Breach = An Incident that results in confirmed disclosure of information to unauthorized third parties.

70 %, losses due to errors with approx. 15 % and phishing with under 10 %.[66] The American IT company IBM has a more technical focus with its services for monitoring customer infrastructure and names unexpected injections (79 %), information collection/analysis (8 %) and employment of probabilistic techniques (5 %) as the main attack mechanisms.[67] The UK insurance company Hiscox reported that 45 % of respondents had suffered a cyber-attack in the last 12 months, but did not specify the underlying types of attack or what was considered an attack.[68] Klahr et al. also mention the type of attack that caused the most damage (12-month prevalence/largest damage) in addition to the 12-month prevalence.[69] These were mainly fraudulent emails or forwarding to fraudulent websites (72 %/ 43 %), malware or spyware (33 %/ 20 %), others impersonating organisation in emails or online (27 %/ 12 %) and ransomware (17 %/ 8 %).[70] The Ponemon Institute sees general malware (77 %), exploit of existing software vulnerability (75 %) and web-borne malware attacks (64 %) as the three most common types of attack. It is noticeable here that advanced persistent threats, with 51 %, is already in fifth place out of eleven named, which seems a lot for such highly individualized and cost-intensive attacks.[71]

(b) Industries

The picture is also heterogeneous when it comes to the impact on the business sectors. According to Rantala, telecommunications (82 %), computer system design (79 %) and the manufacture of durable goods (75 %) were most affected, while the forest/fishing (44 %), agriculture (51 %) and catering (54 %) sectors were least affected[72]. According to the results of the UK Commercial Victimisation Survey, the sectors most affected by online crime between 2014 and 2017 were administration and support (36 %), information/communication (23 %) and manufacturing (7.5 %), based on different data sets.[73]

According to Bitkom, the most affected sectors were chemicals and pharmaceuticals (74 %) and automotive engineering (68 %), with the study focusing on industrial companies.[74] The British insurance company Hiscox sees the sectors financial services, energy, telecommunications and government institutions as being most affected, but without giving more precise figures.[75] Verizon mainly lists the health (24 %), hotel and catering (15 %) and public sector (14 %) sectors as victims,[76] and IBM cites information and communication technology (33 %), manufacturing (18 %) and financial services (17 %) as the main targets of attacks.[77] When differentiating prevalence by sector, it is striking that hardly any uniform sector definitions are

[66] Cf. Verizon (2018).; all incidents were assigned to the groups Error, Hacking, Malware, Misuse, Physical and Social.

[67] Cf. IBM Cooperation (2018).

[68] Cf. Hiscox (2018).

[69] Cf. Klahr et al. (2017).

[70] Cf. ibid.

[71] Cf. Ponemon Institute (2016).

[72] Cf. Rantala (2008).

[73] Cf. Osborne et al. (2018).

[74] See Bitkom (2018).

[75] Cf. Hiscox (2018).

[76] Cf. Verizon (2018).

[77] Cf. IBM Cooperation (2018).

used, e.g. according to WZ08, NACE or ISIC, which makes direct comparison of these studies almost impossible.

(c) Size of companies

Prevalence by size of company show a comparatively homogeneous picture: larger companies are attacked more frequently than smaller companies. For 2018, the BSI states that 43 % of large (>250 employees) and only 26 % of small and medium-sized companies (<250 employees) were affected by cyber security incidents, but without defining more precisely what a cyber security incident actually means.[78] Also according to Rantala, across all types of attack, larger companies are more affected than smaller ones.[79] Hiscox also supports this observation, but also makes clear that there is no linear relationship (the larger the company, the greater the risk). Rather, large differences are also apparent within the groups. For example, companies with up to 250 employees have prevalence of between 15 % and 55 % and companies with more than 250 employees have prevalence of between 60 % and 85 %.[80] Deviating from the divided observation of higher prevalence rates in larger companies, Bitkom reports that industrial companies with more than 500 employees are less affected by cyber-attacks with a share of 60 % than smaller companies (10 to 99 employees: 68 %; 100 to 499 employees 73 %).[81] The communication company Verizon states that the majority (58 %) of the data breaches considered across all industries occur among small companies.[82] However, the Northern Chamber of Industry and Commerce (IHK) sees no significant difference between the two directions and states that "the size of the company has relatively little influence on the attack rate".[83]

(d) Regional distribution

Comparatively few studies examine regional differences in the prevalence of cyber-attacks against companies. In its 2018 report, Hiscox found that companies in Spain were most frequently affected (57 % of incidents). This was followed by the Netherlands (50 %), Germany (48 %), UK (40 %) and the USA (38 %).[84] This is very different from the previous year's report, which only compared larger companies from three countries: According to this report, US companies were most affected with 72 %, Germany was second most affected with 65 % and the UK with 59 %.[85] In their meta-analysis based on data from the online platform Hackmageddon for 2013, Gehem et al. also name the USA as the country most affected by cyber-attacks (approx. 58 %), followed by the UK (approx. 14 %).[86]

In view of the findings of the state of research described above, it is hardly possible to identify clear trends with regard to prevalence, i.e. the extent to which companies are affected by cyber-

[78] Cf. Bundesamt für Sicherheit in der Informationstechnik (2019b).

[79] Cf. Rantala (2008): victimisation of companies in 2005 across all types of attacks: 2-24 employees (50%), 25-99 (59%), 100-999 (70%) and >1,000 employees (82%).

[80] Cf. Hiscox (2018).

[81] Cf. Bitkom e.V. (2018).

[82] Cf. Verizon (2018).

[83] Cf. Industrie- und Handelskammer Nord e.V. (2013).

[84] Cf. Hiscox (2018). Only the five countries mentioned were considered.

[85] Cf. Hiscox (2017). Only the three countries mentioned were considered.

[86] Cf. Gehem et al. (2015).

attacks. On the contrary, almost any statement seems possible, possibly due to different definitions, procedures and samples.

2.4.4 IT security structures

IT security structures are understood to be all technical and organisational measures of an organisation to protect itself against cyber-attacks in a preventive, compensatory or detective manner. Information on IT security structures can be found in 25 of the 31 studies.

a) General self-assessment

According to a survey of more than 2,900 IT specialists conducted by the US technology company Cisco, 58 % rate their security infrastructure as currently secure.[87] At a similar level, with 54 %, the surveyed companies estimate their cyber-resistance as high or very high, according to the Ponemon Institute.[88] The GDV figures are higher: According to this, 74 % of small (10 to 49 employees) and 63 % of medium-sized companies (50 to 249 employees) state that they are sufficiently protected against cybercrime.[89]

(b) Technical measures

According to the GDV, almost all companies surveyed use virus scanners and firewalls (97 %), (automatic) security updates (94 %) and systematic data backups (84 %).[90] Hillebrand et al. and the IHK Nord also come to similar conclusions.[91] Password-protected access for all employees (68 %), encryption of sensitive data (54 %) and a ban on the use of private devices (41 %) are, however, less frequently implemented measures.[92] According to a Bitkom study, all companies surveyed also use password protection on all devices (100 %), firewalls (100 %), virus scanners (100 %) and regular data backups (100 %). Less frequently used measures include encryption of data media (47 %), encrypted e-mail traffic (36 %), penetration tests (24 %) and intrusion detection systems (20 %).[93] Bollhöfer et al. see deviations from the Bitkom study, especially in the use of penetration tests and crisis simulations. For companies with more than 50 employees these deviations are only around 16 %, for less than 50 employees even only 5 % of the companies surveyed.[94] According to Cisco (2016), only 58 % of the companies surveyed used firewalls, 44 % encryption/data protection, 42 % e-mail/messaging security, 41 % anti-malware/endpoint security, 40 % access control and 35 % identity administration.[95] In particular, the information on the use of firewalls and anti-virus solutions deviates from the previously mentioned studies. The British market research institute Vanson Bourne, on the other hand, sees the use of intrusion detection/prevention systems as significantly higher than Bitkom, with

[87] Cf. Cisco (2017).

[88] Cf. Ponemon Institute (2016) Cyber-resistance here consists of the single items Ability to contain a cyber-attack, Ability to quickly detect a cyber-attack, Ability to recover from a cyber-attack, Ability to prevent a cyber-attack and was measured on a scale of ten. For this statement, all figures higher than six were combined.

[89] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[90] Cf. ibid.

[91] Cf. Hillebrand et al. (2017); Industrie- und Handelskammer Nord e.V. (2013).

[92] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[93] Cf. Bitkom e.V. (2018).

[94] Cf. Bollhöfer & Jäger (2018).

[95] Cf. Cisco (2017).

56 % of the companies surveyed using them, whereas anti-virus (71 %) and e-mail security solutions (70 %) are below the figures of other studies.[96] With regard to the use of multi-factor authentication, Vanson Bourne states a share of 43 %, which PwC puts at around 51 %.[97] Osborne et al. note that the use of IT security measures can vary by industry and company size. While the use of anti-virus solutions across all industries and company sizes is between 80 % and 88 %, encryption software (1-9 employees: 40 %; >50 employees: 66 %), restrictions on e-mail and web use (1-9 employees: 33 %; >50 employees: 80 %) and restrictions on storage media (1-9 employees: 26 %; >50 employees: 63 %) are used significantly more frequently by larger companies than by small companies in the wholesale and retail sector. Across all company sizes, it is particularly noticeable that companies in agriculture, forestry and fisheries have data security guidelines less frequently (13 %) than, for example, companies in wholesale and retail trade (47 %). These two sectors also differ by at least a factor of two in the measures restrictions on email and web use and restrictions on storage media.[98] The Security Monitor 2016 from “Deutschland sicher im Netz e.V. (DsiN)” summarizes for small and medium-sized companies that single technical solutions still predominate and that there is a lack of holistic approaches to IT security.[99]

(c) Organisational measures

In its study, Rantala does not ask about the existence of IT security measures, but about the detection of incidents by these measures in the companies surveyed. All the internal measures that were asked and which uncovered incidents, such as guidelines for employees (60 %), network watch centre (71 %), intrusion testing (63 %), employee training (59 %) and business continuity plan (60 %), were relatively close to each other between 59 % and 71 %. The apparently only measure that led to fewer discoveries or perceptions of incidents was "Other" (34 %), which includes limiting system access, automated patch management and measures to comply with the Sorbanes-Oxley Act.[100] Critical to this is above all the assignment of a concrete measure to a detection by the person interviewed, as well as the fact that not all measures are designed to detect incidents, but rather, especially in the case of patch management and the limitation of access, to prevent incidents. Bitkom states that the industrial companies surveyed implement the following organizational measures, among others: Determination of access rights for certain information (100 %), clear classification of company secrets (84 %), regulations for taking IT equipment on business trips (66 %), clean desk policy (50 %), security certifications e.g. according to ISO 27001 or German BSI Grundschutz (49 %), introduction of an information security management system (35 %)[101] and regular security audits (34 %). Security measures in the area of personnel include background checks to fill sensitive positions (59 %), training on security issues (59 %) and whistle-blower systems (22 %).[102] Vansom Bourne, in

[96] Cf. Vanson Bourne (2014).

[97] Cf. PricewaterhouseCoopers Network (2018).

[98] Cf. Osborne et al. (2018).

[99] Cf. Brandl et al. (2016).

[100] Cf. Rantala (2008).

[101] According to the Bundesamt für Sicherheit in der Informationstechnik (2019a) 47% of those surveyed have an information security management system (ISMS), 61% of which are large companies and 37% small and medium-sized companies.

[102] Cf. Bitkom e.V. (2018).

contrast to Bitkom, states the use of audits/reporting with 56 %, whereas user training is stated to be similarly high with 56 % use among the companies surveyed.[103] Klahr et al. put the total participation of employees in training for the last 12 months at only 20 %, although there are sometimes significant differences between industries and company sizes. In addition to these measures, Klahr et al. mention, among others, the restriction of user access (all companies: 79 %; large companies 96 %), the monitoring of user activities (all companies: 42 %; large companies 80 %) and the existence of formal cyber security guidelines (all companies: 33 %; large companies 71 %).[104]

As already explained under the restrictions in section 2.2, it is not always possible to make clear distinctions between the security measures mentioned. For example, some studies group the measure "encryption" into a generic term,[105] while others distinguish between the encryption of network connections (80 %), encryption of data media (54 %) and e-mail encryption (45 %), the characteristics of which can vary greatly, as shown in this example.[106] In addition, it is noticeable that the existing studies very rarely place the security features mentioned in a direct connection with the prevalence, but rather present both independently of each other.

2.4.5 Investments and budgets

This section describes which investments in information and cyber security the surveyed companies have already made or intend to make and which financial resources are available or have been made available for this purpose. Information on investments and budgets was identified in 13 of the 31 studies.

Similarly, the studies included show different results regarding the investment in information security. For 2016, PwC reports that 51 % of the companies surveyed expect investment in information security to increase and 35 % expect it to remain unchanged in the current year,[107] while in another PwC study 67 % of companies expect investment to increase and 24 % expect it to remain unchanged.[108] However, there is no definition of what such investments include. The Association of the Internet Industry (eco) also reports for 2017 of predominantly increasing investments (61 %) without, however, indicating whether these are expected or actual developments.[109] However, PwC noted that actual investments were sometimes significantly lower than the higher investment expectations expressed by companies. As reasons for investment, the companies surveyed in the PwC study cited primarily regulatory requirements (76 %), digitization (74 %) and customer requirements (66 %) as the main reasons for investment, while current security incidents in their own company (46 %) and their own industry (37 %) ranked last.[110]

[103] Cf. Vanson Bourne (2014).

[104] Cf. Klahr et al. (2017).

[105] See for example Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018), Cisco (2017) and eco - Verband der Internetwirtschaft e.V. (2017).

[106] Cf. Bundesdruckerei GmbH (2017). Among others also Hillebrand et al. (2017) and Bitkom e.V. (2018) distinguish similar encryption types.

[107] Cf. PricewaterhouseCoopers AG WPG (2017) The sample on which the survey is based contains companies with 200 to 1,000 employees.

[108] Cf. PwC Strategy& GmbH (2016). The sample on which the survey is based includes companies with one to >10,000 employees.

[109] Cf. eco - Verband der Internetwirtschaft e.V. (2017).

[110] Cf. PricewaterhouseCoopers AG WPG (2017).

Klahr et al. found deviating results regarding the reasons for investments. The most frequently cited reasons were the protection of customer data (51 %), the protection of intellectual property or business secrets (28 %) and business continuity (19 %). Compliance reasons followed in seventh place with a share of 7 %.[111] In contrast, the Ponemon Institute reports that 66 % of the companies surveyed invest in IT security primarily to maintain the availability of systems and 46 % for compliance reasons, but only 35 % for fear of data loss or theft and only 6 % due to fears of declining sales.[112]

Klahr et al. note in this respect that investments and their justifications vary according to company size and sector. For example, the information/communication/utilities sectors spent an average of GBP 19,500, but the hospitality sector spent only GBP 620 in the last financial year on hardware, software, salaries, training and outsourcing related to cybersecurity.[113] The German Bundesdruckerei also reports that the majority (56 %) of German companies will make higher investments in IT security. Around one third of the companies with more than 2,000 employees stated that they would even increase investments considerably, whereas companies with less than 100 employees only do so to 18 %. Above all, the energy/supply sector (75 %), transport/logistics (75 %) and banks/insurance companies (62 %) report increasing investments, while only 40 % of companies in the mechanical and plant engineering sector report this.[114] It remains unclear whether and which industries possibly already have a higher level of safety and therefore invest less. In addition, certain industries will probably be more strongly induced to invest by regulatory requirements than others (e.g. by the German IT security law (ITSiG) or foreign equivalents).

Hillebrand et al. quote concrete figures in EUR but note that the results are to be assessed with caution due to the low willingness of the surveyed SMEs to provide information. For 2017, SMEs planned to spend an average of EUR 2,600 on IT security, with the level of investment increasing with the size of the company. Overall, only around 2 % of SMEs planned investments of more than EUR 10,000 in 2017[115], with Klahr et al. citing higher investments, albeit in British pounds. According to this, British companies spent an average of GBP 4,590 (median GBP 200) in the last financial year, with around a third of the companies making no investments in cybersecurity at all.[116]

According to Hillebrand et al., IT security expenditures account for about 11 % of the IT budget of SMEs.[117] According to a report by the British market research institute Vanson Bourne, this share averages 12 % for large companies if the company has not yet experienced a data breach. After such a data breach, the IT security budget accounts for 18 % of the IT budget. Overall, the IT budget of the companies surveyed accounts for around one-fifth of their annual turnover.[118] However, this breakdown of the IT security budget does not apply to all companies. In

[111] Cf. Klahr et al. (2017).

[112] Cf. Ponemon Institute (2016).

[113] Cf. Klahr et al. (2017).

[114] Cf. Bundesdruckerei GmbH (2017).

[115] Cf. Hillebrand et al. (2017).

[116] Cf. Klahr et al. (2017) differences by size class (mean/median in GBP): 2-49 employees 2,600/200; 50-249 employees 15,500/5,000; >250 employees 387,000/21,200.

[117] Cf. Hillebrand et al. (2017).

[118] Cf. Vanson Bourne (2014).

55 % of the companies surveyed, the budget for security is included in the IT budget, but 36 % of the companies report that this is only partly the case. After all, 9 % of the companies separate the security and IT budget completely.[119]

When asked what companies whose investments have increased in the last 12 months spent money on, the companies surveyed in the Vanson Bourne study cited employee training (67 %), cloud security (58 %) and monitoring services (54 %) as the most important reasons. In contrast, investments in outsourcing software (40 %), outsourcing infrastructure (39 %), outsourcing services (39 %) and outsourcing staff (35 %) were the least ones named.[120] The Ponemon Institute goes one step further and has calculated an estimated return on investment (ROI) for nine of the surveyed investments. According to this, investments in security intelligence systems (ROI: 21.5 %), advanced identity and access solutions (ROI: 19.7 %) and automation, orchestration and machine learning (ROI: 17.1 %) were particularly profitable, while enterprise deployment of governance, risk and compliance (ROI: 9.4 %) and automated policy management (ROI: 6.9 %) came in last.[121] Interestingly, subject to a comparison with an internal rate of return, all investments in the nine technologies mentioned above seem to be profitable.

Also, for the budgets and investments presented, the literature presents a mixed picture. Although a tendency towards increasing investments could be identified, it remains open at what level and in which areas this is the case.

2.4.6 Damages and consequences

This section describes the negative, direct or indirect effects of cyber-attacks against companies that are not expressed in monetary units (e.g. EUR, GBP or USD). Details can be found in 17 of the 31 studies. Also, in the area of the damage and consequences of cyber-attacks, inconsistent definitions and possible responses of the studies under consideration are often striking, which makes a direct comparison of the available findings difficult or even impossible.

According to the German Insurance Association (GDV), the companies surveyed cited the economic damage caused by cyber-attacks mainly as costs for recovery and investigation (59 %), business interruptions (43 %), damage to reputation (14 %), theft of customer data (11 %) and theft of own data/company secrets (8 %).[122] In contrast, the German BSI reports first of all of business disruptions, which resulted in costs for 87 % of organizations, and only afterwards in costs for recovery (65 %).[123] According to Cisco, approximately one-fifth of companies have lost customers and almost 30 % have lost revenue due to a cyber-attack.[124] Hiscox, on the other hand, reports that only 7 % of companies affected by a data breach have lost customers.[125] Of the companies that lost customers, Cisco reports that less than 20 % of customers were lost in 60 % of cases, with around 5 % of companies reporting that between 80-100 % of customers

[119] Cf. Cisco (2017).

[120] Cf. Vanson Bourne (2014).

[121] Cf. Ponemon Institute (2017b). To determine the ROI, the income was divided by the costs of the investment. In addition, a term of 3 years, a discount interest rate of 2% p.a. and no residual value were assumed. Operating and maintenance costs were considered conservatively.

[122] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[123] Cf. Bundesamt für Sicherheit in der Informationstechnik (2019a).

[124] Cf. Cisco (2017).

[125] Cf. Hiscox (2018).

were lost. The same order of magnitude (± 2 %) applies to lost sales.[126] Bitkom mentions, albeit with a broader focus on economic security instead of cyber-security, deviating cases of loss. Image damage among customers and suppliers (41 %) is most frequently cited, followed by undefined data protection measures (40 %) and the failure/theft/damage of information systems (27 %). The costs of investigations and replacement measures (16 %) are also mentioned significantly less frequently than, for example, at the GDV.[127] Also in contrast to the studies by the GDV and Bitkom, but with a focus on the most expensive consequences, the Ponemon Institute cites loss of information (43 %), business interruptions (33 %), loss of turnover (21 %) and damage to equipment (3 %) as losses that occurred in the companies surveyed.[128] In addition to the above-mentioned, quite frequent consequences of cyber incidents, Klahr et al. state that the theft of money (6 %) and the loss or theft of assets, trade secrets or intellectual property (1 %) were relatively rare among the companies surveyed. The impact of cyber incidents in the last 12 months on the overall organisation in terms of customer complaints (5 %), damage to reputation (4 %), loss of sales or share price (4 %) and penalties or legal costs (<1 %) were also mentioned rather rarely.[129] However, Klahr et al. also state that the consequences indicated vary according to the size of the company.[130]

In its representative survey of US companies for 2005, Rantala reports that[131] companies across all industries and size classes had a median system downtime of 16 hours caused by security incidents. In 40 % of companies, the downtime was 25 hours or more. The longest downtime was in the consumer durables manufacturing industry, with a median of 32 hours.[132] Overall, no information was provided on the types of attacks that led to these failures, the distribution of the downtime among the respective company sizes, or the type of systems that failed.

The US technology company Cisco states that 13 % of companies surveyed had less than one hour of system downtime due to security breaches. Around 45 % of companies reported downtime of between one and eight hours, and 9 % of companies surveyed reported downtime exceeding 24 hours. For the vast majority (60 %), no more than about one-third of a company's systems were affected by an incident, while in 15 % of cases more than half of the company's systems failed.[133]

The Ponemon Institute shows how many days on average it took to overcome cyber-attacks of certain attack types. According to this, consequences caused by malicious code (55.2 days), malicious insiders (50 days) and ransomware (23.1 days) lasted the longest, whereas attacks by malware (6.4 days) and botnets (2.5 days) were resolved relatively quickly.[134] According to Klahr et al,[135] 57 % of UK companies did not need any time at all to restore normal operations after the most severe attack of the past 12 months. Another 23 % of the companies surveyed

[126] Cf. Cisco (2017).

[127] Cf. Bitkom e.V. (2018).

[128] Cf. Ponemon Institute (2017b).

[129] Cf. Klahr et al. (2017).

[130] Cf. ibid.

[131] See Rantala (2008).

[132] Cf. ibid.

[133] See Cisco (2017).

[134] Cf. Ponemon Institute (2017b).

[135] Cf. Klahr et al. (2017).

were able to restore it within one day and another 13 % within one week. Only 2 % of companies took a month or more. Similar to Klahr et al., Paoli et al. find that the companies were able to manage the majority of cyber-attacks (Illegal access: 81.7 %; Data/system compromise: 79.6 %; Cyber blackmail: 68.2 %) within one working day.[136] With a focus on industrial espionage and competitive intelligence, Bollhöfer et al. state that the effects of incidents did not lead to restrictions in 39 % of the companies surveyed or could be remedied in the short term (38 %).[137] A total of 5 % of the companies affected report that the effects threatened their existence. Regarding SMEs, Hillebrand et al. state that impairments due to IT security problems were either non-existent or minor (31 %) or lasted less than one day (41 %).[138]

As the literature about damage and consequences shows, there are a large number of negative consequences for companies, with varying degrees of severity. Although the perceived threat of cyber-attacks may be very acute, most companies tend to report relatively manageable damage, which should not diminish the explosive nature of the phenomenon, especially from the perspective of severely affected companies.

2.4.7 Costs incurred

This section presents costs, expressed in monetary units (e.g. EUR, GBP or USD), incurred in connection with cyber-attacks against companies for the selected literature. Concrete details are given in 13 of 32 studies.

On the basis of an extrapolation, but with a focus on digital industrial espionage, sabotage and data theft, the Bitkom study estimates total losses for industrial companies in the past two years at around EUR 43 billion.[139] Of these, image damage (EUR 8.8 billion), patent law infringements (EUR 8.5 billion) and loss, theft, damage to systems and operational processes (EUR 6.7 billion) make up the largest items, while data protection measures (EUR 1.4 billion), extortion with stolen/encrypted data (EUR 0.3 billion) and other losses (EUR 0.3 billion) make up the smallest items.[140] However, the losses are not shown for different industries, company sizes or types of attack, but only as total losses. In addition, all cost types are added together without taking into account possible accumulation or distribution effects and extrapolated using the prevalence rate for the number of German industrial companies. PwC reports for companies with 200 to 1,000 employees that around 36 % of respondents suffered financial impacts. The average monetary loss amounted to EUR 41,000, with no further structural characteristics being differentiated here either.[141] Since a wide range can be assumed, especially in the case of monetary losses, and the mean value depends heavily on extreme values, the mean loss reported should be interpreted very cautiously without additional information (e.g. standard deviation).

Paoli et al. distinguish four cost components and four types of cybercrime, each related to the most recent incident, to all incidents in total and individually to the most severe attack.[142] For

[136] Cf. Paoli et al. (2018).

[137] See Bollhöfer & Jäger (2018).

[138] Cf. Hillebrand et al. (2017).

[139] Cf. Bitkom e.V. (2018).

[140] Cf. ibid.

[141] See PricewaterhouseCoopers AG WPG (2017).

[142] Cf. Paoli et al. (2018).

the most recent incident of illegal access, internal personnel costs were less than EUR 69 in 44.2 % of cases, hardware and software replacement costs were EUR 0 in 55.6 % of cases and less than EUR 10,000 in 35.8 % of cases, and penalties and compensation payments were EUR 0 in 90.7 % of cases and less than EUR 10,000 in 4 % of cases.[143] In summary, Paoli et al. come to the conclusion that only a minority of the companies surveyed report severe financial damage[144] and that there are differences, especially compared to studies by commercial authors or publishers. According to Klahr et al. [145], it is generally rather unusual for companies to systematically record financial damages from cybersecurity incidents (only about 6 % of the companies surveyed would do so),[146] which could also be a reason for the limited response behaviour of many companies. In the survey of around 1,500 British companies, Klahr et al. conclude that for all incidents of the last 12 months, average costs of GBP 1,570 were incurred across all companies and costs of GBP 19,600 for large companies. In contrast, the median across all companies is GBP 0, which shows that a majority of companies reported no financial losses at all.[147] Vanson Bourne reports significantly higher costs of last year's security breaches for companies with 500 or more employees for the global average. According to this, companies suffered losses of over USD 917,000.[148] However, neither structural differences nor the exact composition of these costs are discussed.

For their 2005 survey, Rantala et al. state that[149] monetary losses were incurred with a median of approx. USD 6,000 across all types of attack or incident and company sizes. Cyber misappropriation/embezzlement (median USD 50,000) and theft of intellectual property (median USD 43,000) weighed particularly heavily, while computer viruses (median USD 5,000) and denial of service attacks (median USD 5,000) caused less financial damage. Around 51 % of companies had to cope with financial losses between USD 1,000 and USD 9,000, with only 13 % reporting losses in excess of USD 100,000. The financial (29 %) and insurance (20 %) sectors in particular reported relatively often that they had suffered financial losses of at least USD 100,000.[150] The composition of these financial losses was not presented.

In its report, the Ponemon Institute points out that the cost of data mismatches[151] can vary between regions and industries. Based on activities following an incident, which are divided into direct, indirect and opportunity costs but unfortunately are not disclosed, the Institute states that in 2017 the average total cost per company was $ 3.62 million. Incidents in US companies are significantly more expensive (USD 7.35 million) than, for example, in Germany (USD 3.68 million) or Brazil (USD 1.52 million). The costs per compromised data set are highest in 2017 in the health (USD 380), finance (USD 245) and services (USD 223) sectors and lowest in the media (USD 119), research (USD 101) and public sector (USD 71).[152] In another report, the

[143] Cf. ibid.

[144] This is also reported by Klahr et al. (2017).

[145] Cf. Paoli et al. (2018).

[146] Cf. Klahr et al. (2017).

[147] Cf. ibid.

[148] See Vanson Bourne (2014).

[149] See Rantala (2008).

[150] Cf. ibid.

[151] Ponemon defines a data breach broadly as an event that could potentially compromise personal information (e.g., medical data, credit card information, etc.) in electronic or non-electronic format.

[152] See Ponemon Institute (2017a).

Ponemon Institute presents the average cost of cybercrime over the past three years per quarter of the number of enterprise seats with network access. According to this report, the 254 companies surveyed incurred high costs in 2017 (Quartile 1 (smallest companies): USD 3.6 million; Q2: USD 5.7 million; Q3: USD 10 million; Q4: USD 16.9 million), which have increased permanently since 2013 with the exception of the fourth quartile. Per enterprise seat with network access, it is shown that the average costs are higher in small companies than in large companies (Q1: USD 1,726; Q2: USD 975; Q3: USD 655; Q4: USD 436).[153] In addition to the limitations of this survey mentioned by the Institute (e.g. no representativeness, sampling frame bias, factors not taken into account, estimated costs/simple extrapolations), the lack of transparency of cost components and calculation steps can also be cited.

The British insurer Hiscox quotes estimated average costs of cybersecurity incidents for German companies over the last 12 months. This shows that larger companies also report higher costs (< 250 employees: USD 55,067; 250 to 999 employees: USD 406,653; > 1,000 employees: USD 640,408). The average cost of the most severe cybersecurity incident of the last 12 months also shows this trend (< 250 employees: USD 11,918; 250 to 999 employees: USD 86,834; > 1,000 employees: USD 150,891).[154] Romanosky takes a different approach to cyber-attack costs and analyses cases from a commercial database of publicly reported cyber incidents, which he distinguishes by four types of attack or incident.[155] On average, phishing incurred the highest internal company costs (USD 20 million; median: USD 0.3 million), followed by Privacy Violations (USD 10.1 million; median: USD 1.3 million), Security Incidents (USD 9.1 million; median: USD 0.35 million) and Data Breaches (USD 5.9 million; median: USD 0.1 million). With the help of regression analyses, he establishes that the size of the company measured in terms of sales and the number of data records affected are significantly related to the amount of losses incurred. Overall, he estimates that the losses average only 0.4 % of annual sales and are thus well behind other threats to the company (e.g. fraud, corruption, theft and bad debts).[156]

Reliable data, especially differentiated according to single cost components of costs caused by cyber-attacks, are difficult to find in the literature. Similar to the reported losses, there is a wide range of reported costs, with the majority of the companies surveyed tending to report no or low costs. Some authors indicate differences between academic and commercial studies, which may also be associated with the aggregation of the data and lead to high calculated costs, especially in the case of linear extrapolations.

2.4.8 Reporting behaviour and cooperation with authorities

The content of this section includes information from the literature on the extent to which companies cooperate with official authorities or report incidents in the event of a cyber-attack and what reasons speak for or against this cooperation. Only 7 out of 32 studies provide information on this.

[153] See Ponemon Institute (2017b).

[154] See Hiscox (2018).

[155] (i) data breaches: unauthorised disclosure of personal data; (ii) security incidents: Malicious attacks on companies; (iii) Privacy Violations: Alleged violation of customer privacy; (iv) Phishing/Skimming: Individual financial crimes.

[156] Cf. Romanosky (2016).

Klahr et al. report from their survey of UK companies that[157] only 26 % of respondents reported the most severe attack of the last 12 months to external parties other than security providers. Of these, most incidents were reported to banks or credit card companies (28 %), the police (19 %) and suppliers (10 %). The main reasons cited for not reporting the incident that had an impact to external parties are the insignificance of the incident (52 %), ignorance of who should have been informed (24 %), no obligation to report (8 %) and no prospects of success (7 %).[158] Bollhöfer et al. also report similarly high reporting rates to the police (22 %), with a focus on industrial espionage and competition spying.[159] The reported reporting rates of the IHK Nord are even lower. Only 13.2 % of the companies surveyed stated that they had reported at least one attack in the last twelve months. Similar to the study by Klahr et al., 22.1 % of the companies surveyed stated that they did not know who to contact, while the high amount of work involved in reporting an attack (54.4 %) and negative prospects of success (30.1 %) were reported much more frequently. In addition, 3.7 % of the companies in each case justified not reporting the matter by citing poor previous experience and a fundamental distrust of investigative authorities.[160]

The Bitkom study addresses very similar questions,[161] but with its focus on business security in industry, comes to contrary results. According to the study, only 2 % of the attacked companies did not report their security incidents to government agencies. 78 % of the companies surveyed have filed a criminal complaint for incidents within the last two years and 29 % made a voluntary report to the authorities. When asked to whom incidents were reported, 90 % of companies reported to the police, 70 % to a public prosecutor's office, 14 % to the Federal Office for Information Security, and only a few to the Office for the Protection of the Constitution (7 %) or data protection supervisory authorities (5 %). The main reasons given by companies for not involving government agencies for the purpose of investigation were fear of damage to their image (38 %), no prospects of success (38 %), too much effort (37 %) and fear of negative consequences for the company (36 %). Nevertheless, it would appear that, in addition to their own investigations (57 %), more use is made of government agencies (38 %) than of external specialists (31 %) when investigating incidents.[162] Another Bitkom survey focusing on business security, but not only for industrial companies, indicates that 31 % of the incidents were investigated by government agencies. Of these, 84 % involved the police, 57 % the public prosecutor's office, 15 % data protection authorities, 15 % the BSI and 3 % the Office for the Protection of the Constitution.[163] In a survey on how affected companies are by ransomware in 2016, the BSI cites a reporting rate of 18 % of the companies affected, although this was only collected for this crime.[164]

PwC and Strategy& surveyed 309 companies in 2016 to find out what form collaboration between government and business could take. According to the survey, the companies surveyed

[157] Cf. Klahr et al. (2017).

[158] Cf. ibid.

[159] See Bollhöfer & Jäger (2018).

[160] Cf. Industrie- und Handelskammer Nord e.V. (2013).

[161] Cf. Bitkom e.V. (2018).

[162] Cf. ibid.

[163] Cf. Bitkom e.V. (2017).

[164] See Bundesamt für Sicherheit in der Informationstechnik (2016).

stated that damage limitation, forensics and recovery tasks are primarily seen as their own responsibility, whereas the implementation of research projects and the setting of standards are seen as government tasks. On the other hand, education, sensitization and threat analysis are seen as a common task.[165]

The reporting rates shown vary depending on the study. What is lacking here is above all research on what kind of attacks are reported by what kind of companies. It is possible that this could explain the different reported reporting rates.

2.4.9 Cyber insurance

In this section, statements from the literature examined on the spread of cyber insurance and reasons for and against the use of cyber insurance in companies are presented. Information on this could only be found in four of 33 studies.

Depending on company size, only a small proportion of the companies surveyed in a survey by the GDV stated that they had taken out cyber insurance (micro companies: 6 %; small: 15 %; medium-sized: 9 %).[166] Some other companies are planning to take out or are interested in cyber insurance (Smallest companies: 15 %; Small: 15 %; Medium: 25 %), whereas the majority of respondents had no insurance or were not interested in it (micro companies: 79 %; Small: 67 %; Medium: 63 %).[167] In a survey Bitkom mentions insurance against digital industrial espionage, sabotage or data theft and states that 14 % of the companies surveyed had such insurance.[168] Here, too, there are differences in company size (10-99 employees: 10 %; 100-499 employees: 23 %; >500 employees: 32 %). Compared to the GDV, fewer companies stated that such insurance is currently not an issue within the company (10-99 employees: 43 %; 100-499 employees: 23 %; >500 employees: 24 %). Only 28 % of the companies surveyed that had at least one incident in the last two years stated that it was more or less worthwhile taking out such insurance. In contrast, smaller companies (10 to 99 employees) reported more worthwhile deployment (48 %) than larger companies (100 to 499 employees: 10 %; >500 employees: 16 %).[169]

Hiscox mentions significantly higher percentages in his report. According to the report, a total of 33 % of the companies surveyed in Germany, Spain, the UK, the Netherlands and the USA stated that they had cyber insurance.[170] A further 25 % are planning to take out insurance in the next 12 months. Here, too, there are significant differences in size. While companies with more than 250 employees have completion rates between 49 % and 62 % depending on the nation, this is only between 20 % and 33 % for companies with less than 250 employees.[171]

Klahr et al. report that contrary to investments in cyber security, the existence of cyber insurance does not correlate positively with revenues.[172] According to the report, companies with revenues of between GBP 2 million and GBP 10 million are most likely to encounter cyber

[165] Cf. PwC Strategy& GmbH (2016).

[166] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[167] Cf. ibid.

[168] Cf. Bitkom e.V. (2018).

[169] Cf. ibid.

[170] Cf. Hiscox (2018).

[171] Cf. ibid.

[172] Cf. Klahr et al. (2017).

insurance (46 %), whereas this proportion is 36 % for companies with lower or higher revenues. Cyber insurances are also more likely to be found in education, health, social services (57 %), finance (53 %) and administration or real estate (52 %). Klahr et al. also asked the companies to what extent they knew which damages were covered by the insurance and which were not. Without significant differences in company size, an average of 59 % of the companies stated that this content was well or very well understood. Conversely, a further 37 % stated that they did not know the scope of insurance at all or not well.[173]

Despite divergent information, it appears that the majority of companies tend to have no insurance against cyber and information security breaches. In addition to the limitations mentioned in Section 2.3, the reasons for the different results can also be different types and scopes of corresponding insurance policies. For example, it would be possible for companies to regard the existence of a comprehensive business interruption insurance policy that also covers certain damages caused by cyber-attacks as the existence of a cyber insurance policy.

2.5 Interim summary

As the excerpt of the state of research presented here shows, the phenomenon of cyber-attacks against companies is very dynamic and versatile. As a result, there is a wide range of literature from different groups of authors whose research shows strong differences in methodological approaches and the respective operationalization. In addition to the limitations mentioned in Section 2.3, which may be the cause of different results, there is a lack of tried and tested standardised instruments for data collection, as is common in many areas of quantitative empirical research. Among other things, this greatly limits the direct comparability of these studies.

In addition to the different and sometimes contradictory information on the topics described above, open questions are stand out which have not been addressed or have been addressed only very rarely. These include, in particular, the differentiated effects of individual attack-types on technology, processes, organisation and employees of companies, the type and amount of costs incurred as a result of cyber-attacks, and, last but not least, risk and protection factors of cyber-attack.

[173] Cf. ibid.

3 SURVEY

In addition to the preparation and presentation of the state of research, nine guideline-based qualitative interviews were conducted with representatives of the law enforcement agencies (Central points of Contact for Cybercrime (ZAC) and specialized public prosecutor's offices), the Office for the Protection of the Constitution, the Federal Office for Information Security and insurers in order to gain access to the research field and to determine the need for research. The detailed description of the methodological procedure as well as the documentation of the results of the qualitative content analysis of these interviews will be published in a separate research report.[174]

A key result of this preparatory work is that the extent and consequences of cyber-attacks against companies can only be assessed very imprecisely by law enforcement authorities. In particular, the number of non-registered crimes suspected to be very large and a perceived low level of willingness to report make it difficult to assess the phenomenon and thus to raise the awareness of companies, the public and politicians. In addition, a large discrepancy between small and medium-sized companies on the one hand and large companies on the other hand is perceived by law enforcement authorities, inasmuch as SMEs often seem to be insufficiently protected due to fewer resources and less awareness of the issue of cyber-attacks.[175]

3.1 Method

The survey method of Computer Assisted Telephone Interviews (CATI) was used to obtain valid information, particularly on the extent of cyber-attacks, the damage caused and appropriate protective measures.

In comparison to postal and online surveys, the main argument in favour of the CATI survey method was that the survey can be carried out in a relatively short time and that the "right" target persons in the companies can be reached more quickly and, if necessary, persuaded to take part in a survey. To this end, professional interviewers called selected companies, promoted participation in the survey and, if they were willing to participate, arranged an appointment with the target person within the company for the survey. During this appointment, software guided the interviewer through the questionnaire so that he or she could concentrate on the answers of the participants and enter them directly in electronic form. A major advantage of the CATI survey is that the data quality can be monitored during the survey. Errors in the questionnaire construction could have been detected and corrected in time. Refusals to participate and cancellations are also registered in good time and can be compensated by follow-up drawings. By means of technical validation rules, unrealistic entries or incorrect sequences of filter questions can be prevented directly at the moment of data collection and, if necessary,

[174] Stiller et al. (2020).

[175] Cf. Stiller et al. (2020).

inquired about. This makes it possible to achieve high data quality, a relatively high participation rate and thus a sufficiently large data set in the time available for the desired analyses.[176]

The survey institute Kantar EMNID was commissioned to carry out the CATI survey of the targeted 5,000 companies following an official Europe-wide invitation to tender. Kantar EMNID is a member of the industry associations BVM (Berufsverband Deutscher Markt- und Sozialforscher e.V.) and ADM (Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.), is committed to the applicable data protection and professional standards and is certified in particular according to the international standard for the field of opinion and social research ISO 20252. Kantar EMNID also holds certifications in the areas of quality management (ISO 9001) and information security management (ISO/IEC 27001). The survey institute has already carried out various surveys on the subject of white-collar crime, cyber security and information security of small and medium-sized companies and is therefore also a suitable partner for the implementation of the project in terms of the subject matter.

The standardized questionnaire for this quantitative survey contained a total of 40 questions, which were divided into four sections. Section A contained a short introduction and questions on the professional function of the interviewee as well as own risk assessments. Subsequently, section B contained about 21 questions on detected cyber-attacks in the last 12 months or all times and more detailed questions on the most severe cyber-attack of the last 12 months. The existence of technical and organizational security measures was surveyed in Section C, and finally, in Section D, several structural characteristics of the participating companies were asked. The questionnaire was developed and subjected to a qualitative pre-test after a review of the state of research, discussions with the project-accompanying company headquarters[177] and with the inclusion of the results of nine expert interviews within the research project. For this purpose, six IT employees of companies of different sizes and from different industries - mainly in the situation of a telephone interview - were asked to answer the questions asked thinking aloud[178], i.e. by expressing difficulties in understanding or considerations for finding an answer, etc. Questions and definitions that were expected to cause difficulties in advance were specifically addressed and questioned by the test leader.[179] On this basis, the questionnaire was revised again and adapted accordingly.[180] A brief description of the questionnaire used can be found in Appendix 2.

Prior to the field phase, training courses were conducted with the 141 interviewers in the CATI studios used in Berlin and Bielefeld together with the survey managers from Kantar EMNID. Also the questionnaire was provided with additional information for the interviewers. In order

[176] Bollhöfer & Jäger (2018) report a response rate of 9.3% for a postal company survey on the subject of industrial espionage. During the four-month survey period, only 583 of the 6284 companies contacted returned a completed questionnaire. Paoli et al. (2018) indicated a response rate of 4.9% for a questionnaire sent by e-mail.

[177] The project-accompanying company roundtable is made up of eight to twelve companies from different sectors in the Hannover region, who regularly discuss the content and results of the research project in order to promote the practical relevance for and transfer of knowledge to the economy.

[178] On the method of the "Think-Aloud" see e.g. Blanke et al. (2011: 644) or Willis (2005).

[179] For the method of "probing" see e.g. Prüfer & Rexroth (2005).

[180] In addition to the adaptation of wording, additional possible answers to questions B18 on the reasons for not reporting ("Did not know who to contact for this") and D08 on the online presence of sensitive data ("partially") were added, and two additional questions (B03: Probability assessment of an undetected cyber-attack; C02: Type of firewall used) were included.

to increase the willingness of the contacted companies to participate, an official letter of motivation from the German Federal Ministry for Economic Affairs and Energy was used during the contact phase and the later sending of the results report was offered.

The field phase took place between August 2018 and January 2019.

3.2 Investigation Unit

Studies on organizations as a unit of investigation "sometimes have special requirements in terms of survey methodology and differ significantly from surveys of individuals"[181], as usually only one representative of the organization is interviewed. Apart from the problem of accessibility within the organisation, the selection of an appropriate representative is of decisive importance.

As already explained in section 1.1.2, legally independent companies form the investigation unit. In the case of companies with several establishments[182] within a legally independent unit, only the head office was surveyed in each case.[183] Employees responsible for IT and information security were defined as preferred target persons. If there was no such specific position in the surveyed company, the person in whose area of responsibility the topic of IT & information security within the company fell was interviewed. Depending on the size of the company, this occurred more or less frequently.[184]

3.2.1 Basic Population

Accordingly, the basic population consisted of all companies, i.e. legally independent units (e.g. AG, GmbH, GbR etc.), which had their registered office in Germany and more than nine employees subject to social insurance contributions during the period covered by the survey.[185]

The size and composition of this population can be estimated using the Business Register System (URS) of the Federal Statistical Office, which contains all companies that contribute to the gross domestic product, are based in Germany and belong to the economic sectors (according to the WZ 2008 classification) of Sections B to N or P to S.[186]

Alternatively, the "Statistics for small and medium-sized companies" of the Federal Statistical Office provides an estimate of the population for all companies based in Germany that are not classified as financial and insurance activities (WZ08-K). As in the URS, a distinction is made between employee size classes *0 to 9*, *10 to 49*, *50 to 249* and *250 and more employees subject*

[181] Hartmann (2017: 186).

[182] "An establishment is a place of business at a given location, including locally and organisationally attached units" (Statistisches Bundesamt 2018: 5).

[183] Hartmann (2017: 189).

[184] See section 3.4.3.

[185] Micro-companies with up to nine employees were excluded from this survey, as their inclusion would have exceeded the time and financial framework of the planned survey. A major reason for this is that this large group is subject to relatively strong changes, e.g. more frequent business registrations and deregistrations or start-ups and insolvencies (cf. Statistisches Bundesamt (2019a, 2019b)), and as a result the availability and timeliness of telephone contact information in the company databases used is very limited.

[186] Source: Federal Statistical Office, Wiesbaden 2015 (https://www-genesis.destatis.de).

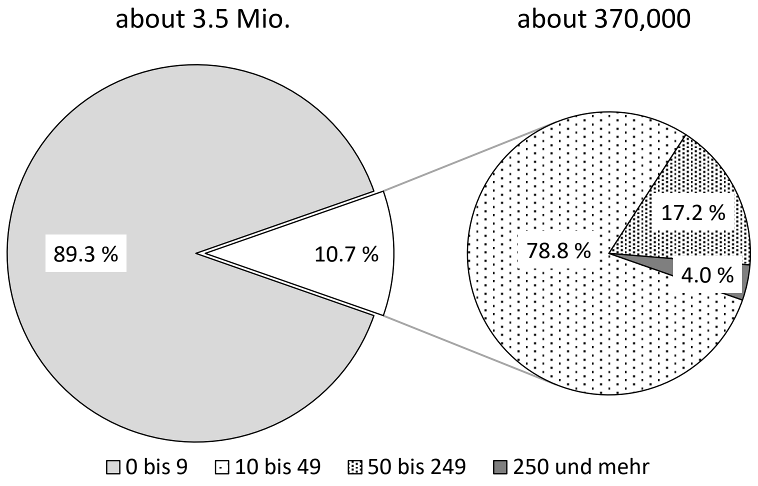
to social insurance contributions (SVB). However, a comparison with the URS is not meaningful, as other definitions and the methods of data collection differ.[187]

Both statistics therefore offer only a rough categorisation of employee size classes and do not provide a comprehensive picture of all German companies with regard to the WZ classes[188]. Since the available data from the URS are more up-to-date and, with regard to the WZ classes, contain the larger intersection with the companies examined, they were used to estimate the population.

According to URS data (as of 2017), only 10.7 % (372,599) of all companies (3,481,860) have more than nine employees and thus belong to the survey population. Of these, companies with between ten and 49 employees have the largest share (78.8 %), followed by companies with between 50 and 249 employees (17.2 %) and large companies with 250 or more employees (4.0 %).

Figure 3 **Shares of companies by employee size class**

Source: URS, Federal Statistical Office, 2017; own illustration



Although this population represents only 10.7 % of the companies in Germany, the companies included in the survey represent approximately 81.5 % of the employees in Germany.[189]

[187] Source: Federal Statistical Office, Wiesbaden 2018 (https://www-genesis.destatis.de).

[188] No companies in sector WZ08-A: Agriculture, Forestry and Fishing.

[189] In 2017, companies in the sectors WZ08-B to N (except K) employed around 29.7 million people (micro companies: 5.5 million; small companies: 6.9 million; medium-sized companies: 5.7 million; large companies: 11.6 million). However, companies in the WZ classes A, K, O, P, Q, R, S are not included in these statistics, but are included in the population of this study. Depending on the distribution of companies in these WZ classes among the employee size classes, the 81.5% share of employees represented by the companies in the population may increase or decrease. Source: Statista.com (https://de.statista.com/statistik/daten/studie/731962/umfrage/beschaeftigte-in-unternehmen-in-deutschland-nach-unternehmensgroesse/

Table 1 **Companies in Germany by employee size class and economic activity from 10 employees upwards**

WZ 2008; Source: URS, Federal Statistical Office, 2017

		Size classes of persons employed							
		10 to 49		50 to 249		250 and more		total	
WZ08 (sections): URS, 2017		Quantity	Percent	Quantity	Percent	Quantity	Percent	Quantity	Percent
B	Mining and Quarrying	487	0.2	113	0.2	18	0.1	618	0.2
C	Manufacturing	43,540	14.8	15,845	24.8	4,340	28.8	63,725	17.1
D	Electricity, Gas, Steam and Air Conditioning Supply	692	0.2	518	0.8	194	1.3	1,404	0.4
E	Water Supply; Sewerage, Waste Management and Remediation Activities	2,517	0.9	829	1.3	157	1.0	3,503	0.9
F	Construction	37,002	12.6	3,397	5.3	280	1.9	40,679	10.9
G	Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles	54,140	18.4	9,582	15.0	1,781	11.8	65,503	17.6
H	Transportation and Storage	17,020	5.8	3,867	6.0	693	4.6	21,580	5.8
I	Accommodation and Food Service Activities	17,493	6.0	2,123	3.3	213	1.4	19,829	5.3
J	Information and Communication	10,352	3.5	2,812	4.4	523	3.5	13,687	3.7
K	Financial and Insurance Activities	2,023	0.7	1,132	1.8	777	5.2	3,932	1.1
L	Real Estate Activities	3,722	1.3	510	0.8	64	0.4	4,296	1.2
M	Professional, Scientific and Technical Activities	28,041	9.6	4,037	6.3	703	4.7	32,781	8.8
N	Administrative and Support Service Activities	16,552	5.6	5,617	8.8	1,553	10.3	23,722	6.4
P	Education	11,360	3.9	2,022	3.2	441	2.9	13,823	3.7
Q	Human Health and Social Work Activities	33,533	11.4	8,868	13.9	2,855	19.0	45,256	12.1
R	Arts, Entertainment and Recreation	3,979	1.4	601	0.9	126	0.8	4,706	1.3
S	Other Service Activities	11,157	3.8	2,055	3.2	343	2.3	13,555	3.6
		293,610	100.0	63,928	100.0	15,061	100.0	372,599	100.0

3.2.2 Selected Population

Even if the excluded micro companies (zero to nine employees)[190], the largest share of all companies resident in Germany, is not taken into account, a complete survey of the included small, medium-sized and large companies is not possible from a research-economic point of view due to their still large population. As an alternative, only a randomly selected subset of the population is to be examined, which approximates this. In addition to official business registers, commercial company databases[191] can be considered as a basis for the sampling (sample population). These have the great advantage that, in addition to the address of the companies, contact persons and contact details are also available, which greatly facilitates telephone surveys. In addition, the sample can be drawn without much effort and much faster than official sources. The disadvantage of such commercial databases is that they are usually not complete. The companies that are not included therefore have no chance of being included in the sample (undercoverage) and the selection population is therefore only a more or less good approximation of

[190] See footnote 184.

[191] Cf. Hartmann (2017: 193).

the population,[192] where attention must be paid to where the company information comes from and whether the data sets have been obtained selectively.[193]

The databases of the providers Bisnode (formerly Hoppenstedt) and Heins & Partner used by the survey institute Kantar EMNID for sampling purposes contain, according to telephone information, almost all companies based in Germany and are updated daily. Nevertheless, the contact data (especially telephone numbers) required for the CATI survey are not available in both databases without gaps. Since Bisnode's database, in line with its business orientation, mainly contains contact information of companies in the two largest employee size classes and Heins & Partner's database mainly contains information of medium and small companies, it was possible to share a database that "adequately covers all facets of the quota structure".[194] An automated duplicate check prevented companies from being surveyed more than once. Against this background and with the exclusion of the most volatile and thus most incomplete group of micro companies with less than ten employees, a good approximation to the population can be assumed.

3.3 Sampling and realization

As can be seen in the Figure 3 and Table 1, the distribution is very skewed in terms of the size classes of employment and the economic activity. The sub-populations that are rarely present in the population (e.g. large companies with 500 employees or more) would therefore hardly be represented in the sample if a simple random selection were made, because of their correspondingly lower selection probability.

Table 2 **Stratification plan of the disproportionately stratified sample**

	Target figure	Sector distribution
10-49 employees	1,000	proportional to the total selection; WZ08-A to S (without WZ08-O,T,U)
50-99 employees	1,000	
100-249 employees	1,000	
250-499 employees	1,000	Best-Effort-Basis; WZ08-A to S (without WZ08-O,T,U)
500+ employees	500	
Companies of general interest	500	Branch and size distribution on a best-effort basis[195]
Total	5,000	

[192] Schnell & Noack (2015: 9f.) This circumstance is problematic from an inferential statistical point of view, since, strictly speaking, the probability of selection can no longer be calculated and there is no "true" random selection (cf. Hartmann 2017: 194).

[193] Snijkers & Meyermann (2017: 252). See also Smith (2013).

[194] Kantar Emnid (2019: 3).

[195] In the area of the economic provision of services, the following sectors are included in the canon of services of general interest: electricity supply, gas supply, commercial waste disposal / recycling management, health (hospitals, outpatient care, pre- and post-operative care, nursing care), postal services, traffic and transport (railways, roads, waterways, air transport), money and credit supply (with a binding mandate to the savings banks to provide services), telecommunications/internet and housing (cf. Schäfer 2018). The WZ08 classes assigned to the companies of general interest are shown in Annex 1 in table 43.

In order to obtain sufficient information from the survey for such groups, a disproportionately stratified net sample according to a predetermined stratification plan (Table 2) was aimed at with regard to the employee size classes.[196]

In order to carry out 5,000 interviews according to this stratification plan (net sample) 43,219 companies were contacted (gross sample; Table 3). This corresponds to a participation rate of 11.6 %.[197]

Table 3 **Utilisation**

		Quantity	Percent
failure after contact with Company	No target person in the company	6,160	14.3
	no interest in the subject	7,156	16.6
	Refusal on behalf of the target person	3,634	8.4
	Refusal without giving reasons	14,582	33.7
	other reason (e.g. language problems, data protection)	101	0.2
Failure in contact with Target person	Refusal for reasons of time	1,006	2.3
	no interest in the subject	2,136	4.9
	Refusal without giving reasons	3,266	7.6
	Interrupting the interview	165	0.4
	other reason (e.g. language problems, data protection)	13	0.0
	Net sample	5,000	11.6
	Gross sample	43,219	100.0

The gross sample was drawn at random within the individual stratification cells, which were based on employee size class and industry affiliation (WZ08 class), taking into account the ADM lock file.[198] A further characteristic that was taken into account in the stratification is the affiliation of the companies to the area of companies of general interest.[199]

Regarding the loss of participation, two contact phases can be distinguished: The largest proportion of dropouts occurred in the first phase, in which the companies were contacted for the first time in order to present the background of the survey, identify suitable target persons within the companies and ask for their contact information. About one third of the companies were not willing to participate in this phase without giving reasons (33.7 %), another 16.6 % were not interested in the survey topic, in 14.3 % no target person could be identified within the company and in 8.4 % participation was refused on behalf of the target person.

In the second phase, in which the previously determined target persons were contacted by the interviewers and asked to participate in the survey using the accompanying letter from the Federal Ministry for Economic Affairs and Energy, 7.6 % dropped out without giving reasons,

[196] The economic activity classes WZ08-T (Activities of Households as Employers; Undifferentiated Goods and Services Producing Activities of Households for Own Use) and WZ08-U (Activities of Extraterritorial Organisations and Bodies) were not included because these are not private sector companies and they cannot be classified as services of general interest.

[197] Only a few studies report transparently on participation and response rates: Examples are Paoli et al. (2018) (4.9 %); Computer Security Institute (2011) (6.4 %); Rantala (2008) (23 %).

[198] The blocking file of the Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. (ADM) contains companies that are generally not available for social science surveys.

[199] See footnote 194.

4.9 % had no interest in the topic and 2.3 % did not participate in the survey due to time constraints. A proportion of 0.4 % dropped out of the interview. Other reasons (e.g. language problems or data protection reasons) played a subordinate role in both contact phases (0.2 % and 0.03 % respectively).

3.4 Sample description

In the presentation of the sample distribution and subsequently the survey results, the percentages given refer to the valid cases, i.e. excluding the cases with missing information. Since the number of these valid cases (N) can vary, it is also shown. Should the number of missing cases be conspicuously high, this will be pointed out separately at the appropriate place.

Especially for the later comparison of the results between certain groups of companies, the 95 % confidence intervals (95 % CI) are sometimes[200] shown in the diagrams with the help of so-called error bars starting from the end of the columns or from the points.[201] If the confidence intervals of two values do not overlap, a significant difference can be assumed with a five percent probability of error. An overlap, on the other hand, indicates that the difference may have been accidental. In addition, significance tests (Chi² tests) are carried out for all other group comparisons and any significant differences are shown in bold.[202]

Due to the disproportionate stratification of the sample, the probability of selection has changed, especially large companies and companies of general interest are more strongly represented in the net sample than in the basic and selection population (oversampling). Thus, meaningful statements can also be made about these groups.

For statements on all companies, i.e. across all employee size classes and branches, the sample is reproportionalised with a subsequent weighting so that the sample is distributed according to the selection population and thus approximately to the population and there are no longer any indications of distortion with regard to these company characteristics.

3.4.1 Employee classes

Table 4 shows the sample distribution in terms of the size classes of persons employed. While the proportions of companies in the individual employee size classes (with the exception of companies with 500 or more employees subject to social insurance contributions) are approximately the same in the unweighted sample, their proportions in the weighted sample correspond to those in the sample population. For example, companies with 10 to 49 employees as well as companies with 50 to 99 employees have a share of around 24 % in the unweighted sample and 79.1 % and 10.5 % respectively in the weighted sample. In the evaluations across all companies

[200] The confidence interval is a range of values (expectation range) that belongs with a certain probability (here 95 %) to the ranges of values that contain the true value of a parameter of the selection population. This is a conservative estimate, i.e. compared to other significance tests, it is more likely to conclude that there is no correlation under the same conditions.

[201] The range of values thus covered may vary; for example, the smaller the number of valid data on which the estimate of the true unit value of the selection population is based, the wider the range will be.

[202] The underlying significance level is again at least 95 %, i.e. there is still a residual probability of at most 5 % ($p < .05$) that there is no difference between the comparison groups in the selection population and that the observed difference in the investigated sample was random.

in all employee size classes, small companies thus receive a higher weight and larger companies a lower weight.

Table 4 **Sample by size class of employment and companies of general interest**

		disproportionate sample		
		unweighted		weighted
Size classes of persons employed		Quantity	Percent	Percent
	10-49 employees	1,190	23.8	79.1
	50-99 employees	1,181	23.6	10.5
	100-249 employees	1,120	22.4	6.5
	250-499 employees	1,005	20.1	2.2
	500+ employees	504	10.1	1.8
	Total	5,000	100.0	100.0
Companies of general interest				
	yes	847	16.9	11.2
	no	4,153	83.1	88.8
	Total	5,000	100.0	100.0

Companies of general interest are slightly over-represented in the unweighted sample (16.9 %) in terms of their share in the total sample and are therefore weighted down to 11.2 %.

3.4.2 Sector

The classification of the economic sectors of the companies is already included in the company database used for sampling up to the second breakdown level in the form of the 2008 Classification of Economic Activities of the Federal Statistical Office (WZ 2008)[203] and did not have to be collected separately. The classification at the first level of breakdown (WZ08-A to S) serves as a further characteristic used to weight the data set, i.e. the sector distribution is weighted for each employee size class on the basis of the respective sector distribution within the sample population.

Table 5 shows the distribution of the 19 WZ classes (level 1) across all companies in the unweighted and weighted sample. Larger differences can be seen in particular in manufacturing (WZ08-C), construction (WZ08-F) and wholesale and retail trade; repair of motor vehicles and motorcycles (WZ08-G). These are mainly due to differences between the employee size classes. For example, the share of manufacturing companies in the group of small companies (10-49 persons employed), at 18.8 %, is significantly smaller than for the larger ones (50-99 persons employed: 26.0 %; 200-249 persons employed: 30.1 %; 250-499 persons employed: 30.1 %; 500 persons employed and over: 26.4 %). Since small companies receive a higher weight in evaluations of the total data set, the share of WZ08-C companies is reduced in this case from 26.6 % in the unweighted sample to 20.7 % in the weighted sample. Similarly, but exactly the opposite is true for the shares of WZ08-F and WZ08-G companies, which occur significantly more frequently in the group of small companies (10-49 employees) than in the larger ones.

[203] See Statistisches Bundesamt (2008).

Therefore, larger shares can be seen in the weighted sample compared to the unweighted sample.

Table 5 **Sample by industry (WZ 2008)**

	disproportionate sample		
	unweighted		weighted
Industry (WZ08)	Quantity	Percent	Percent
Agriculture, forestry and fishing (A)	39	0.8	1.4
Mining and Quarrying (B)	17	0.3	0.3
Manufacturing (C)	1,328	26.6	20.7
Electricity, Gas, Steam and Air Conditioning Supply (D)	68	1.4	0.5
Water Supply; Sewerage, Waste Management and Remediation Activities (E)	89	1.8	0.9
Construction (F)	310	6.2	12.9
Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles (G)	607	12.1	18.0
Transportation and Storage (H)	329	6.6	4.7
Accommodation and Food Service Activities (I)	130	2.6	4.2
Information and Communication (J)	152	3.0	3.1
Financial and Insurance Activities (K)	209	4.2	2.1
Real Estate Activities (L)	105	2.1	1.6
Professional, Scientific and Technical Activities (M)	434	8.7	9.1
Administrative and Support Service Activities (N)	235	4.7	4.3
Public Administration and Defence; Compulsory Social Security (O)	19	0.4	0.4
Education (P)	274	5.5	6.4
Human Health and Social Work Activities (Q)	436	8.7	5.8
Arts, Entertainment and Recreation (R)	64	1.3	1.2
Other Service Activities (S)	155	3.1	2.5
Total	5,000	100.0	100.0

The classification of the companies on the second level of the Classification of Economic Coding is used for a more detailed presentation, especially in case of conspicuous variances. The distribution and allocation of the second to the first level can be found in the appendix of the Table 44

3.4.3 Position of the interviewees within the company

As already described under 3.1, one difficulty with company surveys is the selection of a company representative to provide information about the company. The preferred target person was an employee responsible for IT & information security. In those cases where such a specific position does not exist, for example because this area is outsourced to external service providers or is taken over by employees from other areas, a representative was asked to participate in the survey, in whose area of responsibility the topic of IT & information security falls. Since the respondents' field of activity may have an impact on their response behaviour, the position within the company was asked and is included as a control variable, especially in multivariate analyses.

Table 6 **Sample by position of respondents**

multiple answers possible

	unweighted		weighted				
			Percentages according to employee size classes				
Position	Quantity	Percent	10-49	50-99	100-249	250-499	500+
IT & Information Security	3,484	69.8	38.8	67.3	78.6	86.7	91.9
Management, Board of Directors	1,171	23.5	51.3	25.8	14.9	8.1	4.4
Data protection	342	6.8	8.7	8.0	5.6	5.9	5.0
Revision, testing	104	2.1	2.8	2.9	1.9	1.4	0.4
Plant safety	56	1.1	1.9	1.4	0.7	0.8	0.2
Miscellaneous[204]	402	8.1	12.8	9.6	6.9	5.5	4.2

Table 6 shows that the majority of the surveyed representatives work in the field of IT & information security (69.8 %), but as expected there are relevant differences between the companies of the different employee size classes. While almost all respondents in companies with 500 or more employees stated that they worked in this area (91.9 %), only 38.8 % of respondents in companies with between 10 and 49 employees said they worked in this area. Respondents from the area of management & board of directors are correspondingly more strongly represented in small companies.

For further evaluation (especially in chapter 6), multiple answers were resolved and the items were summarized as follows: Respondents who indicated "management, board of directors" and another position were only assigned to the management. Respondents who stated "IT & Information Security" and one further position with the exception of "Management, Board of Directors" were assigned exclusively to "IT & Information Security". All others were summarized in the category "other position" (Table 7).

Table 7 **Sample according to summarised positions of the interviewees**

	unweighted		weighted				
			Percentages according to employee size classes				
Position	Quantity	Percent	10-49	50-99	100-249	250-499	500+
IT & Information Security	3,345	67.0	34.0	63.4	76.7	85.2	91.1
Management	1,171	23.5	51.3	25.8	14.9	8.1	4.4
Other position	477	9.6	14.7	10.8	8.4	6.8	4.6
Total	4,993	100.0	100.0	100.0	100.0	100.0	100.0

3.5 Limitations and strengths

In summary, the methodological limitations and strengths of this study, some of which have already been pointed out in the previous sections, are described below. This compilation should enable the reader to interpret the statements of the study more appropriately, also in comparison to other studies, and ultimately to make better-informed decisions.

[204] These include in particular the areas of finance and accounting, management, purchasing and sales, as well as operations and technology.

Sampling was carried out from a selection population (company databases) and not directly from the population. Even if the sample largely corresponds to the population in terms of the distribution of all controlled characteristics and there are no indications of systematic bias, this means that there is still an uncertainty regarding the coverage problem, insofar as companies not included in the sample had no chance of being included. Although the object of investigation "company" is an organization and not an individual, such company surveys are limited to the fact that only one person can be interviewed as a representative of the company. Besides the problem of selecting suitable representatives, their answers always reflect the respective level of knowledge as well as personal motivations and attitudes (so-called self-reporting bias). In addition, the questions about cyber-attacks were asked retrospectively, which can be associated with corresponding distortions, e.g. if the events in question are not remembered at all or in reality are longer ago than in the memory of the interviewees. Of course, respondents can also only provide information about events that they themselves are aware of. Cyber-attacks unnoticed by the organisation or the respondent, the absolute number of non-registered crimes, cannot be investigated by these forms of study. In addition to ignorance and difficulties in understanding, so-called social desirability can also lead to respondents giving information that does not correspond to reality. In order to control social desirability at least to some extent, the response behaviour of different groups of respondents is compared here (e.g. whether managing directors answer the question about the assessment of the working atmosphere differently than IT employees). With regard to the survey phase of several months, it is also possible that disruptive events, e.g. media reporting on a new wave of cyber-attacks such as emotet, had an influence on the response behaviour. For example, the proportion of companies that rated the risk of cyber-attacks as (rather) high might have been overestimated. A further limitation is that, for pragmatic research reasons, it was only possible to inquire about the existence of certain characteristics and measures and therefore no statements can be made about qualitative differences. Complex question constructs and technically detailed answer possibilities are only applicable to a limited extent by the CATI method.

Compared to many other studies in which the methodological procedure and the significance of the results are not reported and reflected at all or only superficially and which partly resort to arbitrary samples, the transparently documented drawing of a stratified random sample is one of the strengths of this study. Taking into account the limitations mentioned above, conclusions can be drawn on the basis of the weighted data about the selection population[205] and, assuming that this comes very close to the population, also about the population[206], which is almost impossible, for example, with arbitrary samples. The comparatively large net sample of 5,000 companies also makes it possible to present results and correlations in a more differentiated manner than in many studies with a smaller sample size. In addition, the use of WZ08 classes for assigning the sectoral affiliation of the companies allows comparability with other official business statistics and also the international applicability of the results for specific sectors. Furthermore, the collection of numerous structural company characteristics and IT security measures allows the analysis and presentation of correlations with the impact of cyber-attacks.

[205] Companies in Germany with more than ten employees that are included in the Bisnode and Heins & Partner company databases.

[206] Companies in Germany with more than ten employees.

4 COMPANY CHARACTERISTICS

In addition to the employee size class and sector affiliation already described, there are other company characteristics which also help to describe the sample, but which are sometimes also brought into connection with the extent to which cyber-attacks affect the company at a later stage as risk or protection factors.

4.1 Federal state

The state in which the company is located was not included in the stratification of the sampling. A comparison of the regional distribution of the surveyed companies in the weighted sample with the regional distribution in the population (Table 8) shows that they are very similar and therefore there is no indication of systematic distortion in this respect.[207] The greatest differences are found in shares in Bavaria, North Rhine-Westphalia, Saxony and Hesse, in that Bavarian and Saxon companies are slightly overrepresented in the weighted data set and companies from North Rhine-Westphalia and Hesse are slightly underrepresented.

Table 8 **Sample by federal state**

	URS*		disproportionate sample		
	WZ08 (B-N, P-S)		unweighted		weighted
Location	Quantity	Percent	Quantity	Percent	Percent
Schleswig-Holstein	12,766	3.5	169	3.4	4.0
Hamburg	10,735	2.9	140	2.8	2.7
Lower Saxony	34,792	9.5	565	11.3	11.0
Bremen	3,625	1.0	46	0.9	0.4
North Rhine-Westphalia	77,133	21.2	950	19.0	19.0
Hesse	27,588	7.6	304	6.1	5.8
Rhineland Palatinate	16,393	4.5	196	3.9	4.4
Baden-Württemberg	49,458	13.6	712	14.2	12.6
Bavaria	60,935	16.7	930	18.6	19.3
Saarland	3,920	1.1	59	1.2	1.1
Berlin	16,052	4.4	138	2.8	3.5
Brandenburg	9,465	2.6	144	2.9	2.6
Mecklenburg Western Pomerania	6,690	1.8	103	2.1	2.1
Saxony	17,147	4.7	270	5.4	6.5
Saxony-Anhalt	8,852	2.4	124	2.5	2.7
Thuringia	8,907	2.4	150	3.0	2.4
Total	364,458	100.0	5,000	100.0	100.0

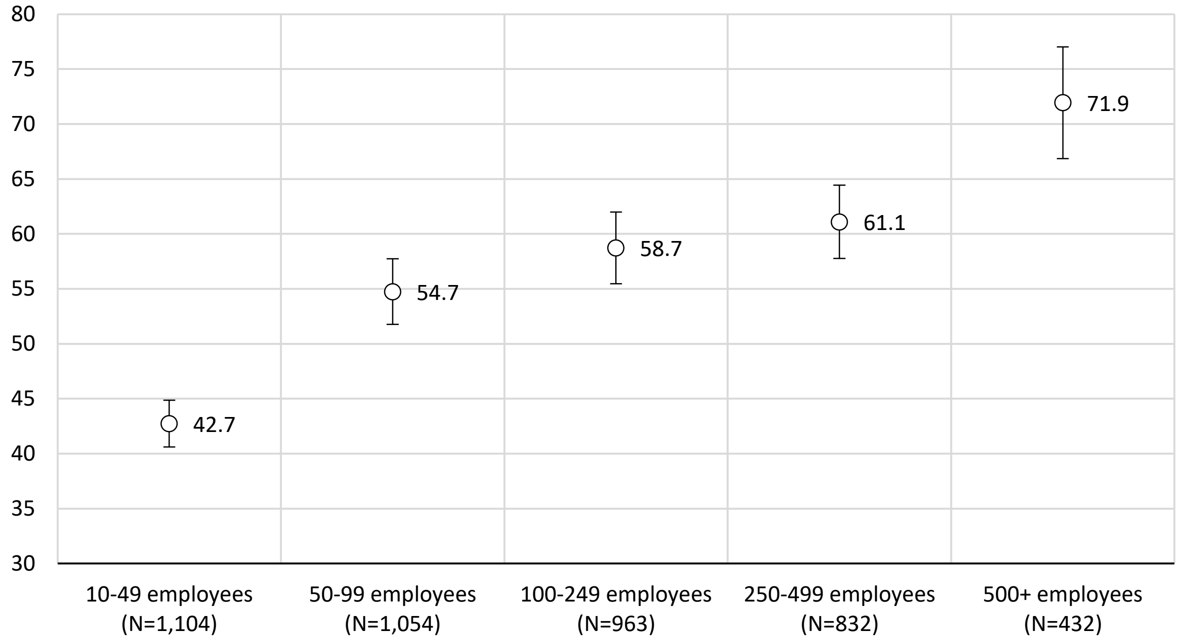
*) Source: Federal Statistical Office, 2017

[207] To limit the comparison, it should be mentioned that no companies from WZ08-A (Agriculture, Forestry and Fishing) and WZ08-O (Public Administration and Defence; Compulsory Social Security) were included in the URS data.

4.2 Company age

The age of the company was calculated on the basis of the concrete data on the year of foundation and is 56 years on average and 39 years on the median[208] (N=4,371). There are significant differences between the various employee size classes (Figure 4) in that larger companies are on average older than smaller ones.

Figure 4 **Average company age by employee size class**
in years, weighted data, 95 %-CI



Interviewed representatives of companies that could not give the exact year of establishment (11.2 %) were asked to estimate the age of the company using a given scale.

Figure 5 **Share of companies by age group**
in percent; weighted data

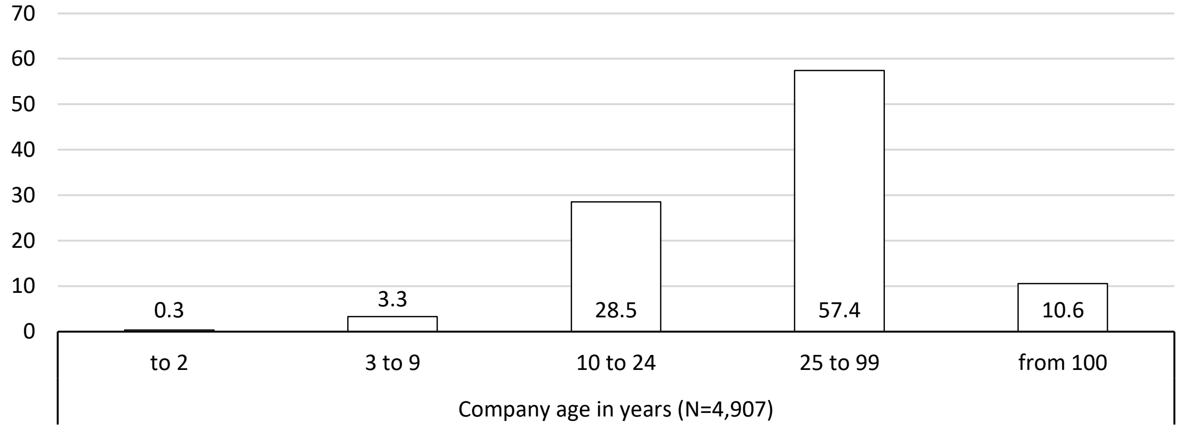


Figure 5 summarises and classifies the estimated data and the data calculated on the basis of the year of foundation. The class of 25 to 99-year-old companies is most strongly represented

[208] This means that half of the companies surveyed are under 39 years old and the other half are over 39 years old.

(57.4 %) followed by the class of 10 to 24-year-old companies (28.5 %). Young companies under 10 years of age have only a very small proportion within the sample.[209]

4.3 Legal form

The legal form of the participating companies could be found in the company databases and therefore did not have to be inquired (Table 9).

Table 9 **Interviewed companies by legal form**

	disproportionate sample		
	unweighted		weighted
Legal form	Quantity	Percent	Percent
Limited liability company	2,925	60.9	64.5
Limited liability company & Co. limited partnership	827	17.2	13.6
Registered businessman/businesswoman	124	2.6	5.2
Public limited company	139	2.9	1.9
Cooperative	177	3.7	4.7
Corporation/public law institution	224	4.7	1.9
Limited partnership	48	1.0	0.7
General partnership	31	0.6	1.4
Registered association	224	4.7	5.0
Partnership company	28	0.6	0.7
Foundation	27	0.6	0.3
Total	4,805	100.0	100.0

The legal form most frequently encountered in the sample (64.5 %) is the limited liability company (GmbH), followed by the limited liability & Co. limited partnership (GmbH & Co. KG; 13.6 %).

Table 10 **Distribution of companies by legal form**

	URS[210]		disproportionate sample		
	WZ08 (B-N, P-S)		unweighted		weighted
Legal form	Quantity	Percent	Quantity	Percent	Percent
Sole proprietors	66,310	17.8	124	2.6	5.2
Partnerships (for example OHG, KG)	69,916	18.8	940	19.6	16.5
Corporations (GmbH, AG)	200,328	53.8	3,076	64.0	66.3
Other legal forms	36,045	9.7	665	13.8	12.0
Total	372,599	100.0	4,805	100.0	100.0

[209] Since the sample was drawn on the basis of a company database, it is conceivable that very young companies in particular have not yet been included in this database and are therefore possibly underrepresented.

[210] Source: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Unternehmensregister/Tabellen/unternehmen-rechtsformen-wzbefragunhtml (last checked on 06.05.2019).

In comparison with the distribution of companies with ten or more employees according to legal form in the Federal Statistical Office's business register system (Table 10[211]), it is striking that individual entrepreneurs in particular are underrepresented in the sample and that corporations are overrepresented.

4.4 Annual turnover

The annual turnover of the companies was partly taken from the underlying company database and partly requested.[212] Companies with an annual turnover of one to less than EUR 2 million (25.0 %) and two to less than EUR 10 million (40.3 %) are most strongly represented in the weighted data set (Table 11).[213]

Table 11 **Interviewed companies by annual turnover**

	disproportionate sample		
	unweighted		weighted
Turnover size class	Quantity	Percent	Percent
Less than EUR 500,000	111	2.4	5.6
500,000 to less than EUR 1 million	194	4.3	12.1
1 to under EUR 2 million	384	8.4	25.0
2 to under EUR 10 million	1,268	27.9	40.3
10 to less than EUR 50 million	1,533	33.7	12.5
50 to less than EUR 500 million	978	21.5	4.1
EUR 500 million and more	83	1.8	0.3
Total	4,551	100.0	100.0

As the business register system only provides information on turnover size classes across all companies, the distribution in the sample of companies with 10 persons employed or more cannot be compared with a corresponding distribution in the population. Against the background of the bias in the legal forms, according to which sole proprietors are less represented in the weighted sample than in the population, it can be assumed that companies in the lower turnover size classes are also underrepresented.

Together with the employee size class, the surveyed companies can be divided into small, medium-sized and large companies according to the SME definition of the Institut für Mittelstandforschung (IfM) Bonn of 01.01.2016. According to this definition, companies with up to 49 employees and a turnover of up to 10 million EUR/year are classified as small[214] and up to 499

[211] The legal forms represented in the sample were summarized as follows: sole proprietors (e. Kfm, e. Kfr), partnerships (GmbH & Co. KG, KG, OHG, AG & Co. KG, GbR, GmbH & Co OGH, PartG), corporations (GmbH, AG, Europa-AG, KGaA, Ltd.) and other legal forms (Gen., AdöR, KdöR, Stiftung, Eigenbetrieb, e.V., VVaG). The comparison is only possible to a limited extent (see footnote 206).

[212] Especially if data was missing in the company database ("How high was the total turnover of your company in the last financial year?").

[213] With a share of 9.0% of the companies, no information on annual turnover was available in the company database, nor was any information provided in the survey.

[214] Micro companies (up to nine employees and an annual turnover of EUR 2 million) are not included in this figure.

employees and 50 million EUR annual turnover as medium-sized companies.[215] Companies with 500 or more employees are therefore classified as large companies.

Table 12 **Surveyed companies by SME affiliation**

	disproportionate sample		
	unweighted		weighted
	Quantity	Percent	Percent
Micro companies (up to 9 employees and up to EUR 2 million annual turnover)	0	0.0	0.0
Small companies (up to 49 employees and up to EUR 10 million annual turnover)*	1,103	22.1	74.4
Medium-sized companies (up to 499 employees and up to EUR 50 million annual turnover)**	2,749	55.0	21.0
Large companies (500 or more employees)	1,148	23.0	4.6
Total	5,000	100.0	100.0

*) and not a micro company
**) and not a micro or small company

In the weighted sample, about three quarters of the companies (74.4 %) are small, just over a fifth (21.0 %) are medium-sized and 4.6 % are large (Table 12).[216]

4.5 Number of locations

The participating company representatives were asked how many locations their company has with its own IT infrastructure in Germany and abroad. A share of 71.5 % of the surveyed companies have only one location in Germany in the weighted data set (Table 13). A further quarter (26.0 %) has between two and nine sites in Germany. With regard to sites abroad, the picture is even clearer: 93.4 % stated that they do not operate any sites with its own IT infrastructure abroad, while 6.6 % reported at least one site abroad.

[215] Source: https://www.ifm-bonn.org/definitionen/kmu-definition-des-ifm-bonn/ (accessed on 07.06.2019). The European Commission uses a definition of SMEs that differs in terms of the size class of employees: only those with up to 249 employees and annual turnover of EUR 50 million or annual balance sheet total of EUR 43 million are counted as medium-sized companies (source: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition/ (accessed on 7th June 2019)).

[216] Companies for which information on annual turnover was missing were allocated solely on the basis of the size class of employment.

Table 13 **Interviewed companies according to the number of sites at home and abroad**

		disproportionate sample		
		unweighted		weighted
Number of sites with own IT infrastructure		Quantity	Percent	Percent
in Germany	1	2,826	57.6	71.5
	2 to 9	1,735	35.4	26.0
	10 to 24	203	4.1	1.4
	25 to 99	113	2.3	0.9
	100+	26	0.5	0.1
	Total	4,903	100.0	100.0
abroad	0	4,199	85.7	93.4
	1	255	5.2	3.7
	2 to 9	318	6.5	2.3
	10 to 24	60	1.2	0.2
	25 to 99	41	0.8	0.2
	100+	25	0.5	0.2
	Total	4,898	100.0	100.0

4.6 Export activity

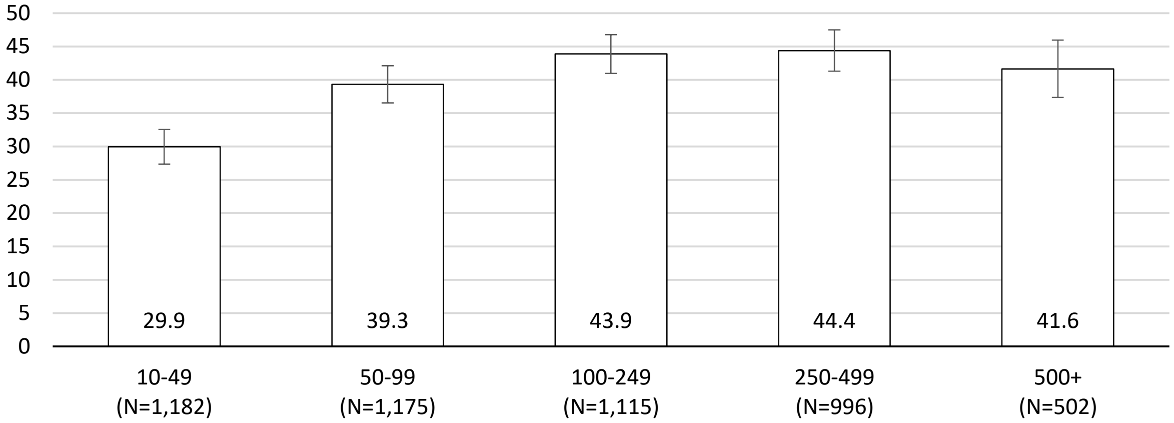
The question of whether the company exports products or services abroad was answered in the affirmative by almost a third of the company representatives (32.5 %) in the weighted data set.

Table 14 **Surveyed companies by export activity**

	disproportionate sample		
	unweighted		weighted
Export of products or services	Quantity	Percent	Percent
Yes	1,997	40.2	32.5
No	2,972	59.8	67.5
Total	4,969	100.0	100.0

Statistically significant differences can be seen in the comparison of the employee size classes (Figure 6). In particular, the share of exporting small companies, at 29.9 %, is significantly lower than the shares of larger companies, of which about two-fifths are active in export business.

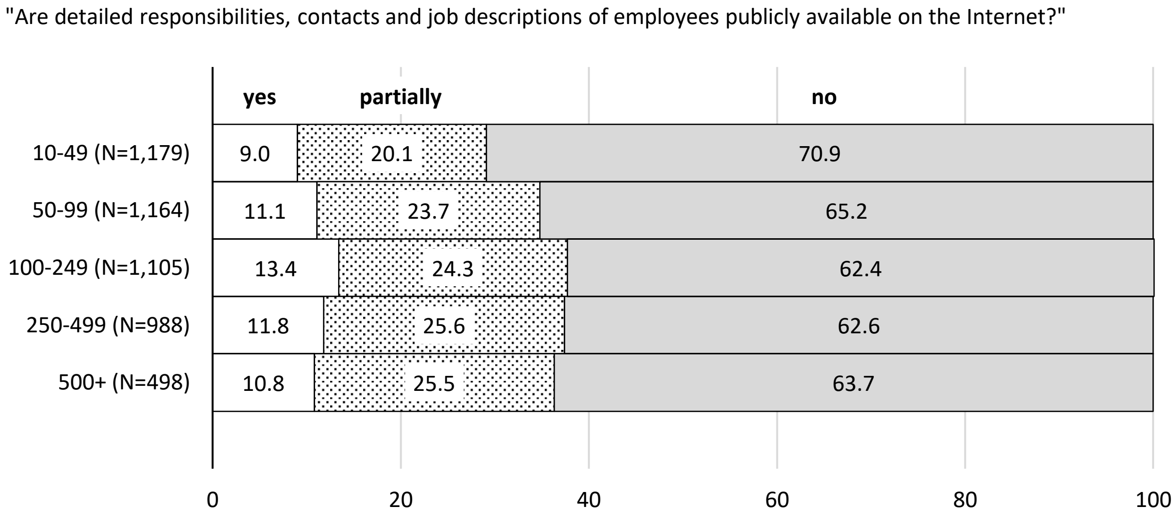
Figure 6 **Share of exporting companies by employee size class**
in percent; weighted data; 95 %-CI



4.7 Publicly available information

The availability of information on companies and its employees could encourage attacks such as social engineering and phishing, and was surveyed with the question: "Are detailed responsibilities, contacts and job descriptions of employees publicly available on the Internet?" The possible answers were "yes", "partially" and "no". More than two-thirds of the companies surveyed answered the question in the negative and thus do not make such information publicly available online (69.5 %; N=4,948). About one in ten companies answered the question in the affirmative and one in five publishes such company information at least partially on the internet (21.0 %). Here, too, there are statistically relevant differences between the employee size classes, according to which small companies are less likely to have such information available on the internet than larger companies (Figure 7).

Figure 7 **Employee information publicly available on the Internet by employee size class**
in percent; weighted data



5 IT SECURITY STRUCTURE IN THE COMPANY

On the one hand, the IT security structures of companies offer further characteristics to describe the sample. On the other hand, these characteristics also play a central role in explaining differences with regard to the extent to which different forms of cyber-attack affect organizations. As described in Section 2.4.4, various studies report on the existence of certain IT security features. However, these are usually presented in a purely descriptive manner and independent of prevalence.[217] In the following, the security structure features are also initially described in isolation and discussed in Chapter 10 in connection with the affectedness or non-affectedness of cyber-attacks as potential protection factors.

5.1 IT staff

A first characteristic concerns the number of persons employed in the company who are investing the majority of their working time in the operation of IT as a whole and IT- & information security in particular.

Table 15 **Interviewed companies by IT employees**

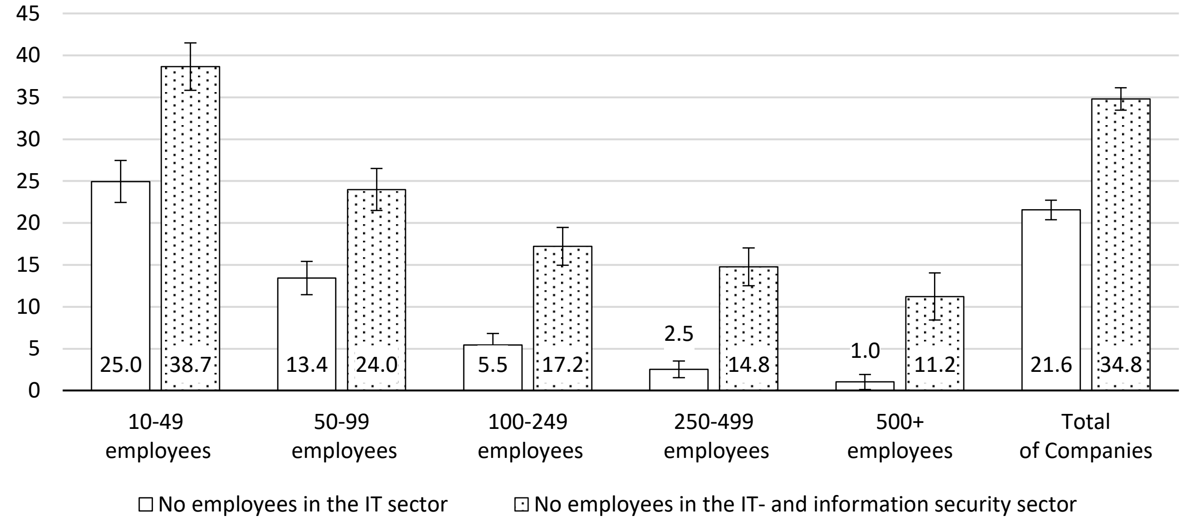
	disproportionate sample		
	unweighted		weighted
Employees in the IT department in total	Quantity	Percent	Percent
0	517	10.8	21.6
1	1,091	22.8	30.0
2 to 9	2,375	49.7	39.4
10 to 24	405	8.5	5.1
25 to 99	280	5.9	2.9
100+	111	2.3	1.0
Total	4,779	100.0	100.0
Of these, ... invest the majority of their working time in the operation of IT- and information security.			
0	562	13.2	16.8
1	1,979	46.6	54.0
2 to 9	1,583	37.3	27.4
10 to 24	85	2.0	1.3
25 to 99	26	0.6	0.3
100+	9	0.2	0.2
Total	4,244	100.0	100.0

About one fifth of the companies with ten or more employees (21.6 %) have no employees that invest the majority of their working time in IT (Table 15). A share of 30.0 % employs one employee in this area and the remaining half of the companies at least two.

[217] An exception to this is for example Rantala (2008) which relates outsourcing of IT functions to prevalence.

In companies that have at least one IT employee, in most cases at least one is also specifically responsible for the operation of IT & information security (one person: 54.0 %; at least two persons: 29.2 %).

Figure 8 **Interviewed companies without IT employees by employee size classes**
in percent; weighted data; 95 %-CI



Whether and how many employees in the company's work predominantly in the IT department as a whole and IT & information security is related to the employee size class. Figure 8 show that nearly two-fifths of small companies (10-49 employees) have no employees working in the IT & information security field (38.7 %; N=1,133) and one-quarter of these companies also had no employees working in the IT overall field (25.0 %). The larger the company, the smaller these shares become. Nevertheless, one out of every nine large companies (500 employees or more) has no employees in the IT & information security field (11.2 %; N=481). The non-employment of employees in these IT areas is related to whether or not IT functions have been outsourced to external service providers. Klahr et al. put the number of employees in British companies whose job descriptions include information security or governance at a slightly lower level and quote a total share of 38 % (10-49 employees: 46 %; 50-249 employees: 61 %: >250 employees: 73 %).[218] In contrast, Hillebrand et al. report higher proportions of employees with IT security skills (< 49 employees 54 %, > 49 employees 85 %).[219]

5.2 Outsourced IT functions

Overall, only a relatively small share of 18.6 % of companies with ten or more employees do not use external service providers for outsourced IT functions (Table 16). A large share (81.4 %) has outsourced at least one IT function to external service providers. At 76.0 %, external service providers are most frequently responsible for the company's web presence, followed by network administration and maintenance (63.0 %), IT security (49.3 %) and e-mail and communication operations (48.8 %). Cloud software and cloud storage are used comparatively rarely by external service providers (36.8 %) or other IT functions are outsourced

[218] Cf. Klahr et al. (2017).

[219] Cf. Hillebrand et al. (2017: 56).

(10.8 %).[220] The proportion of outsourced IT security was also surveyed by Klahr et al. and is also estimated at 49 % (10-49 employees: 58 %; 50-249 employees: 64 %; >500 employees: 49 %) of the companies surveyed, although the figures for both studies diverge further with increasing company size (see Figure 9). [221]

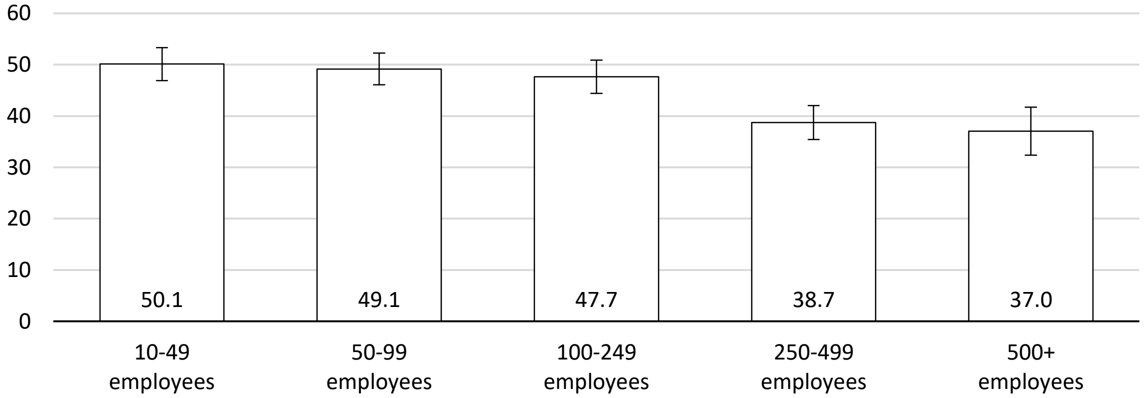
Table 16 **Interviewed companies according to outsourced IT functions**
Multiple answers possible regarding IT functions

	disproportionate sample		
	unweighted		weighted
IT function(s) outsourced?	Quantity	Percent	Percent
No	817	16.6	18.6
Yes	4,116	83.4	81.4
Total	4,933	100.0	100.0
If "yes," in what area?			
E-Mail & Communication	1,876	45.6	48.8
Network Administration & Maintenance	2,267	55.1	63.0
Web presence	3,297	80.1	76.0
Cloud Software & Cloud Storage	1,597	38.8	36.8
IT Security	1,872	45.5	49.3
Other	550	13.4	10.8

When comparing companies by employee size classes with regard to the question of whether external service providers perform certain IT functions, only small differences are noticeable. Companies with 10 to 49 employees (80.5 %) were the least likely to answer this question in the affirmative, while companies with 50 to 99 and 250 to 499 employees (both 85.7 %) were the most likely to answer in the affirmative.[222]

With regard to the outsourcing of IT security, on the other hand, there are significant differences between the employee size classes: Small companies are more likely to hire service providers in this area than large companies (Figure 9).

Figure 9 **Share of companies with outsourced IT security by employee size class**
in percent; weighted data, 95 %-CI



[220] The category "other" cannot be resolved in this question, since for reasons of time economy it was not always possible to collect free-text information during the interviews.

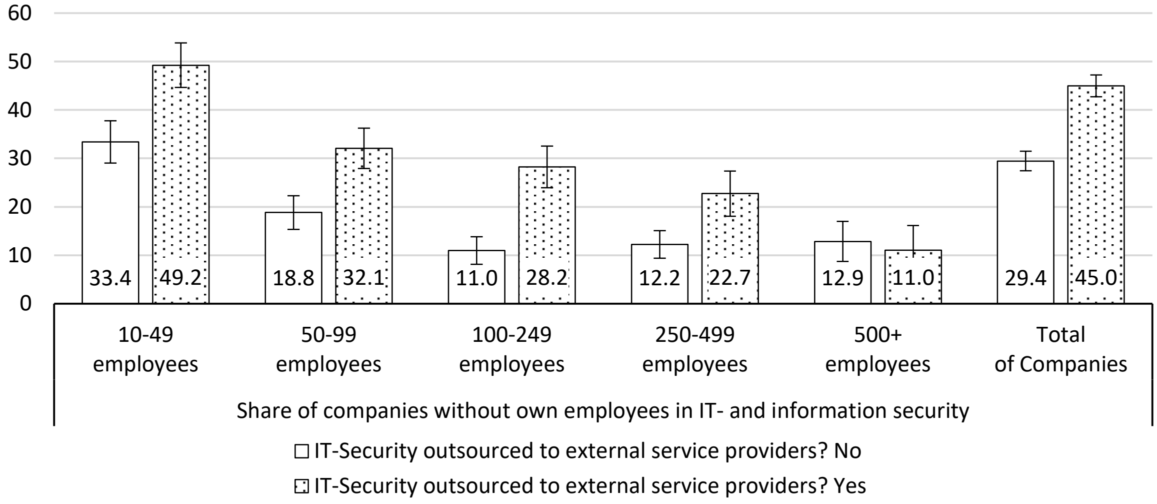
[221] Cf. Klahr et al. (2017).

[222] Companies with 100-249 employees: 83.0 %; companies with 500 employees or more: 82.3 %.

If the information on whether external IT service providers are used or not is put in connection with the information on the employment of internal employees in the IT sector, then it can be seen, as expected, that companies that use external IT service providers significantly more frequently do not employ their own employees in the IT sector as a whole (23.1 %) and for IT and information security (37.1 %) than companies that have not outsourced any IT functions (14.8 % and 24.9 % respectively). If the employee size class is also included, it can also be seen that this only applies to small and medium-sized companies (up to 249 employees) in terms of IT as a whole. With a few exceptions, large companies (250 employees or more) always have their own IT employees, whether they use external IT service providers or not.

Figure 10 **Interviewed companies without employees in the IT & information security sector**

in percent; weighted data, 95 %-CI



With regard to the connection between outsourced IT security and the employment of own employees in the area of IT and information security, Figure 10 shows on the one hand that, with the exception of large companies (500 employees or more), the proportion of companies without own employees in the area of IT and information security is significantly higher among those who have entrusted external service providers with IT security. On the other hand, it can be seen that there are relatively large shares of small companies (10-49 employees and 50-99 employees) in particular that have neither their own specialised IT employees nor external service providers for IT security (33.4 % and 18.8 % respectively; N=455 and 489 respectively).

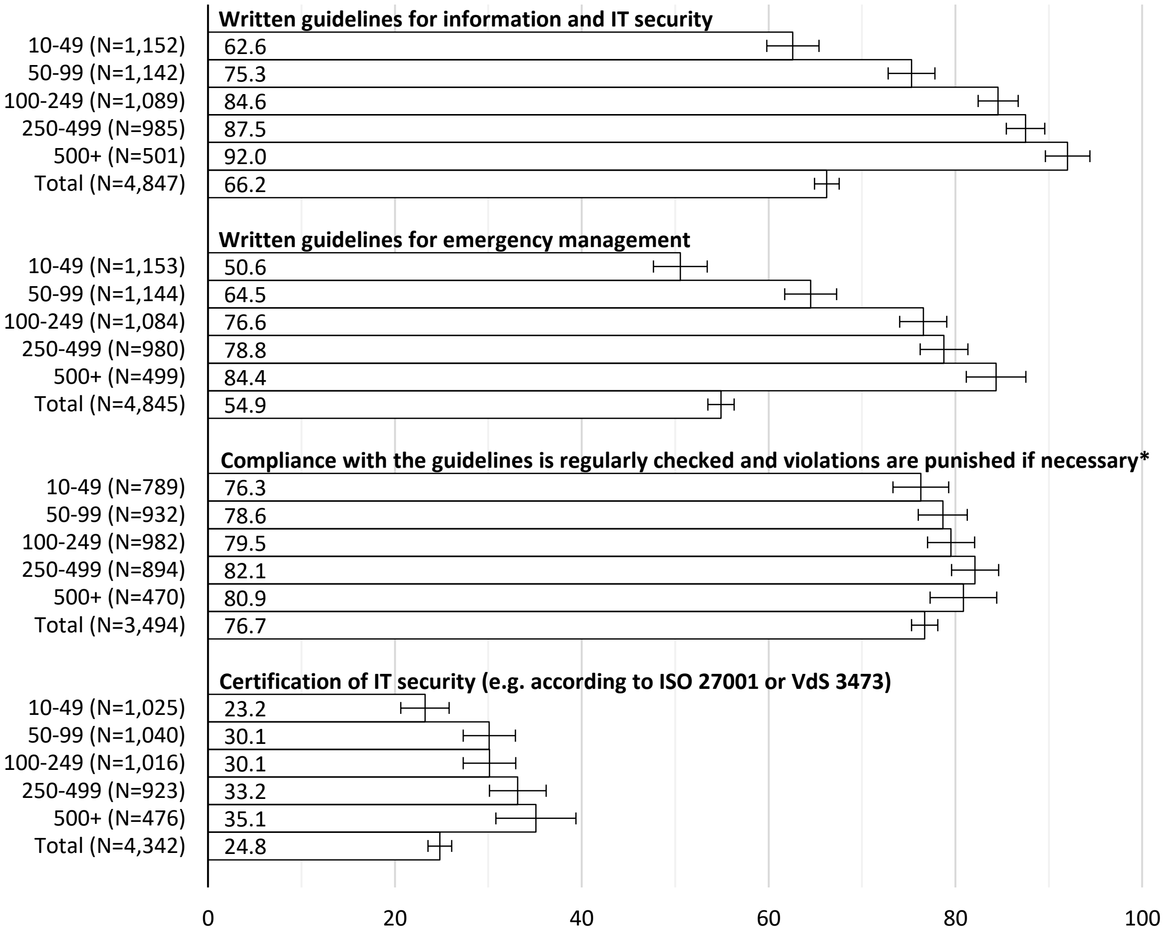
5.3 IT security measures

5.3.1 Organizational measures

Organizational measures, such as written guidelines for information or IT security or for emergency management, are available in many companies with ten or more employees (66.2 % and 54.9 % respectively; N=4,847; Figure 11).[223]

[223] No information on the scope and content of such guidelines was collected.

Figure 11 **Companies with guidelines and certifications by employee size class**
in percent; weighted data, 95 %-CI



*) Just companies that have written guidelines

Of these, three quarters (76.7 %; N=3,494) regularly check compliance with these regulations and, if needed, punish any violations. With regard to similar surveys, Hillebrand et al. show a lower proportion of companies with written regulations on IT security (> 49 employees: 22 %; < 49 employees: 68 %) and emergency management (> 49 employees: 29 %; < 49 employees: 71 %),[224] although this may also be due to the fact that companies with 0-9 employees were also included. The results of the two studies converge, particularly with regard to larger companies. Klahr et al. also estimate the proportion of companies with formal guidelines that are affected by cyber security risks to be significantly lower overall (10-49 Employees: 39 %; 50-249 Employees: 59 %; >500 Employees: 71 %).[225]

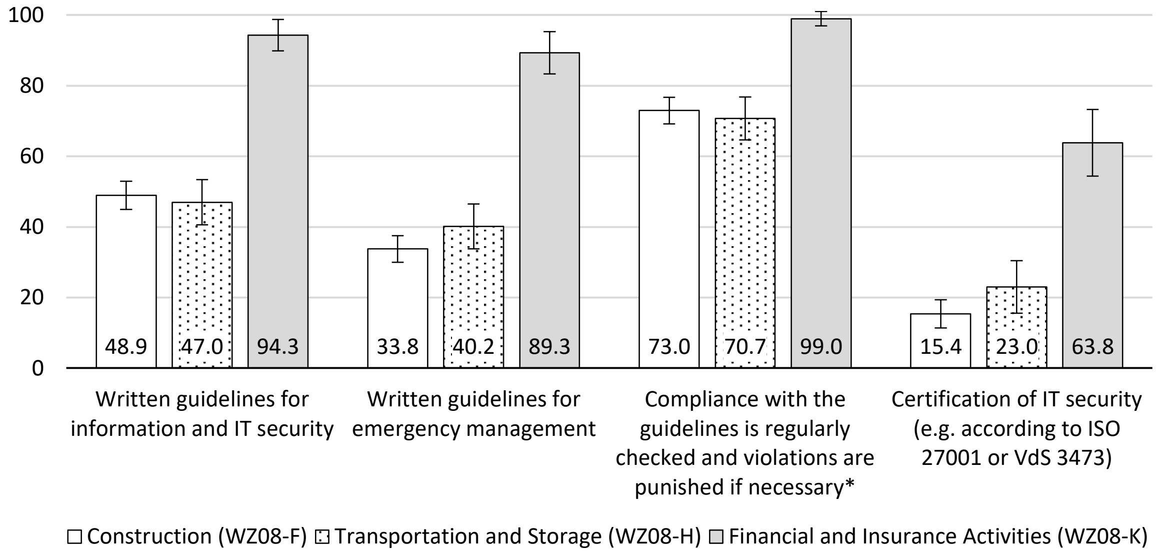
[224] Cf. Hillebrand et al. (2017).

[225] Cf. Klahr et al. (2017).

The certification of IT security (e.g. according to ISO 27001[226] or the BSI Grundschutz[227]) is comparatively rare but surprisingly widespread; about a quarter of the companies with ten or more employees report certified IT security. It should be noted, however, that 12.1 % of company representatives were unable to answer this question due to a lack of knowledge, which reduced the number of valid cases. The Bitkom study puts the proportion of respondents who have security certification (e.g. according to ISO 27001, BSI Grundschutz or similar), but with a focus on industrial companies, at around 49 %, which is significantly higher.[228] Bundesdruckerei also mentions a share of companies with security certifications of 45 % in its survey.[229]

A comparison of companies by employee size classes shows, as expected, that in some cases the spread of these measures is significantly lower in smaller companies than in the large ones. For example, about two-thirds of small companies (10-49 employees) have a directive on information or IT security (62.6 %; N=1,152), but nearly every large company (500+ Employees: 92.0 %; N=501) has one.

Figure 12 **Companies with guidelines and certifications according to WZ08 classes (F, H, K)**
in percent; weighted data; 95 %-CI



*) Just companies that have written guidelines

With regard to the sectoral affiliation of the companies, significant differences can also be observed. As an example of this, the economic sectors F, H and K are compared in Figure 12.[230] WZ08-F and H (Construction and Transportation and Storage) have the smallest shares with regard to existing organizational and technical IT security measures, while WZ08-K (Financial

[226] The international standard ISO 27001 refers to different areas of information security management systems. It should be noted that the International Organization for Standardization (ISO) itself does not carry out certifications, but only issues them. A company can announce that it has achieved ISO conformity itself, have it confirmed by business partners and customers or have it determined and certified by an external audit procedure (Kersten et al. 2016).

[227] The IT-Grundschutz catalogues of the German Federal Office for Information Security (BSI) aim at the information security of organisations as well as the development of a management system for information security (ISMS) and should be ISO 27001-compatible (source: https://www.bsi.bund.de). See also (Kersten et al. 2016).

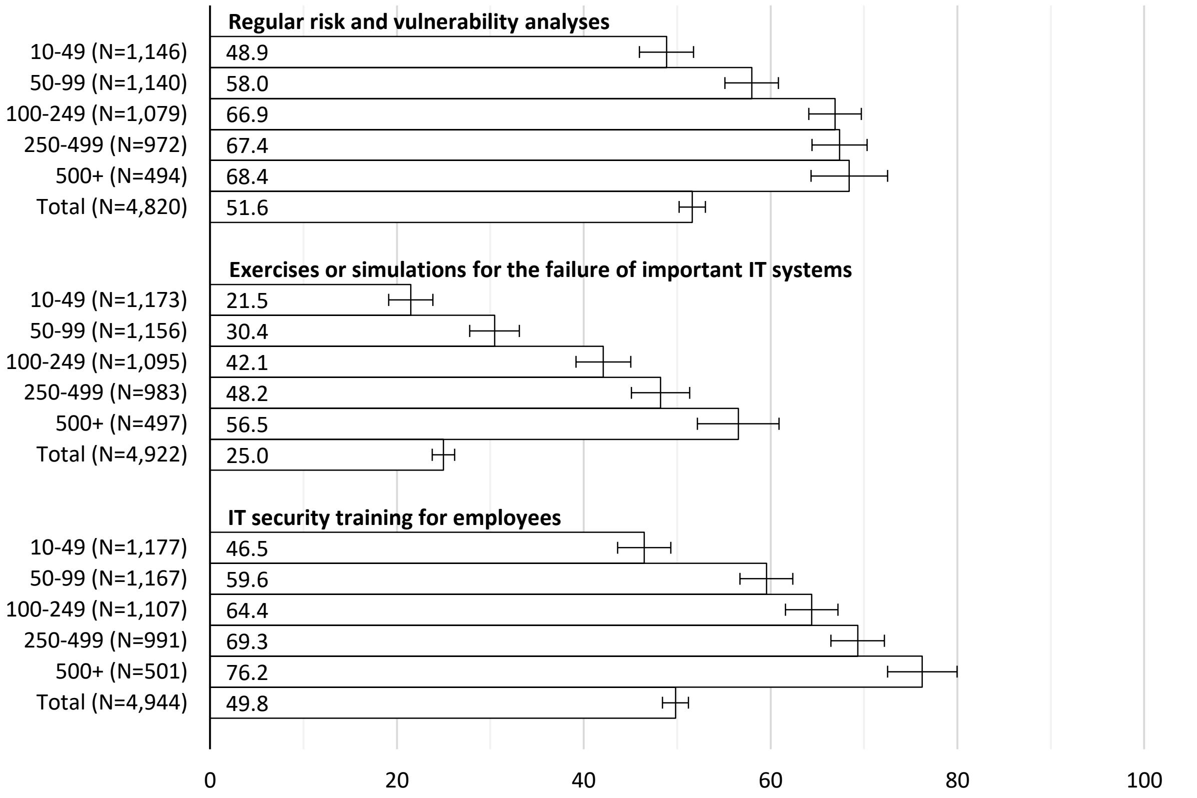
[228] Cf. Bitkom e.V. (2018).

[229] Cf. Bundesdruckerei GmbH (2017).

[230] The shares of existing IT security measures according to the first and second level WZ classes are shown in the Appendix in Table 45 to Table 48.

and Insurance Activities), with one exception, has the largest shares throughout[231] and serves as a positive example. Almost all financial and insurance service providers have written guidelines on information and IT security (94.3 %; N=105) and on emergency management (89.3 %; N=103) and review them regularly (99.0 %; N=94). In contrast, the shares of the other two branches of the economy are significantly and noticeably lower. However, it should be noted that, for example, the share of small companies (10-49 employees) is smaller in the group of financial and insurance service providers than in the other two WZ classes.

Figure 13 **Companies with analyses, exercises and training courses on IT security according to employee size**
in percent; weighted data; 95 %-CI



About half of the companies with ten or more employees carry out regular risk and vulnerability analyses (51.6 %) and train their employees in IT security (49.8 %). For British companies Klahr et al. report lower training rates within the last 12 months (10-49 employees: 25 %; 50-249 employees: 43 %; >250 employees: 63 %).[232] Active technical testing (e.g. penetration testing) is also reported to be lower (25 %). With regard to training rates, however, the German Bundesdruckerei states similar results to this study with 46 %.[233]

Exercises or simulations for the failure of important IT systems are carried out by a quarter (25.0 %) (Figure 13). Here, too, the connection with the employee size class of companies is clearly visible in that the proportion of larger companies that implement these IT security

[231] The exception concerns the existence of physically separate backups, although the difference to the WZ08 classes with higher percentages is not statistically significant.

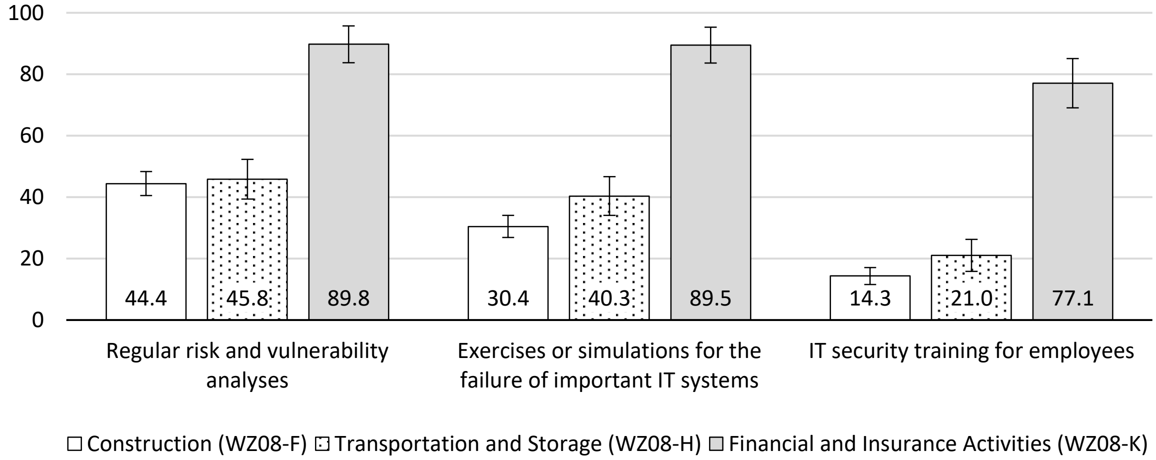
[232] Cf. Klahr et al. (2017).

[233] Cf. Bundesdruckerei GmbH (2017).

measures is larger than that of smaller companies. For example, only one-fifth of small companies (10-49 employees) conduct exercises or simulations on the failure of IT systems (21.5 %), while this measure is used by more than half of large companies (500+ employees) (56.5 %).

In addition to differences in the comparison of the employee size class of the companies, differences can also be seen with regard to the branch of industry (Figure 14). While nine out of ten companies in Financial and Insurance Activities (WZ08-K) regularly carry out risk and vulnerability analyses as well as exercises or simulations for the failure of important IT systems, these measures are only used by four or three out of ten companies in the Construction sector (WZ08-F). The difference is even more pronounced when it comes to the implementation of IT security training: Just under eight out of ten companies in the Financial and Insurance Activities sector are opposed to one to two out of ten companies in Construction that rely on training.

Figure 14 **Companies with analyses, exercises and training by WZ08 classes (F, H, K)**
in percent; weighted data; 95 %-CI



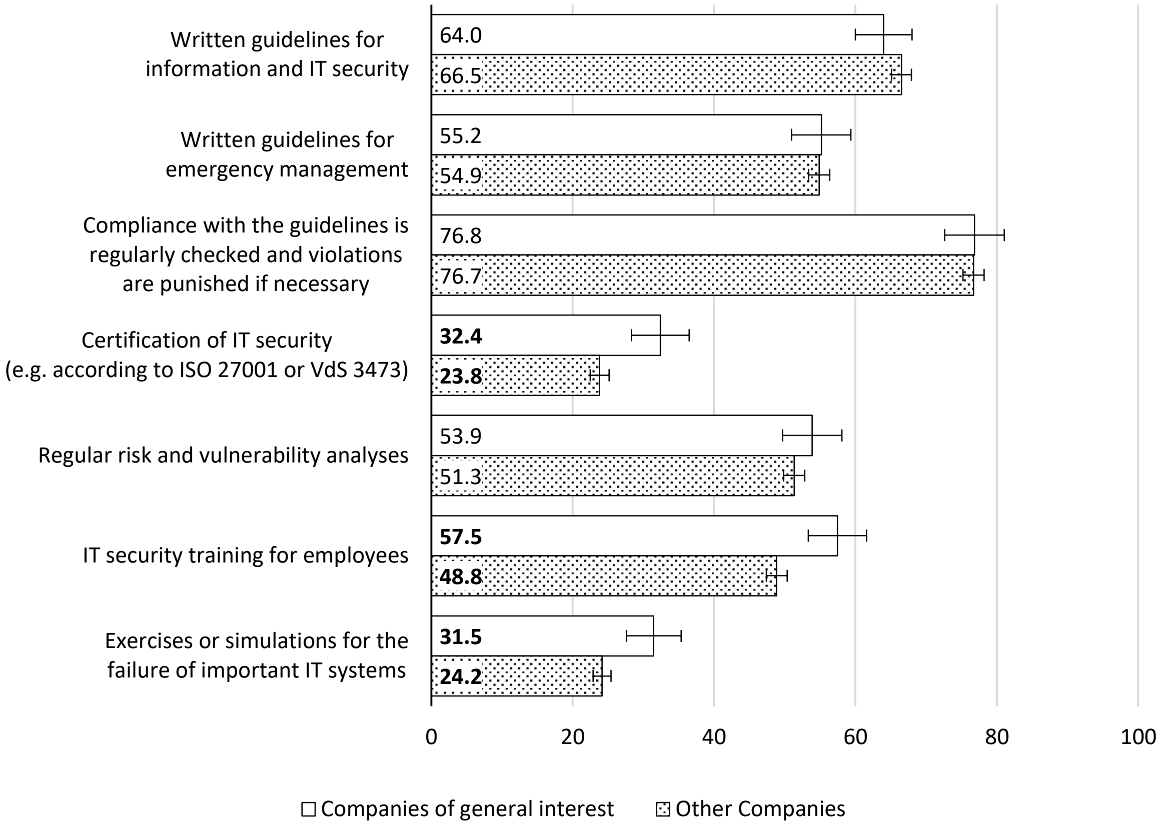
At the second level of the WZ08 classes, the following branches of the economy stand out with relatively low shares in terms of organisational IT security measures[234]: WZ08-16 (Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials), WZ08-23 (manufacture of other non-metallic mineral products) and WZ08-31 (Manufacture of furniture). In contrast, the shares of WZ08-64 (Financial service activities, except insurance and pension funding), WZ08-62 (Computer programming, consultancy and related activities) and WZ08-79 (Travel agency, tour operator and other reservation service and related activities) are in the upper range.

A comparison of companies according to their affiliation to companies of general interest[235] (Figure 15) shows that certifications in the field of IT security, IT security training for employees and exercises or simulations for the failure of important IT systems are proportionally more frequent in companies of companies of general interest (32.4 %, 57.5 % and 31.5 % respectively) than in companies of the other WZ08 classes (23.8 %, 48.8 % and 24.2 % respectively). There are no statistically relevant differences with regard to the other organizational measures.

[234] See Table 47 in Annex 1.

[235] See footnote 194 and Table 4 in Section 3.4.1, and Table 43 in Annex 1 lists all WZ classes belonging to services of general interest.

Figure 15 **Organizational IT security measures according to affiliation to companies of general interest**
in percent; weighted data; 95 %-CI



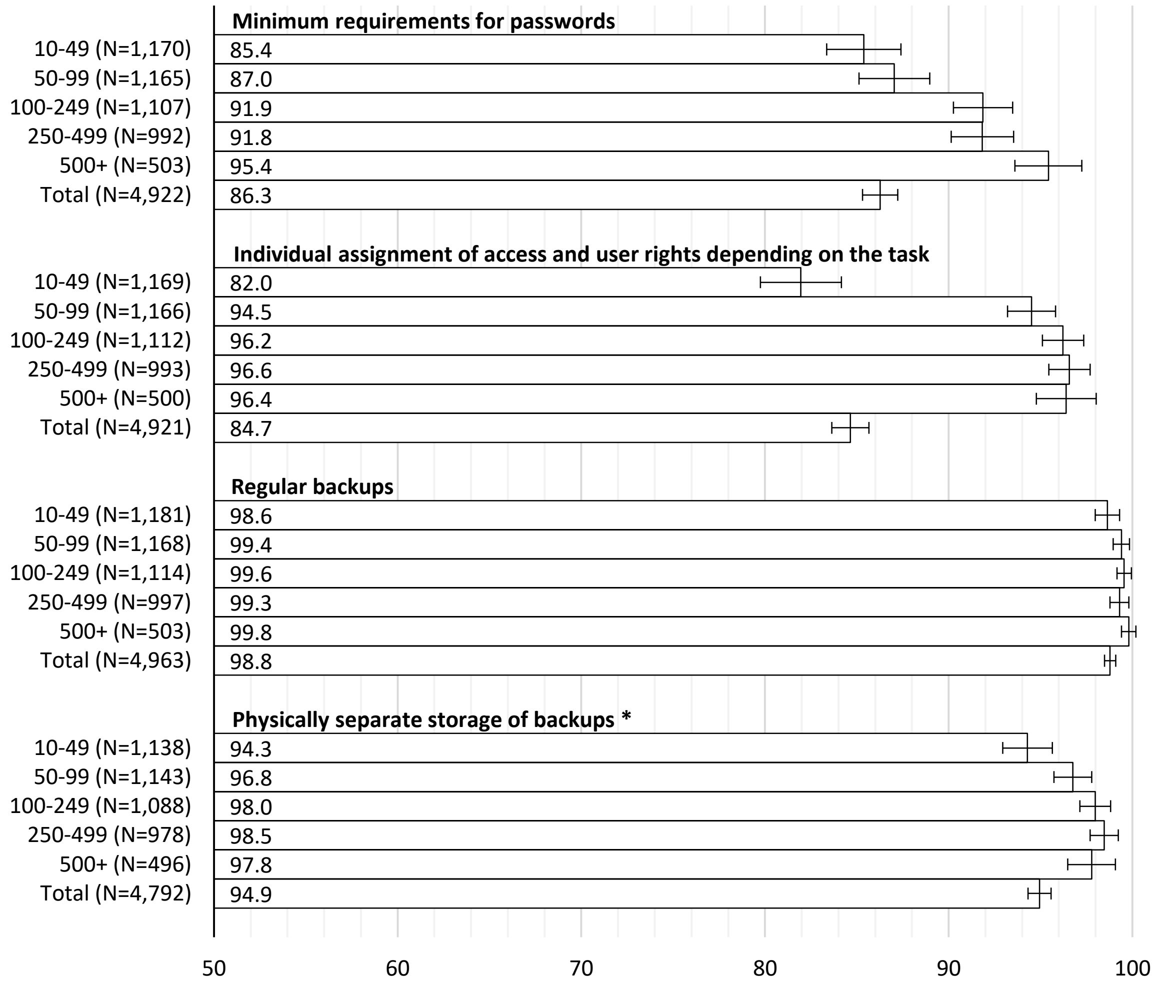
5.3.2 Technical measures

With regard to the spread of technical measures to increase IT security, it is noticeable that this is generally relatively high (Figure 16 and Figure 19) and that the shares of employee size classes no longer differ as clearly as in the case of organisational security measures. In this respect, there now appear to be certain standards that are implemented by most companies with ten or more employees. However, no statements can be made as to how effective and efficient the implementation of the individual measures is. The most significant differences are to be found in terms of minimum requirements for passwords[236] and the individual assignment of access and user rights depending on the task. For example, one in seven companies with ten to 49 employees (14.6 %) has no minimum requirements for passwords and approximately one in six (18.0 %) has no individual, task-specific access and user rights, while this applies to only one in 22 or 28 companies with 500 or more employees (4.6 % and 3.6 % respectively).

[236] There was no further specification as to whether there are minimum requirements for passwords in the company. It therefore remains open which requirements are set for passwords in the companies (e.g. password length, change frequency etc.). In this respect, a paradigm shift has taken place in recent years. The influential password guideline of the US technology standards authority NIST (6 to 8 characters, use lower and upper case letters, numbers and special characters and change the password after 90 days), which has been in existence since 2003, from Burr et al. (2003) was fundamentally revised in 2017. According to Grassi et al. (2017: 67f.) Compared to password complexity, password length is the more decisive criterion for password security. Passwords (memorized secrets) should be as long as possible (at least 8 characters) and without words from the dictionary or "black list". The required complexity (use of lower and upper case letters, numbers and special characters) could be reduced with increasing password length. Especially for the protection of sensitive data and systems, a two-factor authentication (2FA) is also a useful addition.

Virtually all companies regularly back up their data, and although there are small and sometimes significant differences between the employee size classes in terms of the physical separation of the backups (e.g. 10-49 employees: 94.3 % vs. 250-499 employees: 98.5 %), the percentages are over 90.0 % in each case.

Figure 16 **Companies with technical IT security measures by employee size class**
in percent; weighted data; 95 %-CI



*) Just companies that perform backups regularly

Other studies also report the widespread use of the above-mentioned safety measures. For example, Klahr et al. report that a total of 69 % of British companies surveyed have minimum requirements for passwords, with this proportion rising to 91 % for larger companies.[237] According to the findings of Hillebrand et al., between 96 % - 98 % of the companies surveyed use passwords, although minimum requirements were not discussed here. With regard to regular data backups, they cite proliferations of 89 % for small SMEs and 99 % for larger SMEs.[238] Brandl et al. also report a penetration rate of 96 %,[239] which even exceeds the Bikom study with 100 % for industrial companies.[240] However, the Gesamtverband der Deutschen Versicherungswirtschaft (GDV) estimates the individual assignment of access and user rights at 68 % to

[237] Cf. Klahr et al. (2017).

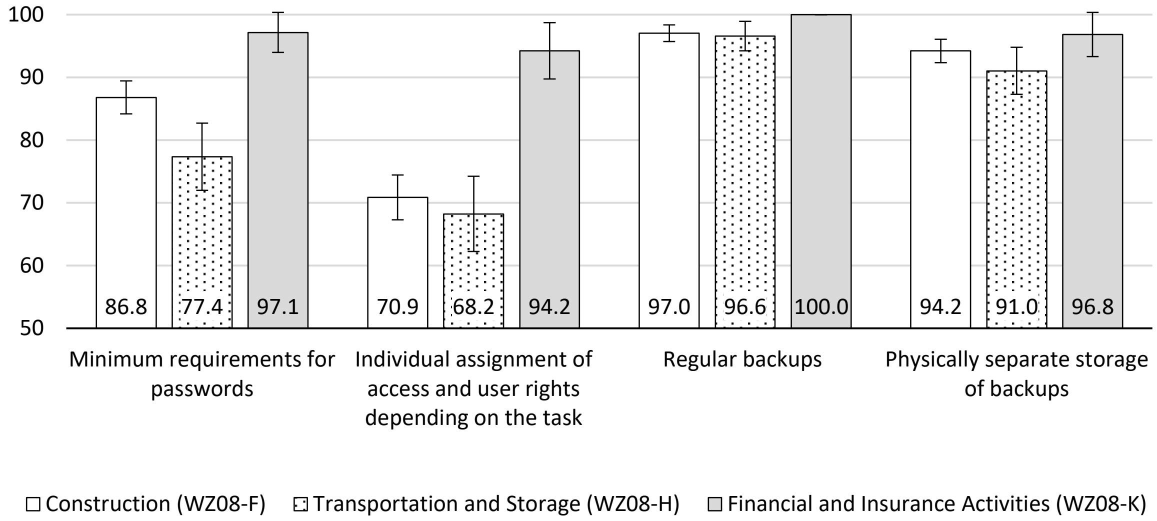
[238] Cf. Hillebrand et al. (2017).

[239] Cf. Brandl et al. (2016).

[240] Cf. Bitkom e.V. (2018).

be lower than this study, [241] whereas Klahr et al. estimate this proportion to be similarly high at 79 %.[242]

Figure 17 Companies with PW requirements, ind. assignment of rights and backups, according to WZ08 classes (F, H, K)
in percent; weighted data; 95 %-CI



When comparing the WZ08 classes F, H and K, significant differences are again apparent (Figure 17).[243] The share of companies using minimum password requirements is significantly lower for companies in the traffic & warehousing sector (77.4 %) than for companies in the construction sector (86.8 %), which in turn is significantly lower than the share for financial and insurance activities (97.1 %). The shares of companies with individual and task-based allocation of access and user rights are significantly lower in the construction sector as well as in transport and warehousing companies than in financial and insurance activities (70.9 % and 68.2 % vs. 94.2 %). There are no statistically relevant differences between these sectors with regard to the performance of regular backups and their physically separate storage.

Table 17 Interviewed companies according to the execution and frequency of backups

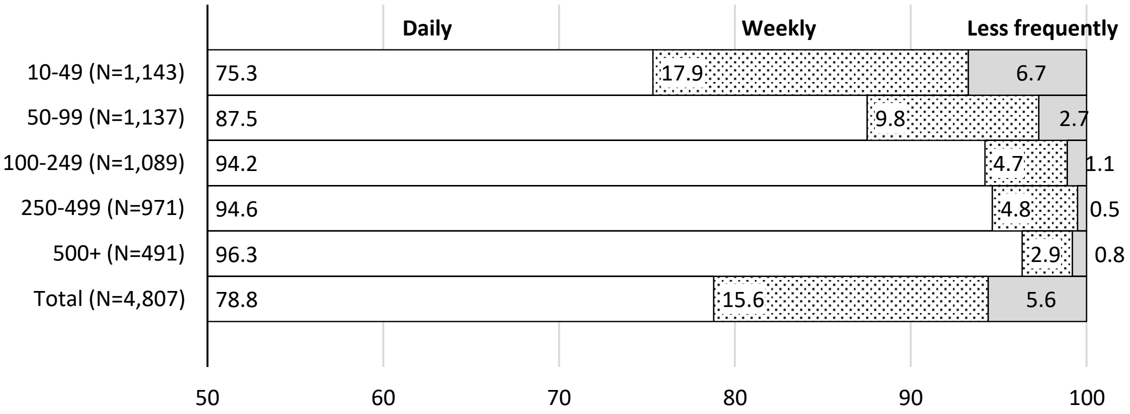
		disproportionate sample		
		unweighted		weighted
Regular backups?		Quantity	Percent	Percent
	No	37	0.7	1.2
	Yes	4,928	99.3	98.8
	Total	4,965	100.0	100.0
If "yes," how often?				
	Daily	4,262	88.4	78.8
	Weekly	425	8.8	15.6
	Less frequently	136	2.8	5.6
	Total	4,823	100.0	100.0

[241] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[242] Cf. Klahr et al. (2017).

[243] See also Table 46 in Annex 1.

Figure 18 **Companies with regular backups by backup frequency and employee size classes**
in percent; weighted data



Larger differences only occur when the question of backup frequency is raised: Overall, over a fifth of all companies (21.2 %) back up their data only weekly or even less frequently (Table 17), although this proportion is in some cases significantly lower for large companies than for smaller ones. As many as a quarter of the companies with 10 to 49 employees (24.7 %) do not carry out daily backups, whereas this proportion is significantly lower at 3.7 % for companies with 500 employees or more (Figure 18). Brandl et al. report that between 76 % and 85 % of the surveyed companies that have not implemented a data backup concept or have not implemented a data backup concept report permanent or daily data backups, which is in line with the results of this study.[244]

Current anti-virus software and the protection of IT systems by means of firewalls are generally used by almost all companies (98.8 % and 98.0 % respectively),[245] which is supported by other studies.[246] A comparison of the employee size classes reveals only very small, albeit in part statistically significant, differences (Figure 19). A similar picture emerges with regard to the regular and timely installation of available security updates and patches.[247] For German companies Hillebrand et al. report comparable patch and update rates (small SMEs: 90 %; larger SMEs: 97 %).[248] Klahr et al. also found that a large proportion of British companies (92 %) stated that they install software updates promptly.[249]

[244] Cf. Brandl et al. (2016).

[245] No statements can be made about the manufacturer, scope and effectiveness of the software used. The high percentage could be explained by the fact that antivirus software is often already included in the operating system (e.g. Windows Defender Antivirus in Windows 10) and that free software is available. On the question of whether antivirus software offers protection against malware, see e.g. Sukwong et al. (2011) or Min et al. (2014).

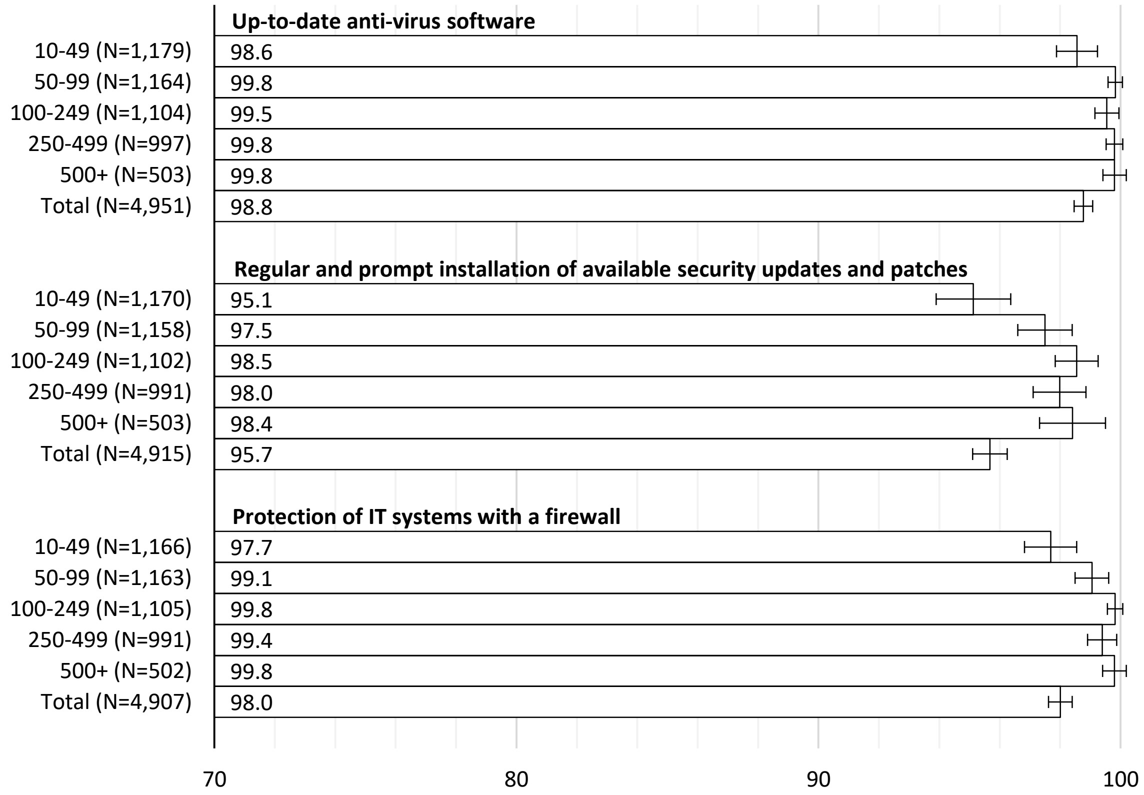
[246] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018); Hillebrand et al. (2017); Bitkom e.V. (2018).

[247] The question remains open as to whether software is used for which no security updates or patches are available.

[248] Cf. Hillebrand et al. (2017).

[249] Cf. Klahr et al. (2017).

Figure 19 **Companies with technical IT security measures by employee size class**
in percent; weighted data; 95 %-CI

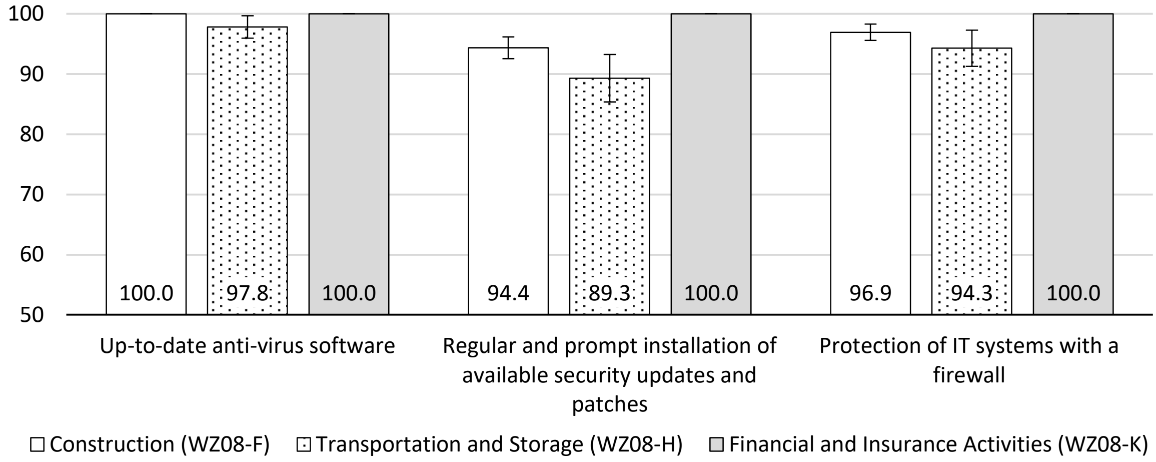


For these three technical IT security measures (see figure 20), there are only small differences between the companies of WZ08 classes F, H and K. The share of transport and warehousing companies that regularly and promptly install security updates and patches (89.3 %) is significantly smaller than for the other two WZ08 classes (F: 94.4 %; K: 100 %). The share with up-to-date anti-virus software and firewall protection is also slightly but significantly lower for transport and warehousing companies (97.8 % and 94.3 % respectively) than for financial and insurance service providers (100 % each).

The second level industries that stand out [250] in terms of technical IT security measures with smaller percentages are in particular WZ08-10 (Manufacture of food product), WZ08-24 (Manufacture of basic metal) and WZ08-49 (Land transport and transport via pipeline). In contrast, again the shares of WZ08-64 (Financial service activities, except insurance and pension funding) and WZ08-62 (Computer programming, consultancy and related activities) and WZ08-26 (Manufacture of computer, electronic and optical products) are in the upper range.

[250] See Table 48 in Annex 1.

Figure 20 **Companies with anti-virus software, security updates and firewall by WZ08 classes (F, H, K)**
in percent; weighted data; 95 %-CI



When asked whether a simple firewall (packet filtering by source and destination address through a software firewall or a network-level router) or an advanced firewall (additional monitoring and filtering by packet content at the application level) is used, more than one-fifth (22.4 %) of the company representatives surveyed were unable to answer (Table 18). Including the "Don't know" response category, about half of the companies with firewall protection use an advanced firewall and over a quarter (28.5 %) use a simple firewall.

Table 18 **Interviewed companies by firewall protection**

	disproportionate sample		
	unweighted		weighted
Firewall protection?	Quantity	Percent	Percent
No	48	1.0	2.0
Yes	4,882	99.0	98.0
Total	4,930	100.0	100.0
If "Yes", what type of firewall?			
Simple firewall, i.e. packet filtering by source and destination address by software firewall or router at network level	981	20.6	28.5
Extended firewall, i.e. additional monitoring and filtering by packet content (Deep Packet Inspection DPI) at application level and logging of data traffic	3,120	65.5	49.1
Don't know	665	14.0	22.4
Total	4,101	100.0	100.0

A comparison of companies by employee size classes (Figure 21) shows that smaller companies in particular make more frequent use of protection by a simple firewall (e.g. 10-49 employees: 30.9 % vs. 14.5 % for companies with 500 employees or more) and that they are significantly less likely to provide information on the maturity level of the firewall (e.g. 10-49 employees: 24.9 % vs. 6.5 % for companies with 500 employees or more). A possible reason for this may be the complexity and high configuration effort, which larger companies are more likely to be able to handle than smaller companies. Furthermore, the proportion of companies that have indicated that they have an advanced firewall appears to be relatively high, given the time and cost required to effectively operate such a firewall. In some cases, these technical security measures may be available in the companies, but whether and to what extent they are efficiently operated and actually effective cannot be fully answered in this study.

Figure 21 **Companies with firewall protection by type of firewall and employee size class**
in percent; weighted data

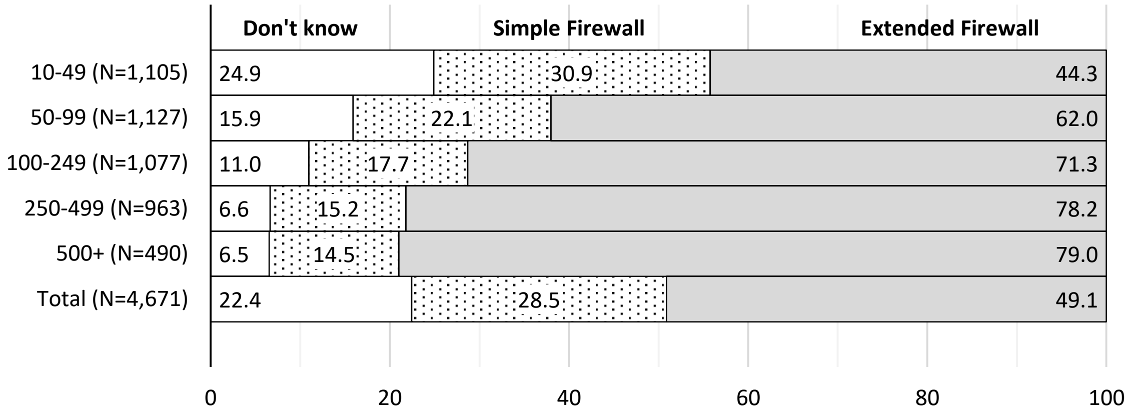
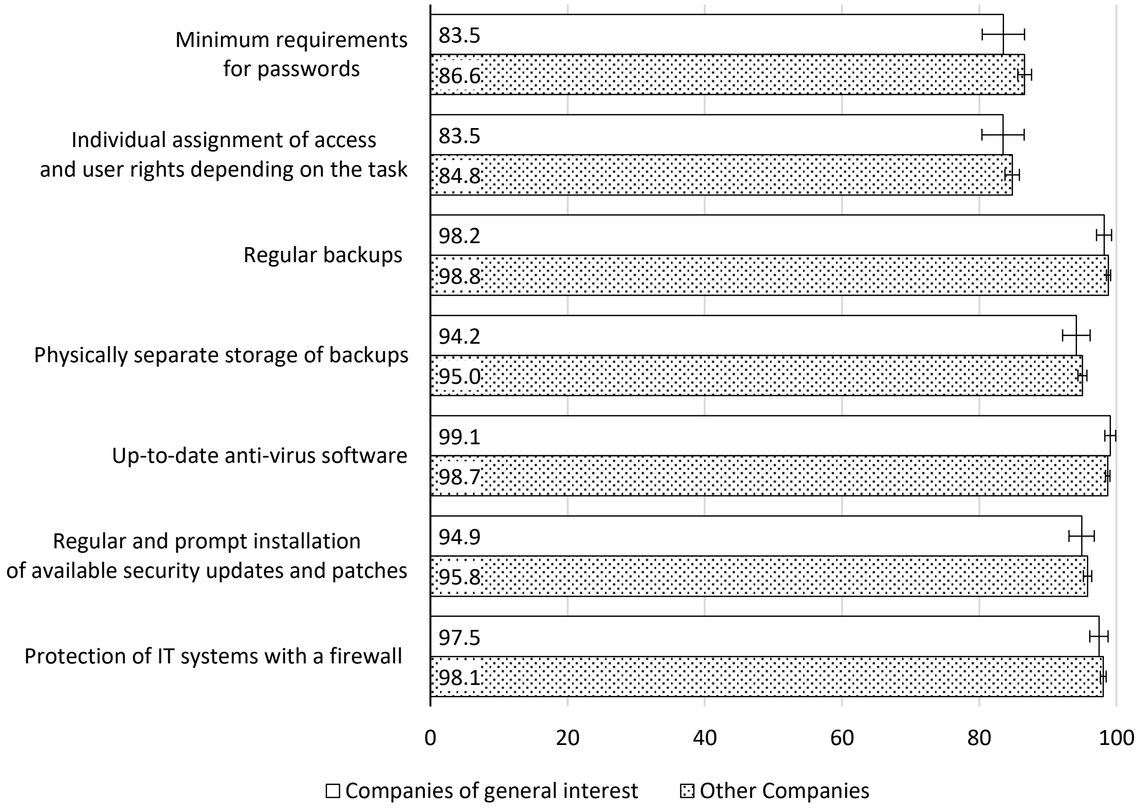


Figure 22 **Technical IT security measures according to affiliation to companies of general interest**
in percent; weighted data; 95 %-CI



As in the case of organisational IT security measures, the shares of companies with existing technical measures are also compared according to their affiliation to companies of general interest[251] (Figure 22). In contrast to the organizational measures, there are no statistically relevant differences.

[251] See footnote 194 and table 4 in Section 3.4.1. Also, table 43 in Annex 1 lists all WZ classes belonging to services of general interest.

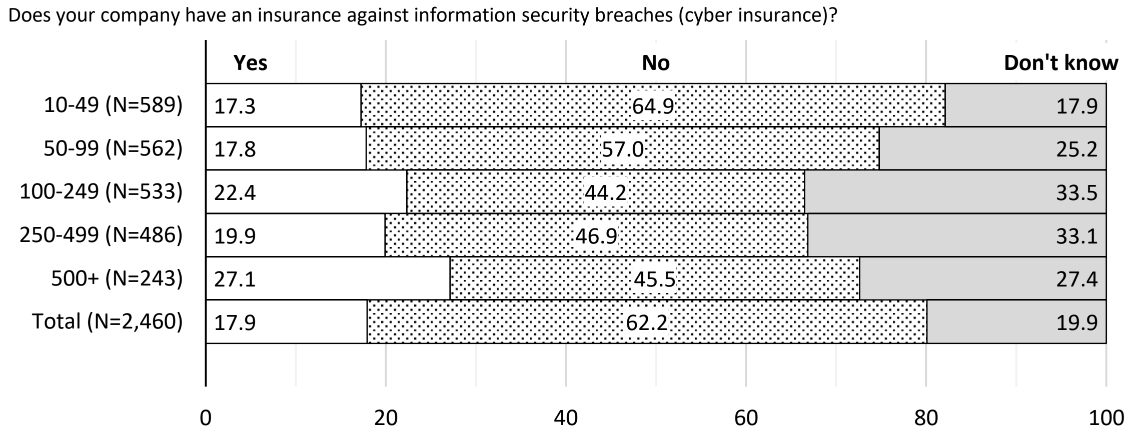
5.4 Insurance against information security breaches

For reasons of time economy, only half of the company representatives were asked the questions on cyber insurance in a split-half procedure. This meant that additional questions on another topic could be included in the questionnaire, which were answered by the other half and did not increase the average interview duration envisaged.[252] In order to avoid systematic bias, the selection of companies for one or the other group was made at random.

Asked whether the company had taken out insurance against information security breaches (cyber insurance), more than a fifth (27.4 %; N=1,767) answered "yes". It should be noted, however, that the proportion of all respondents who did not know this, when excluded from the valid information, was 26.8 % (N=2,483). If the answer category "don't know" is included, 17.9 % (N=2,460) of the companies have cyber insurance, 62.2 % have none and 19.9 % of the company representatives surveyed did not know (Figure 23).

Figure 23 **Companies with cyber insurance by employee size class**

in percent; weighted data; split-half group B



Differentiated by employee size classes, it is noticeable that the proportion without knowledge of the existence of cyber insurance is smaller in small companies than in medium and large ones. On the other hand, the proportion of small companies with cyber insurance is also significantly smaller (10-49 employees: 17.3 %) than of large companies (500+ Employees: 27.1 %). The GDV mentions smaller shares. For example, only around 6 % of micro, 15 % of small and 9 % of medium-sized companies have cyber insurance.[253] Corresponding results of a Bitkom study are in a similarly high range and for companies with 100 or more employees even higher (10-99 employees: 10 %; 100-499 employees: 23 %; >500 employees: 32 %).[254] The focus of Bitkom on industrial companies should be noted at this point. In its survey of 4,100 companies from five different countries, the British insurance company Hiscox even states a share of 33 % of companies that have taken out cyber insurance. Klahr et al. put the highest proportion of insurance policies covering cyber incidents in the reported state of research at 38 % of British

[252] A further increase in the average interview duration of 20 minutes would have led to higher dropout rates, according to previous experience of the survey institute.

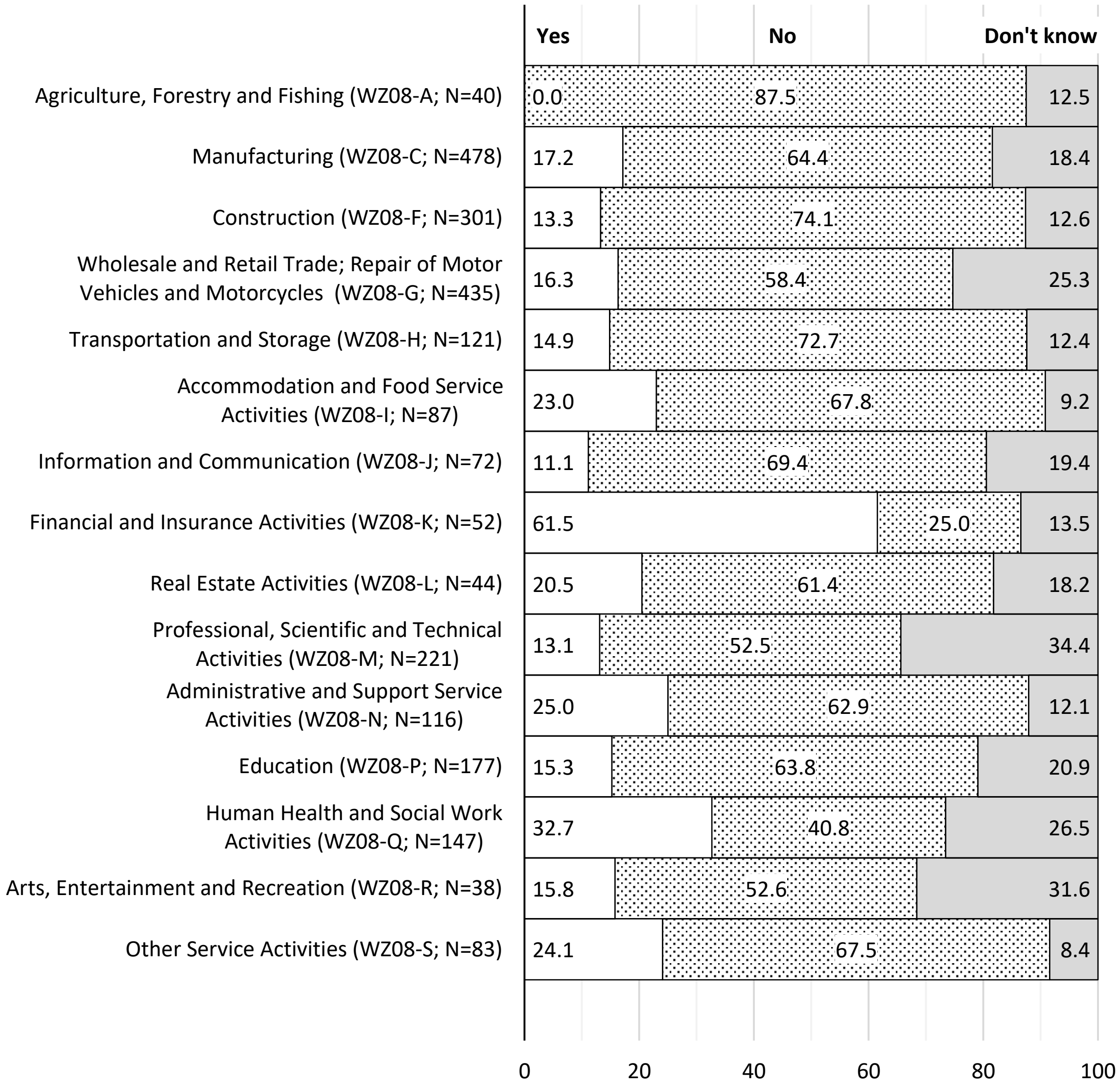
[253] Cf. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018).

[254] Cf. Bitkom e.V. (2018): The cyber insurance is defined as follows: Insurance in the event of the occurrence of digital industrial espionage, sabotage or data theft.

companies.[255] In addition to the limitations described in Section 2.3, it is conceivable that different information on the conclusion rates of insurance policies against information security breaches is due to the fact that certain business interruption insurance policies also cover damage caused by cyber-attacks, which were then named by the companies surveyed. In addition, the proportion of companies insured against information security breaches is likely to have grown in recent years and will continue to grow.

Broken down by industry (Figure 24), WZ08 class K companies (Financial and Insurance Activities) with a share of 61.5 % of those insured against information security breaches are far ahead of all other WZ08 classes. This is followed by companies in the Human Health and Social Work Activities (WZ08-Q: 32.7 %) and Other Service Activities (WZ08-S: 24.1 %). There are hardly any correspondingly insured companies in Agriculture, Forestry and Fishing (WZ08-A: 0.0 %). When interpreting these results, however, it is important to bear in mind the different and in some cases very large proportions of those who are unaware of this.

Figure 24 **Companies with cyber insurance according to first level WZ08 classes**
in percent; weighted data; split-half group B



[255] Cf. Klahr et al. (2017).

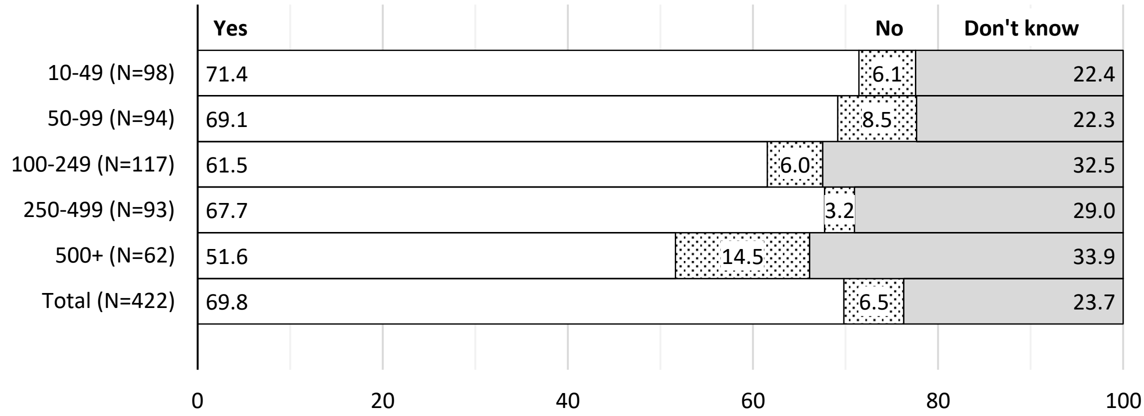
Second-level WZ08 classes whose companies have relatively rarely reported cyber insurance include WZ08-01 (Crop and animal production, hunting and related service activities: 0.0 %), WZ08-16 (Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials: 0.0 %) and WZ08-42 (Civil engineering: 5.3 %). Financial service activities, except insurance and pension funding (WZ08-64: 69.0 %) and human health activities (WZ08-86: 46.9 %), on the other hand, are proportionally more frequently insured, although in the case of health care companies the proportion who did not know whether or not they had cyber insurance is comparatively large (24.5 %).[256]

If cyber insurance was available, they were asked whether they recommended taking out such insurance and whether they had already tried to claim it. Overall, a majority of 69.8 % would recommend cyber insurance, with a further 23.7 % not yet aware of it and only a very small proportion of 6.5 % not recommending it (Figure 25). There are only tendential differences between the employee size classes, but no statistically proven differences: According to this, small companies would recommend taking out cyber insurance more often than large ones (10-49 employees: 71.4 % vs. 51.6 % 500+ employees), although the proportion of those who do not yet know this is larger among large companies than among small ones (500+ employees: 33.9 % vs. 10-49 employees: 22.4 %). In a similar vein, but with the question of whether taking out cyber insurance has so far been worthwhile for the industrial company, Bitkom states that this is not or not at all the case for 61 % of the companies and only 28 % report the opposite. However, the Bitkom study also found that companies with between 10 and 99 employees are more positive about this (48 % very/always paid; 44 % hardly/not paid at all) than companies in other employee size classes.[257]

Figure 25 **Recommendation of cyber insurances by employee size class**

in percent; weighted data; split-half group B with cyber insurance

Would you recommend cyber insurance to others?



The relatively large proportion of undecideds is probably related to the lack of experience in cyber insurance. Only 5.7 % of insured companies (N=424) have ever tried to claim cyber insurance benefits.[258] Eighteen out of 20 companies reported that they had received benefits and

[256] A breakdown of these shares by second level WZ08 classes is given in table 49 in Annex 1.

[257] Cf. Bitkom e.V. (2018).

[258] Klahr et al. (2017) also mention only two of a total of over 1,500 companies surveyed.

13 out of 18 reported that they had covered the entire claim. Due to the small number of cases, however, the significance of these results on the benefits of cyber insurance is very limited.

Table 19 **Reasons for non-insurance**

in percent; weighted data; multiple answers possible; bold: significant at $p<.05$ (Chi² test)

		Employee size class				
Why does your company not have cyber insurance?	Total	10-49	50-99	100-249	250-499	500+
We haven't dealt with this yet	63.0	**63.8**	**59.4**	**60.3**	**57.6**	**41.6**
The price-performance ratio is not right	11.0	10.4	14.2	16.5	14.3	20.8
Other reason	27.6	27.4	27.7	24.7	29.5	39.6
N	1,461	366	310	224	217	101

The companies that did not have cyber insurance were asked for the reasons (Table 19). Almost two thirds said that they had not yet looked into cyber-insurance (63.0 %), one in nine companies said that the price-quality ratio of products tested was not right (11.0 %) and more than a quarter said they had some other reason (27.6 %). The proportion of large companies (500 employees or more) that have not yet dealt with cyber-insurance is, at 41.6 %, significantly smaller than for small companies (10-49 employees). On the other hand, the large companies tended to conclude more often that the price-performance ratio was not right (500 employees and over: 20.8 % vs. 10-49 employees: 10.4 %).

5.5 Interim summary

The examined companies show differences in their IT security structures. About one fifth of the companies with ten or more employees (21.6 %) do not have their own IT staff. The larger the company, the smaller these shares become. Nearly two-fifths of the small companies (10-49 employees) also have no employees in the IT & information security field (38.7 %; N=1,133). If this lack of know-how cannot be compensated for in some other way, e.g. by external service providers, the company may be exposed to increased risks from cyber-attacks. However, the majority (81.4 %) of German companies with more than ten employees appear to resort to outsourcing certain IT functions. For IT security functions, this proportion is around 49 %. As expected, the use of external IT service providers is associated with a small number of in-house IT employees. Larger companies, however, generally have their own IT staff, regardless of whether certain IT functions are outsourced.

With regard to the IT security structures in the companies considered, it is striking that organisational security measures are less common in smaller companies than in larger ones. In addition, there are significant differences within different industries. Companies of general interest have proportionally more frequent certifications in the field of IT security and more frequently conduct IT security training for employees as well as exercises or simulations for the failure of important IT systems than other companies. Questions remain unanswered as to the exact implementation of such organisational measures, i.e. whether there are, for example, regular uses or control loops, etc.

Regarding technical security measures, there is less variance in employee size classes than in organisational security measures. In this respect, there now seem to be certain standards that most companies with ten or more employees at least have in place. In contrast to organisational measures, companies providing companies of general interest also show no statistically relevant differences compared to other companies. What remains open at this point is the quality or degree of maturity with which these technical measures were implemented, whether proper configuration and maintenance takes place and whether the end users adhere to the associated rules of conduct.

In addition to organisational and technical security measures, some of the companies also rely on insurance cover. Including the answer category "don't know", 17.9 % (N=2,460) of the companies have insurance against information security breaches, 62.2 % have none, and in 19.9 % of cases the respondents did not know. Only 5.7 % of the insured companies (N=424) have ever attempted to use cyber insurance services. Companies without such an insurance, most of them stated that they had not yet dealt with the topic (63.0 %)

Since the mere existence of IT security measures without corresponding behavioural patterns or the necessary risk awareness of those affected is unlikely to be very effective, the respondents were asked to provide an assessment for the respective companies. The results of these assessments are presented in the following chapter.

6 ASSESSMENTS OF IT RISKS

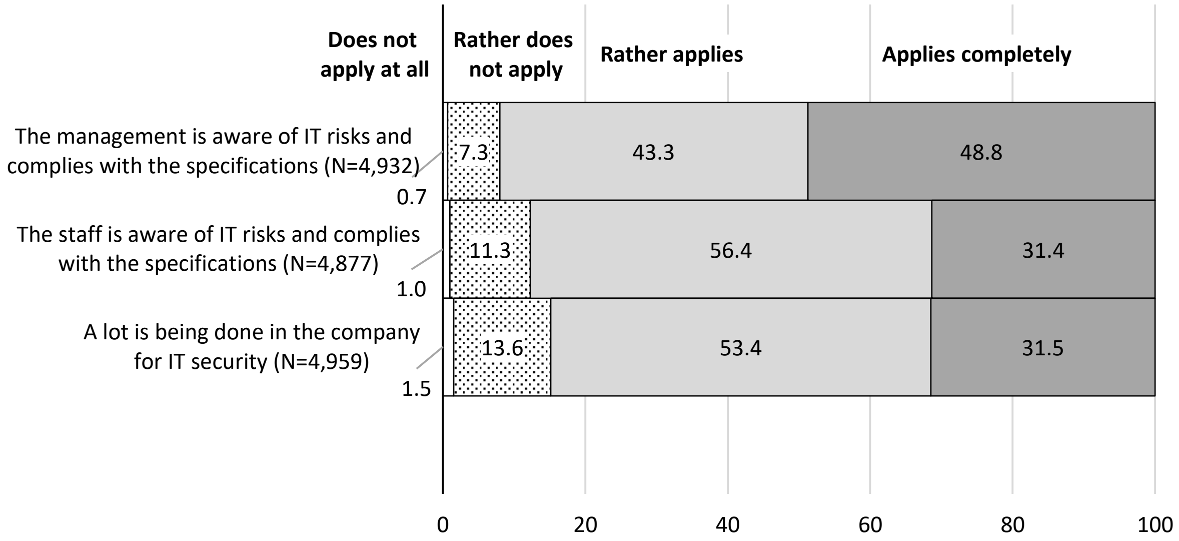
In addition to the existence of IT security measures, risk awareness within the company plays a central role, because above all guidelines and other existing preventive and protective measures must be implemented and lived by management and employees in order to be effective. The participating company representatives were asked to assess both the risk awareness within the company and the risk for the company to suffer a damaging cyber-attack. They were also asked to assess why the company in question could be the target of a cyber-attack. These results can give an indication of the risk awareness within the company, although it remains the assessment of the individual respondent(s).

6.1 Risk awareness within the company

On the subject of risk awareness, the company representatives interviewed were able to rate the following statements on a four-point scale from 1 "Does not apply at all" to 4 "Applies completely": "The management is aware of IT risks and complies with the specifications", "The staff is aware of IT risks and complies with the specifications" and "A lot is being done in the company for IT security ('more than classic protective measures')".

Figure 26

Assessment of risk awareness in the companies
in percent; weighted data



The proportion of respondents who could not agree with the three statements, or rather could not agree at all, is relatively small at 8.0 % with regard to the risk awareness of the management, 12.3 % with regard to the risk awareness of the workforce and 15.2 % with regard to IT security measures in the company (Figure 26). The greatest agreement (43.3 %: "rather applies" and 48.8 %: "applies completely") was given to the statement that the management is aware of IT risks and complies with the corresponding guidelines. This is particularly interesting against the background of the criticism in the literature that cyber security is still not or only to a small extent a "matter for the boss" and therefore a stronger involvement of the management is demanded.[259] It is possible that managing directors are aware of IT risks, but delegate or neglect to deal with the issue despite this.

For further evaluation, an average value index was formed from these three individual aspects.[260]

Table 20 **Assessment of risk awareness in the companies**

in percent; weighted data; bold: differences significant at p<.05 (Chi² test)

		Position within the company			Employee size class				
	Total	Management	IT	Otherwise.	10-49	50-99	100-249	250-499	500+
(Rather) low risk awareness in the company (N=4,797)	8.2	**9.6**	**7.1**	**7.3**	8.4	8.3	7.4	8.1	8.7
To what extent do the following statements apply to your company?	Percentages of answers "Does not apply at all / Rather does not apply".								
The management is aware of IT risks and complies with the specifications (N=4,932)	8.0	**7.0**	**9.2**	**7.3**	7.6	9.5	9.2	10.0	11.2
The staff is aware of IT risks and complies with the specifications (N=4,877)	12.3	**13.0**	**13.1**	**7.2**	**11.6**	**14.4**	**12.8**	**16.7**	**23.3**
A lot is being done in the company for IT security (N=4,959)	15.2	**17.7**	**11.3**	**19.0**	**16.4**	**11.1**	**9.5**	**8.4**	**8.0**

A comparison of the assessed risk awareness within the company between the positions of the responding company representatives[261] reveals relatively small but significant differences (Table 20). Respondents from the management or the board of directors proportionally more frequently state a (rather) low level of risk awareness within the company (9.6 %) than respondents from the IT and information security sector (7.1 %) or other areas (7.3 %) and therefore seem to be more critical. However, this does not apply to all individual aspects of the mean value index: For example, a significantly larger proportion of respondents from the area of IT & information security rather disagrees/does not agree at all with the fact that the management is aware of the risks and complies with guidelines (9.2 %) than respondents from the management itself (7.0 %). According to this, managing directors themselves assess their own IT risk awareness as higher than their IT employees would attribute to them. In relation to the workforce, respondents in other positions are significantly less critical (7.2 %) than the other two groups (Management: 13.0 %; IT: 13.1 %). This could be due, for example, to the fact that they are further away from the topic of IT security in terms of content and thus may come to a milder judgement. More respondents in other positions (19.0 %) and management (17.7 %) are (rather)

[259] Cf. Hillebrand et al. (2017); Georgia Institute of Technology (2016); Bundesamt für Sicherheit in der Informationstechnik (2015); Bitkom e.V. (2018). According to PwC, however, the risk awareness of senior management on this topic is increasing (PricewaterhouseCoopers AG WPG (2017)).

[260] Cronbach's Alpha measure quantifies the extent of the relationship between the individual aspects (items) contained in the index, can assume values between minus infinity and 1 and was used to assess the internal consistency of the index. Cronbach's alpha in this case is 0.72 and indicates a relatively good consistency. The mean values calculated over the three items were then categorised as follows: "low" (1.000-1.749), "rather low" (1.750-2.499), "rather high" (2.500-3.249) and "high" (3.250-4.000).

[261] For the summarized assignment of company representatives, see section 3.4.3.

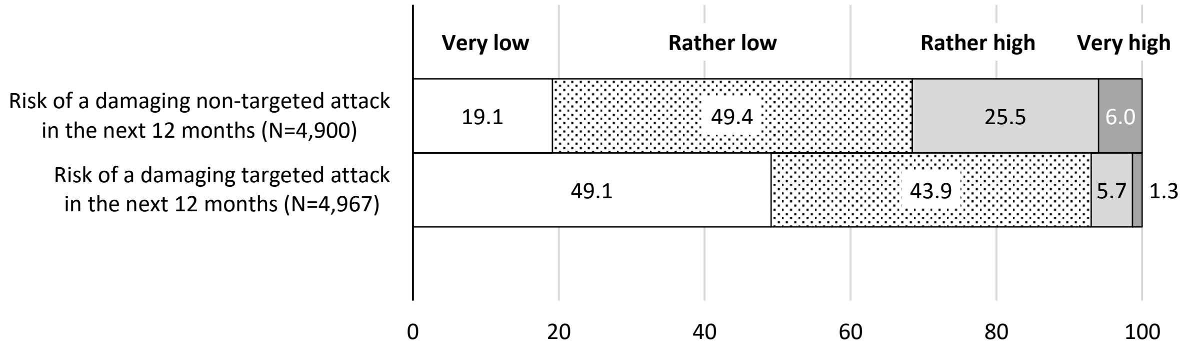
hostile to the statement that a lot is being done in the company for IT security than respondents in IT and information security (11.3 %). At this point it can be assumed that respondents in IT and information security evaluate their own work here and that this is understandably very present or that other groups of employees do not have a complete picture of all security efforts in the company. Where appropriate, greater transparency of existing security measures could help to mitigate the more critical assessments of managers and other employees and thus achieve greater awareness and resilience overall.

Differentiated according to employee size classes, significant differences in response behaviour are noticeable for two individual aspects, which can be explained at least in part by the fact that in larger companies employees from the IT and information security sector were more likely to be surveyed, and in smaller companies management was surveyed more frequently. Nevertheless, it is apparent that the proportion of critical voices is significantly higher among the large companies than among the small ones (500+: 23.3 % vs. 10-49 employees: 11.6 %). With regard to the statement that "a lot is being done in the company for IT security", it is exactly the other way round: here, there are significantly more critical voices in the small companies than in the large ones (10-49 employees: 16.4 % vs. 500+: 8.0 %). This is in line with the general finding in Section 5.3 that more IT security measures are implemented in larger companies, and at the same time indicates that the human factor becomes more important with increasing numbers of employees.

6.2 Assessment of the company risk

In addition to the risk awareness in their company, respondents should assess the risk for their company that it will be damaged in the next twelve months by a cyber-attack that a) hits many other companies at the same time (random attack) and b) hits only their own company (targeted attack). The respondents were also able to make this assessment on a four-level scale from 1 "very low" to 4 "very high".

Figure 27 **Risk assessment for damage to the company through (un)targeted cyber-attacks**
in percent; weighted data



The risk of a targeted cyber-attack in the next twelve months damaging the company is estimated to be even lower than that of a damaging unspecified attack (Figure 27): With a share of 93.0 %, the majority of companies consider the risk of targeted attacks to be very/rather low. Only 68.5 % see this as true for targeted attacks. Almost half (49.1 %) even consider the risk of damage from targeted attacks to be very low, while this proportion is much lower for random attacks (19.1 %).

Table 21 **Risk assessment for damage to the company through (un)targeted cyber-attacks**

in percent; weighted data; bold: differences significant at p<.05 (Chi² test)

How high do you estimate the risk for your company to be damaged by a cyber-attack in the next 12 months, ...	Total	Position within the company			Employee size class				
		Management	IT	Otherwise.	10-49	50-99	100-249	250-499	500+
	Proportion of responses "Very/Rather high								
... which also affects many other companies at the same time? (N=4,900)	31.5	**31.9**	**34.1**	**22.6**	**30.3**	**35.3**	**36.1**	**37.8**	**41.7**
... which only affects your company? (N=4,967)	7.0	**6.3**	**9.0**	**3.6**	**6.6**	**7.7**	**9.4**	**8.6**	**12.4**

A comparison of the risk assessments by position of the respondents within the companies (Table 21) shows that employees in the IT and information security sector in particular differ significantly from employees in other positions: The proportions of those who estimated the risk of damage from a cyber-attack in the next twelve months to be very or rather high are highest among employees in the IT and information security sector (34.1 % and 9.0 %; N=2,043 and 2,067) and lowest among employees in other positions (22.6 % and 3.6 %; N=660 and 676). One possible explanation for this could again be the stronger presence of the topic among employees in IT and information security. At the same time, however, the response behaviour also reflects the lower assessment of the risk awareness of IT employees towards their management.

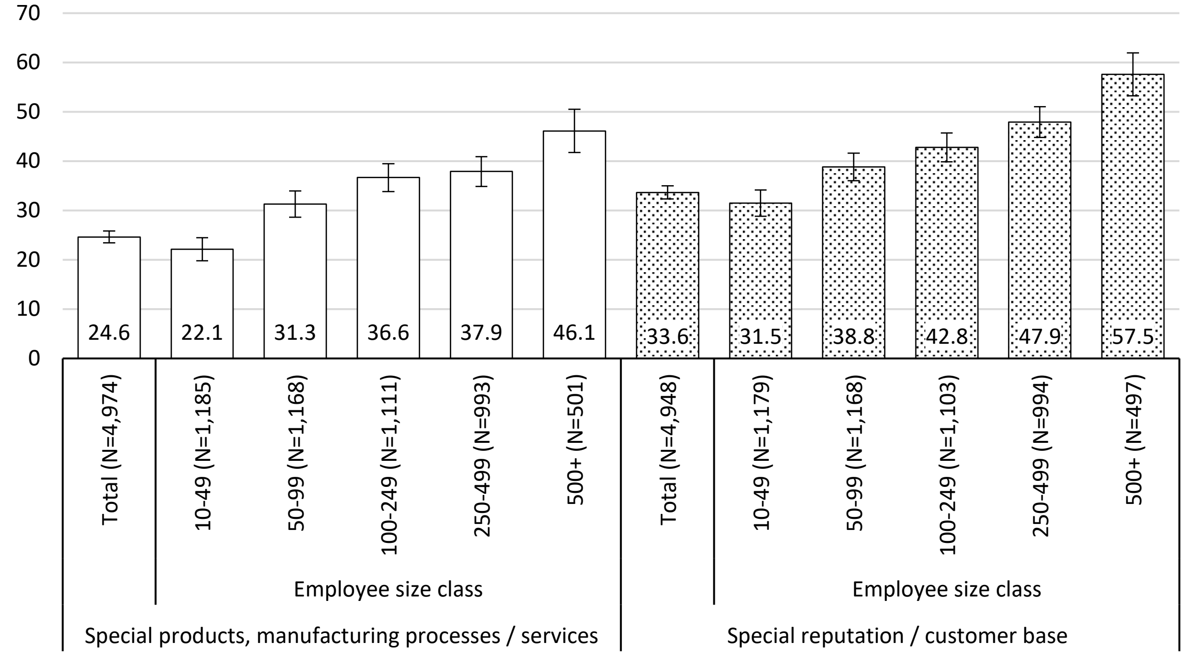
The proportions of the various employee size classes also differ: respondents from small companies were significantly less likely to conclude that the risk of undirected and targeted attacks is very/rather high (10-49 employees: 30.3 % and 6.6 %; N=1,167 and 1,184) than respondents from large companies (500+ employees: 41.7 % and 12.4 %; N=494 and 499). This, in turn, may be at least partially related to the higher proportion of IT and information security employees among the respondents of large companies. Nevertheless, this assessment should not lead smaller companies to the mistaken conclusion that they should protect themselves less or that they would be fewer interesting targets for attacks.

6.3 Potential targets

In connection with the question of why the company could become the target of a cyber-attack, the company representatives had the opportunity to indicate whether or not they had "special products, manufacturing processes or services (e.g. due to special technology, designs, materials, innovations)" and/or a "special reputation/customer base (e.g. high level of awareness, high security standards, special discretion)". The assessment of the "special" nature was deliberately left to the respondents, since an objectified definition is almost impossible to establish across the multitude of different companies and sectors. Rather, the respondents were free to make this assessment in comparison to other companies.

Figure 28 **Potential reasons for a targeted cyber-attack by employee size class**

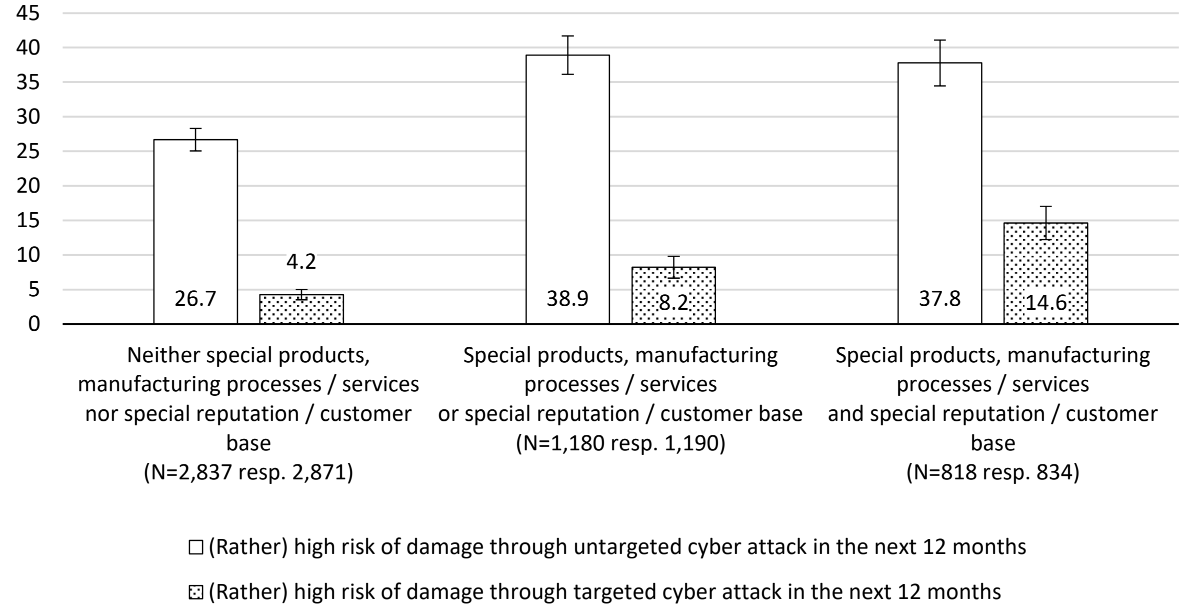
in percent; weighted data; 95 %-CI



About a quarter of the companies have special products, manufacturing processes or services (24.6 %) and a third have a special reputation or customer base (33.6 %) that could make the company a target for individual cyber-attacks (Figure 28). There are significant differences between the employee size classes, according to which large companies in particular are much more likely to have special products etc. and a special reputation/customer base (500+: 46.1 % and 57.5 % respectively) than smaller ones (10-49 employees: 22.1 % and 33.6 % respectively). The proportion of companies that have neither special products, manufacturing processes or services nor a special reputation or customer base is 58.6 % (N=4,927) in total and is significantly higher for small companies than for large ones (10-49 employees: 61.1 %; 500+ Employees: 33.8 %).

Figure 29 shows the proportions of respondents who assess the risk of damage to the company by untargeted or targeted cyber-attacks as (rather) high in the next twelve months, differentiated according to the presence of potential targets. The percentages are significantly lower for companies that have neither special products etc. nor a special reputation/customer base (26.7 % and 4.2 % respectively) than for companies that have either special products etc. or a special reputation/customer base (38.9 % and 8.2 % respectively) or even both (37.8 % and 14.6 % respectively). In other words, companies with potential attack targets estimate the risk of a damaging attack significantly more often (rather) high in the next twelve months. On the one hand, this shows an increased awareness of these particularly exposed companies, and on the other hand it is problematic if companies without these special features weigh themselves in security.

Figure 29 **Risk assessment for damage according to the presence of potential targets**
in percent; weighted data; 95 %-CI



6.4 Sources of information on IT and information security

Information on IT and information security is available from various sources. In addition to state institutions such as the Office for the Protection of the Constitution, the police or the Federal Office for Information Security (BSI), and professional associations and chambers (e.g. IHK, BVMW), e.g. consulting service providers and IT security software manufacturers offer corresponding information. In addition, information can be obtained via own internet research, via technical literature or journals or in any other way (conceivable would be e.g. personal conversations with business partners etc.).

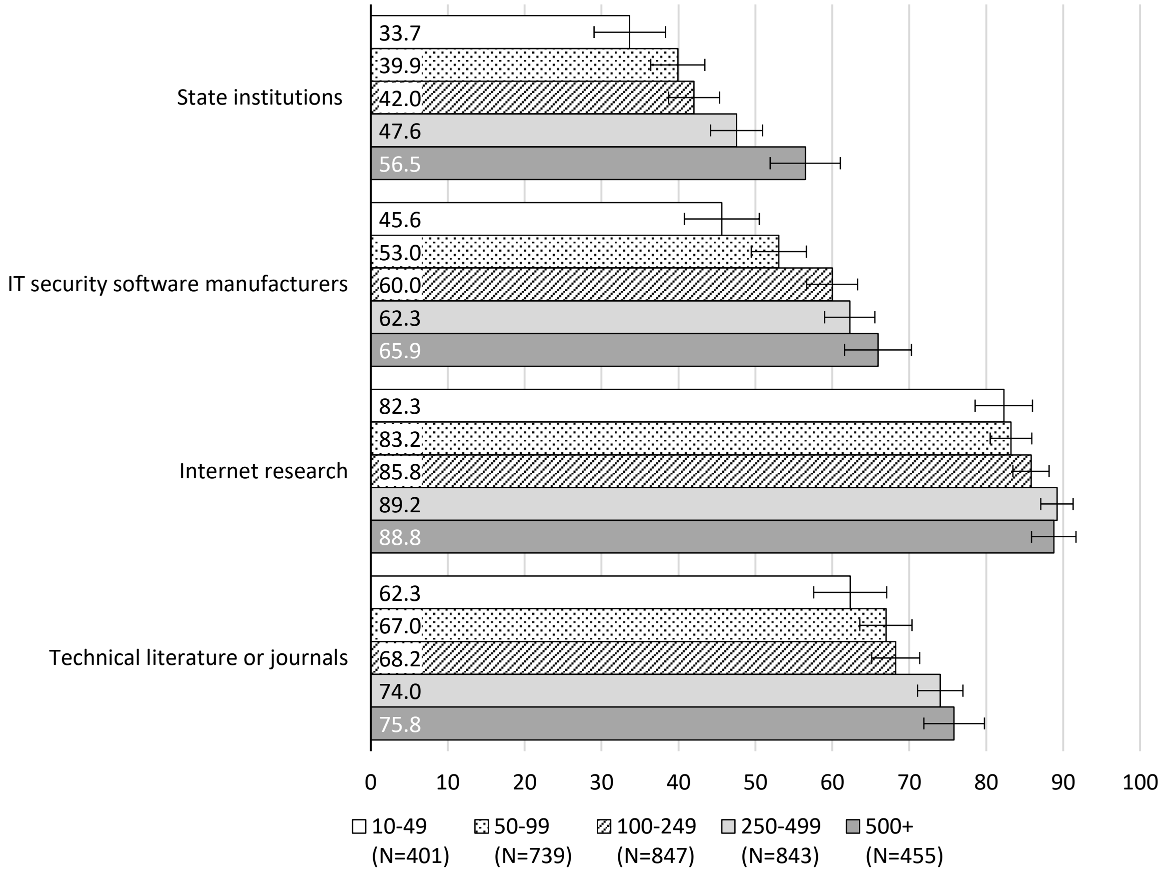
Table 22 **Information sources on IT and information security**
in percent; weighted data; multiple answers possible; bold: differences significant at p<.05 (Chi² test)

Who do you contact to obtain information on IT and information security?		Position within the company			Employee size class				
	Total	Management	IT	Otherwise.	10-49	50-99	100-249	250-499	500+
State institutions (e.g. Office for the Protection of the Constitution, Police, BSI)	23.3	**13.9**	**36.9**	**11.0**	**19.8**	**33.1**	**36.7**	**43.9**	**55.0**
IT security software manufacturers	40.0	**33.9**	**49.7**	**29.2**	**37.1**	**46.5**	**54.8**	**59.2**	**64.9**
Consulting service provider	73.6	**75.1**	**71.0**	**76.9**	73.1	74.7	74.6	75.5	74.9
Professional associations, chambers (e.g. IHK, BVMW)	28.9	**32.7**	**26.7**	**23.7**	29.0	28.7	27.6	28.8	30.4
Internet research	63.3	**49.9**	**83.4**	**44.3**	**59.6**	**73.4**	**79.1**	**84.8**	**87.7**
Technical literature or journals	44.7	**30.5**	**64.8**	**27.9**	**40.7**	**54.9**	**60.7**	**67.7**	**74.7**
Other	12.0	**13.0**	**10.4**	**13.8**	11.9	12.6	12.1	11.5	14.3
N	4,882	2,156	2,067	654	1,159	1,165	1,099	986	500

Consultancy service providers are the most frequently cited source of information overall (Table 22), at 73.6 %, followed by own Internet research (63.3 %), specialist literature and journals (44.7 %) and IT security software manufacturers (40.0 %). Professional associations and chambers (28.9 %) and state institutions (23.3 %) were less frequently used.

For all answer options there are statistically significant differences between the positions of the responding company representatives: IT employees initially inform themselves more frequently about several sources and, in addition to their own Internet research or the information contained in specialist literature and journals, use the information offered by IT security software manufacturers but also by government institutions significantly more frequently than, for example, the management, which in contrast to this more frequently addresses professional associations and chambers and above all consulting service providers. It is also interesting to note that management boards relatively seldom turn to government agencies to obtain information. This indicates that they often do not perceive state authorities as competent contacts, which could also have an impact on their reporting behaviour in the event of a damage.

Figure 30 **Preferred information sources of IT employees by employee size class**
in percent; weighted data; multiple answers possible



A comparison of companies according to employee size classes reveals significant differences with regard to state institutions, IT security software manufacturers, internet research and technical literature/journals as sources of information (Figure 30). Large companies (500+ Employees) use these sources of information much more frequently than small companies (10-49 employees). Against the background that in large companies it was primarily IT employees who responded, these differences are in line with expectations. However, even when the position of the responding company representatives is controlled, these differences between the employee size classes remain, at least in the group of IT employees (Figure 30): IT employees in small companies (10-49 employees) use state institutions, IT security software manufacturers, Internet research and technical literature/journals significantly less frequently for information on the topic of IT and information security than IT employees in large companies (500 employees and over). This difference is particularly clear with regard to state institutions: While one third of IT employees in small companies (10-49 employees: 33.7 %) mention them, the share of IT employees in large companies who do likewise is more than half (56.5 % in companies with 500 employees or more). It could be assumed here that the information and support offered by government agencies is directed more towards larger companies and reaches smaller companies less. Internet research as an information source is dominant in all company size classes.

Overall, it can be seen that the information gathering behaviour of companies on the subject of IT security is differentiated. The choice of the information medium of future knowledge that is appropriate for the addressee therefore seems to play an important role.

6.5 Interim summary

In this chapter it could be shown that companies assess IT risks differently and inform themselves differently about the topic of IT security. It is important to note which person with which function as an individual provides information about the unit of investigation "company". For example, managing directors themselves assess their own IT risk awareness higher than their IT employees would attribute to them. On the other hand, managing directors are more critical than IT employees when it comes to whether much is being done in the company for IT security. This differentiated response behaviour should be monitored in future studies. Company size also plays a role. The proportion of critical voices among large companies with regard to the risk awareness of the workforce is significantly higher than among small companies.

With regard to the statement that "a lot is being done in the company for IT security", it is exactly the other way round: here there are significantly more critical voices in the small companies than in the large ones.

The assessment of the risks to companies from undirected or targeted cyber-attacks in the next 12 months varies widely. Almost all companies (93.0 %) consider the risk of targeted attacks to be very/rather low, while this proportion is much lower for un-targeted attacks (68.5 %). Almost half (49.1 %) even consider the risk of damage from targeted attacks to be very low. For untargeted attacks the percentage is only 19.1 %. Here, too, there are differences in employee size classes. The larger the company, the more frequently both attack variants are assessed. Respondents from small companies came significantly less frequently to the conclusion that the risk of untargeted and targeted attacks is very/rather high.

Specifics were asked with regard to why a company could be attacked specifically. According to the survey, about a quarter of the companies have special products, manufacturing processes or services (24.6 %) and a third have a special reputation or customer base (33.6 %) which could make the company a target for individual cyber-attacks. The larger the company, the higher the proportion of these special features. If the statements on the assessment of the company risk and the potential targets of attack are linked, it is logical to conclude that companies with potential targets of attack assess the risk of a damaging attack significantly more frequently (rather) highly in the next twelve months. On the one hand, this speaks for a functioning awareness of these particularly exposed companies, but conversely it must not mean that companies without these special features can be on the safe side.

Regarding the question of how companies inform themselves about IT security, differences between the sizes of companies as well as the functions of the respondents could be shown. Managing directors show the highest shares of information gathering by consulting service providers, while IT employees obtain the highest share of information on the Internet. Larger companies, for example, make significantly more frequent use of information provided by government agencies than smaller ones. All in all, it can be seen that the information gathering behaviour of companies on the topic of IT security is differentiated and should be taken into account in future publication campaigns.

7 CYBER-ATTACKS AGAINST COMPANIES

One of the difficulties in assessing the impact of cyber-attacks is that a cyber-attack can be carried out in a variety of ways and as a combination of different types of attacks, targeted at a specific company or untargeted, e.g. via malware distributed on a massive scale. In addition, many cyber-attacks can damage the affected company even before the perpetrators have reached their targets, for example if IT clientsare down, working time has to be invested to defend against an acute attack, etc.

Without claiming to cover all possibilities completely, the following types of attack were distinguished within the survey:[262] ransomware, spyware, other malware, manual hacking, (D)DoS, defacing, CEO fraud and phishing. This less technical and relatively broad classification was chosen for two reasons. Firstly, to be independent of specific attack vectors, techniques and tools and affected domains or systems or data,[263] which can change over time.[264] On the other hand, in order to promote comprehensibility and acceptance among the respondents as well as to do justice to the limited possibility of the complexity of a telephone interview.

1) In a ransomware attack, a malware program is used to encrypt the data of infected computers or networks and thus make them unusable for the users. This is often associated with ransom blackmail, as the decryption is linked to the payment of the requested amount (usually in the form of a crypto currency such as Bitcoin or Monero). Whether the release code is sent after the ransom has been paid remains uncertain.
2) Spyware is a term used to describe programs that are used for spying and are designed to identify and extract internal company data as undetected as possible. This type of attack can be used, for example, for product espionage or to prepare other cyber-attacks (see e.g. CEO Fraud).
3) Other malware includes attacks with damaging or "malicious" software such as viruses, worms, Trojans, rootkits, scareware etc. Since the range of malicious programs, their possible variation and combination is constantly increasing and a valid delimitation hardly seems possible, we only record malware attacks collectively, with the exception of ransomware and spyware.
4) Manual hacking stands for unauthorized manipulation or configuration of hardware and software settings of computers without the use of malicious programs (malware). The aim of an unauthorized hacker (sometimes also called cracker or blackhat) could be, for example, to gain illegitimate access to company data, to steal it, to sabotage companies or to prepare another cyber-attack.

[262] The classification of the attack types was created by the project team after reviewing the literature and discussions with the project's own regional company headquarters, taking into account the quality criteria of exhaustion (each attack type can be assigned to one category) and exclusivity (each attack type can only be assigned to one category).

[263] From the point of view of this study, the impact on systems and data does not represent a type of attack, but rather the consequence of an attack and is therefore presented as consequences in chapter 9. 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.

[264] A similar approach was chosen by Paoli et al. (2018).

5) A Denial of Service or short DoS attack targets web or e-mail servers of companies that are to be overloaded with mass requests or e-mail shipments and thus are no longer available for regular operation. If this attack is carried out by combining the computing power of several distributed IT systems in order to overcome protective measures, this is known as a Distributed Denial of Service or DDoS attack. Such an attack can, for example, be aimed at sabotaging companies by temporarily interrupting their operations and/or be associated with blackmail.
6) Defacing attacks include unauthorised manipulation of the contents of the website or entire company websites. These can serve e.g. to sabotage or to gain attention for political or religious reasons, or they can be a publicly visible demonstration of the attacker's abilities. It is also possible to infiltrate malware or deceive visitors to the website in order to intercept personal data.
7) CEO fraud is a form of fraud in which a false identity of a person authorized to issue instructions, e.g. the CEO (Chief Executive Officer), is used to induce other employees to take certain actions, usually by means of fake e-mails. This type of attack has the aim of deceiving or manipulating people and is often referred to as social engineering. It can be, for example, a supposedly urgent financial transaction to conclude a secret deal or the diversion of a regular transaction to another account. Social engineering can also be used to obtain the release of sensitive information. This type of attack is often well prepared and exploits internal company information, e.g. about certain business and communication processes, people involved and their absences, which may also originate from other cyber-attacks.
8) Phishing attacks against companies are aimed at gaining access to sensitive company data, e.g. access data, passwords, bank account or credit card data. To this end, manipulated or forged e-mails are often used to deceive employees into disclosing these data. Knowledge of such data opens many other possibilities of attack for perpetrators, e.g. manipulation and redirection of transaction processes or identity theft to deceive third parties (see CEO fraud attack).
9) Other types of attacks were recorded as free text in the questions on lifetime prevalence and the most severe attack of the last 12 months and then, where possible, assigned to the above-mentioned types of attacks or were considered as missing answers.

As already indicated, these types of attacks can be combined with each other within an attack or carried out step by step. For example, information from a phishing or spyware attack can be used to prepare and execute a CEO fraud attack. If an experienced cyber-attack consisted of multiple attack types and there was evidence of these, the combined or linked attack types should still be reported separately. Thus, the results reported below refer to the types of attacks experienced, whether or not they were related in any way.[265]

[265] Whether different types of attack are part of a coherent cyber-attack could at best be determined by forensic investigation.

7.1 Rate of prevalence

For each type of attack, it was first asked how often the company was affected. This was to include all attacks to which the company had to actively react to, e.g. by taking measures. Attacks that were automatically foiled due to existing IT security structures, for example by filtering out e-mails with damaging software, were not taken into account.[266] The prevalence rate calculated on the basis of this information indicates the proportion of companies that have had experience of at least one cyber-attack that required a response within a defined period (in the last twelve months or ever).

7.1.1 Total cyber-attacks

In total, two-fifths (41.1 %; N=4,981) of the companies stated that they had been affected by at least one of the types of attack surveyed in the last twelve months (Figure 31). More than half of them (57.2 %) have experienced several different types of attack. A direct comparison with corresponding results from other studies is difficult to make. In addition to other results presented in Section 2.4.3, the annual prevalences are partly below and partly above the figures given in this study (e.g. for Belgian companies in 2018: 66.5 %[267] and for German companies in 2018: 33 %.[268]). As mentioned in Section 2.3, the reasons for this may be, in addition to different samples, in particular the different definitions of a cyber-attack.

Those companies that had not experienced any of the cyber-attacks inquired about in the past year were asked whether they had ever been affected by them. Together with the annual prevalence data, a "lifetime prevalence" for companies[269] can be calculated, according to which about two-thirds of companies (65.0 %) have ever been hit by at least one cyber-attack requiring a response.

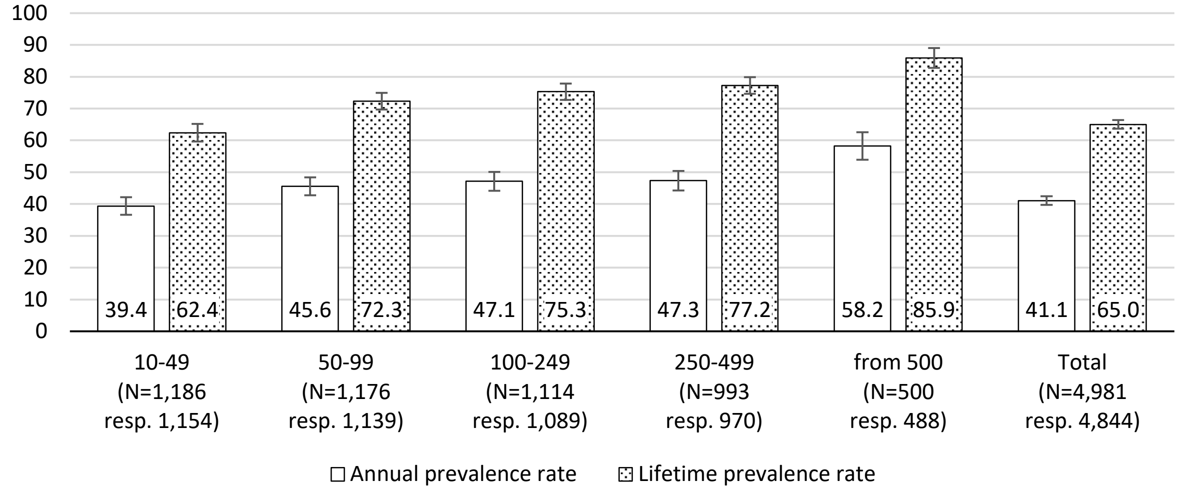
[266] The question was: "Always related to the last 12 months: How often was your company affected by the following types of attacks and had to react?" In addition to naming the type of attack, it was briefly explained: "Ransomware, which had the goal of encrypting company data", "Spyware, which had the goal of spying on user activities or other data", "Other malware - e.g. viruses, worms or Trojans", "Manual hacking, i.e. manipulation of hardware and software without the use of specific malware", "Denial of Service ((D)DoS) attacks, which aimed to overload web or email servers", "Defacing attacks, which aimed to modify unauthorized company web content", "CEO fraud, in which a company executive was faked in order to cause certain actions by employees" and "Phishing, in which employees were fooled with real-looking emails or web pages in order to obtain e.g. sensitive company data".

[267] Cf. Paoli et al. (2018).

[268] Cf. Bundesamt für Sicherheit in der Informationstechnik (2019b).

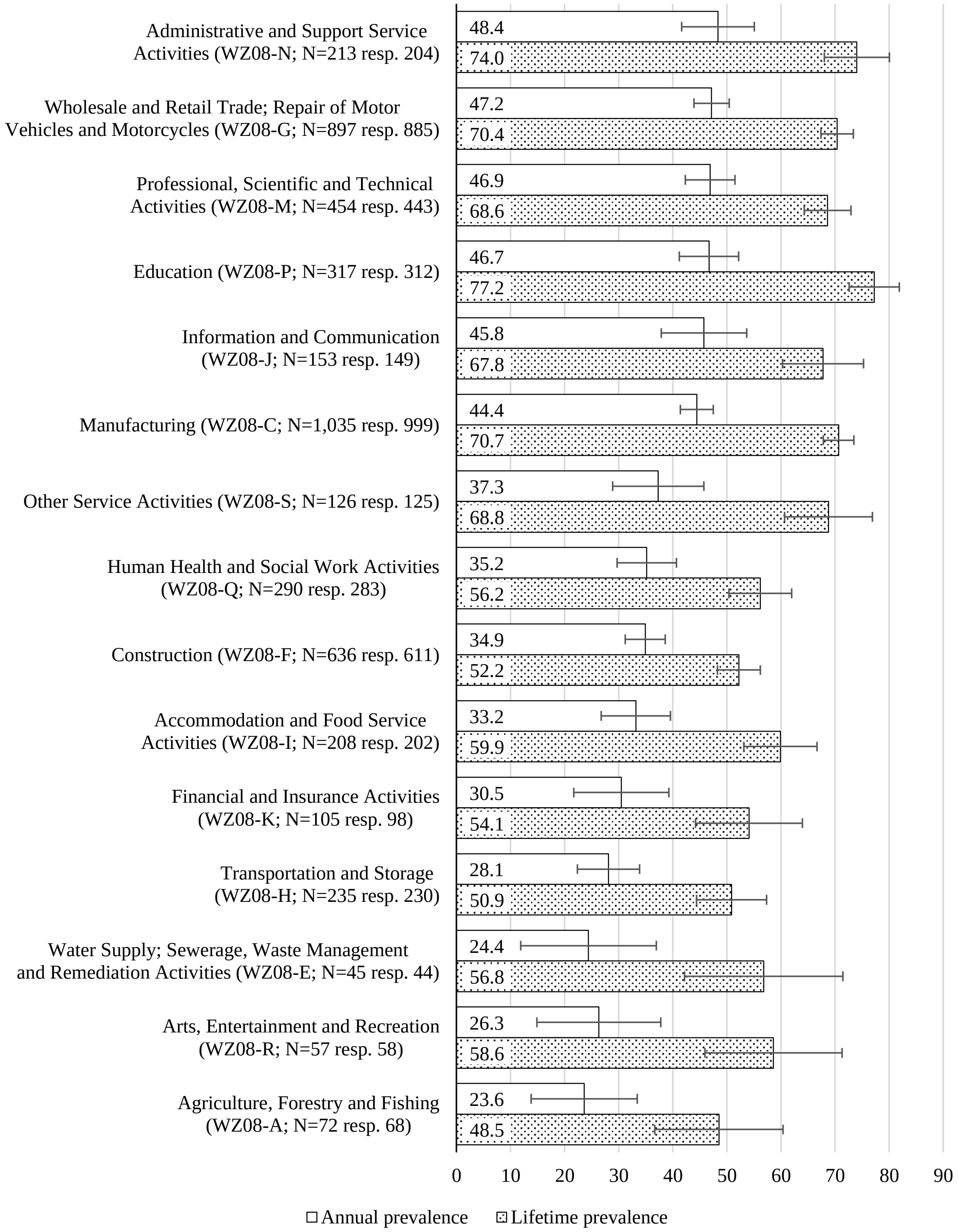
[269] The result of lifetime prevalence is probably still underestimated here, as the interviewed representatives, who also work for the company for different lengths of time, may remember events that occurred longer ago, in particular, less well or not at all than, for example, personal events.

Figure 31 **Total prevalence rates of cyber-attacks by employee size class**
in percent; weighted data; 95 %-CI



When broken down by size class of company (Figure 31), it can be seen that companies with 10 to 49 employees have a statistically significantly lower annual prevalence rate (39,4 %) than all others. In contrast, companies with 500 or more employees have a significantly higher prevalence rate than all others (58.2 %). The differences between companies in the other size classes of employment (50-99, 100-249 and 250-499) are not statistically significant and may be random. A similar picture emerges with regard to the 'lifetime prevalence' of companies. Here, too, a tendential increase can be seen as the number of employees increases, with statistically significant differences between the proportions of small and very large companies (10-49 employees: 62.4 % vs. 500 employees and over: 85.9) and those of the other employee size classes. One hypothesis for this observation would be that larger companies are supposedly more reliable in detecting and subsequently reporting attacks than smaller companies, which are less likely to detect cyber-attacks, due to a higher degree of maturity in the area of IT security and the greater use of resources. According to this hypothesis, the absolute number of non-registered crimes, that cannot be fully investigated by research, is larger for small companies than for large ones. However, this explanation cannot be applied equally to all types of attack, since, for example, ransomware, defacing and CEO fraud attacks (the latter at least after a certain time) are almost always detected due to their obvious consequences.

Figure 32 **Total prevalence rates for cyber-attacks by first-level WZ08 classes**
in percent; weighted data; 95 % CI; only if N≥30



A comparison of the annual and lifetime prevalence rates of individual sectors at the first level of the WZ08 classification (Figure 32) shows that more heavily burdened economic sectors such as wholesale and retail trade; repair of motor vehicles and motorcycles (WZ08-G: 47.2 % annual prevalence and 70.4 % lifetime prevalence), professional, scientific and technical activities (WZ08-M: 46.9 % and 68.6 %), education (WZ08-P: 46.7 % and 77.2 % respectively) or manufacturing (WZ08-C: 44.4 % and 70.7 % respectively), while less burdened sectors such as human health and social work activities (WZ08-Q: 35.2 % and 56.2 %), construction (WZ08-F: 34.9 % and 52.2 %), accommodation and food service activities (WZ08-I: 33.2 % and 59.9 %) and transportation and storage (WZ08-H: 28.1 % and 50.9 %).

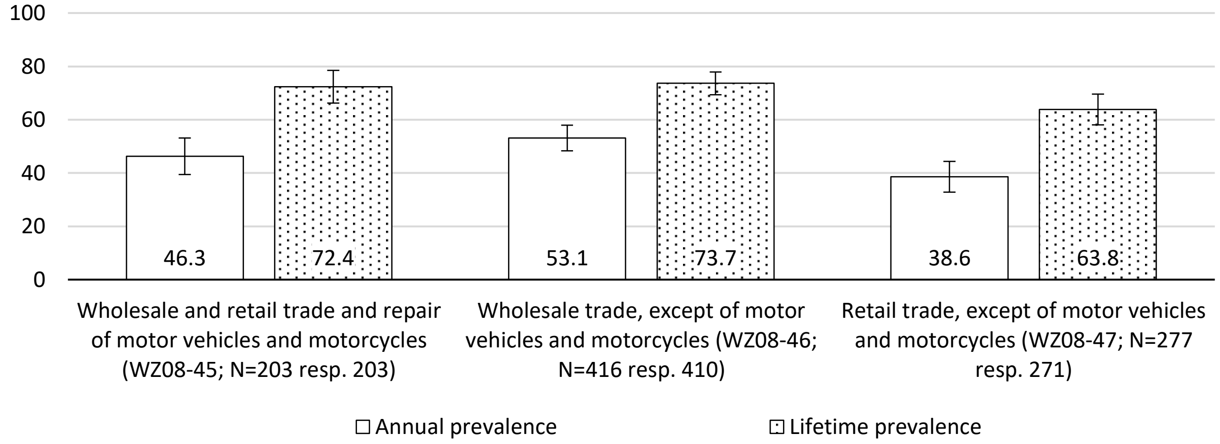
The differences between the WZ08 classes could partly be explained by different distributions according to employee size classes, e.g. in so far as industries with rather smaller companies are less affected by cyber-attacks than industries with larger companies. In order to verify this, Table 23 compares the prevalence of companies in the construction sector (WZ08-F) and the wholesale and retail trade; repair of motor vehicles and motorcycles (WZ08-G) in the respective employee size classes.

Table 23 **Total prevalence rates of cyber-attacks by employee size class and industry**
in percent; bold: significant at p<.05 (Chi² test)

	Annual prevalence rate		Lifetime prevalence rate	
Employee size class	Construction (WZ08-F)	Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles (WZ08-G)	Construction (WZ08-F)	Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles (WZ08-G)
10-49	**34.2** (N=120)	**46.0** (N=163)	**51.3** (N=115)	**68.9** (N=161)
50-99	43.1 (N=72)	53.2 (N=173)	**59.2** (N=71)	**77.8** (N=167)
100-249	**35.4** (N=65)	**53.3** (N=137)	**62.5** (N=64)	**78.8** (N=137)
250-499	45.9 (N=37)	50.5 (N=91)	62.9 (N=35)	77.3 (N=88)
500+	9/13	55.3 (N=38)	13/13	79.5 (N=39)

This shows that differences in both annual and lifetime prevalence rates tend to persist, at least between the two economic sectors in the respective size classes of employment. Statistically significant differences between the two economic sectors are found in companies with between 10 and 49 employees, between 100 and 249 employees and, with regard to lifetime prevalence, between 50 and 99 employees. The result that companies in the construction sector (WZ08-F) are less affected by cyber-attacks overall than companies in the wholesale and retail trade; repair of motor vehicles and motorcycles (WZ08-G) cannot be fully explained by the different sizes of companies in the economic sectors.

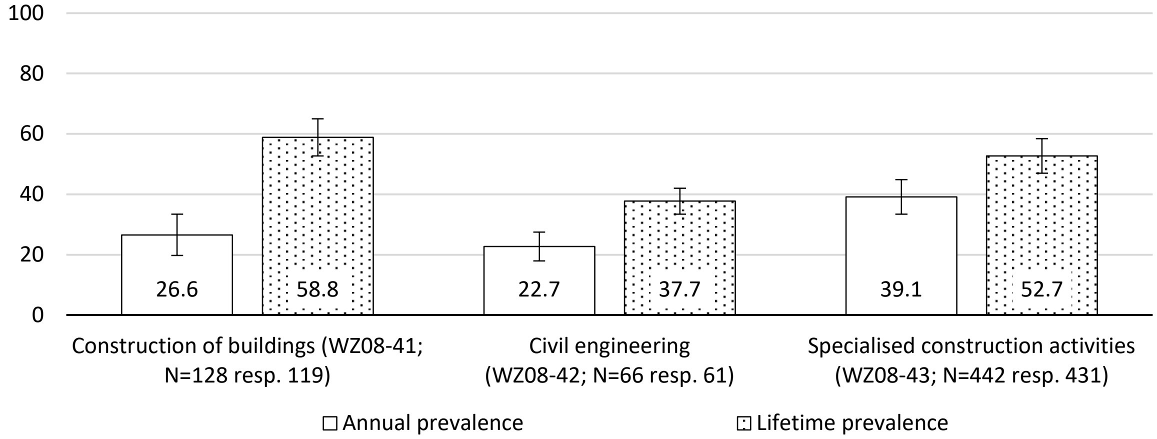
Figure 33 Prevalence rates for cyber-attacks in total within retail sector, maintenance/repair of motor vehicles (WZ08-G)
in percent; weighted data; 95 %-CI



Using the example of companies in wholesale and retail trade; repair of motor vehicles and motorcycles (WZ08-G), it can be shown that it is also possible within one economic sector, i.e.

the retail trade, except of motor vehicles and motorcycles (WZ08-47) has been significantly less affected by cyber-attacks in the past twelve months (38.6 %) and beyond (63.8 %) than the wholesale trade, except of motor vehicles and motorcycles (WZ08-46: 53.1 % and 73.7 % respectively), which only tends to differ from the wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45: 46.3 % and 72.4 % respectively).

Figure 34 **Prevalence rates for cyber-attacks in total within Construction (WZ08-F)**
in percent; weighted data; 95 %-CI

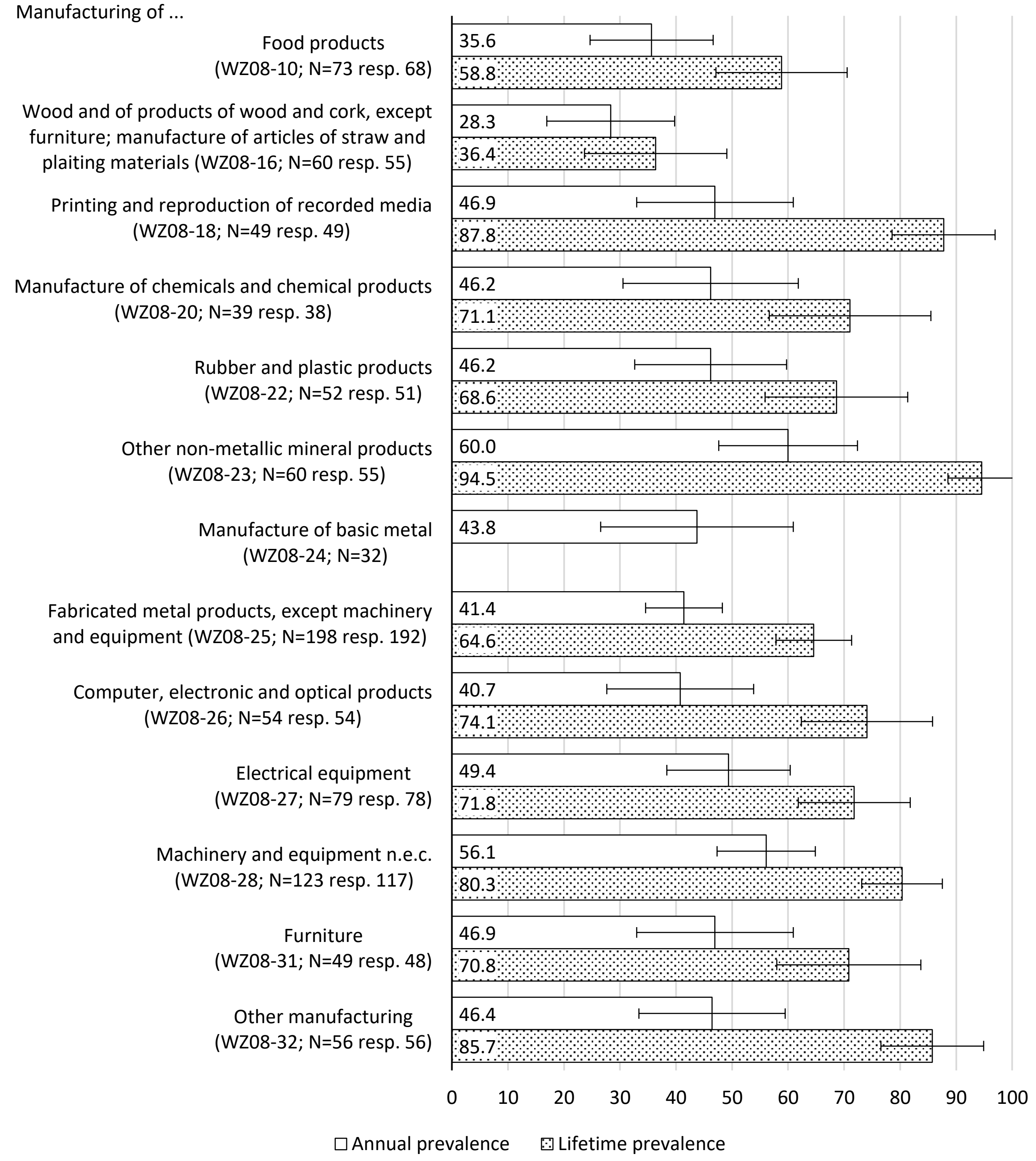


Statistically significant differences can also be seen within manufacturing (WZ08-C) in Figure 34: Companies for specialised construction activities have a statistically significant higher annual prevalence (39.1 %) than civil engineering and building construction companies (22.7 % and 26.6 % respectively). Compared to civil engineering companies, this also applies to the "lifetime prevalence" (52.7 % vs. 37.7 %).

At the second level of the WZ classification, the manufacturing industry is divided into 24 subclasses, some of which are not occupied in the number of cases necessary for comparison. Therefore, only subclasses with at least 30 valid answers are shown in the Figure 35: The annual prevalence of cyber-attacks overall ranges from 28.3 % for companies engaged in the Manufacturing of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials; WZ08-16) to a share of 60.0 % for companies engaged in the manufacture of other non-metallic mineral products (WZ08-23). These two sub-classes also have the lowest and highest 'lifetime prevalence' (36.4 % vs. 94.5 %). The subclasses with the highest prevalence are manufacture of machinery and (WZ08-28: 56.1 % and 80.3 % respectively)manufactures of electrical equipment (WZ08-27: 49.4 % and 71.8 % respectively).[270]

[270] Due to very different industry definitions together with inconsistent definitions of cyber-attacks in the literature studies considered, it is hardly possible to make meaningful comparisons at this point.

Figure 35 **Prevalence rates for cyber-attacks in total within Manufacturing (WZ08-C)**
in percent[271]; weighted data; 95 %-CI



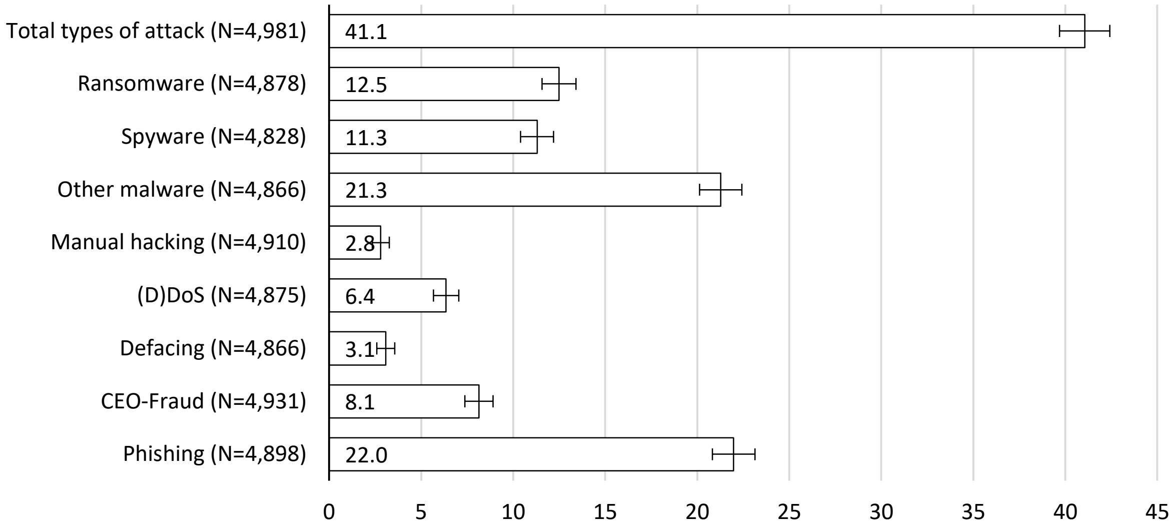
7.1.2 *Cyber-attacks by attack type*

In addition to differentiating between employee size classes and sectoral affiliation, the prevalences[272] can also be compared in terms of the type of attack (Figure 36).

[271] Subcategories with a case number smaller than 30 are not shown. The results for other WZ subcategories that meet this criterion are given in Table 50 in Annex 1.

[272] In the following, only annual prevalences will be presented, since "lifetime prevalence" was not surveyed differentiated by type of attack.

Figure 36 **Annual prevalence rates by type of attack**
in percent; weighted data; 95 %-CI



A large proportion of companies were hit by malware attacks: 12.5 % reported having experienced at least one ransomware attack, 11.3 % one spyware attack and 21.3 % one other malware attack in the last twelve months. More than one-fifth of companies had to respond to at least one phishing attack. One in twelve companies (8.1 %) was affected by CEO Fraud, one in sixteen companies (6.4 %) by (D)DoS attacks. With shares of 3.1 % and 2.8 % affected companies, the attack types defacing, and manual hacking played a comparatively minor role in terms of distribution.

The comparison with results of other studies is only possible to a very limited extent. Despite possible leeway in the definition of what is affected, e.g. ransomware, (D)DoS and malware attacks can be compared approximately due to their generally clearer demarcations. For example, in a survey from 2016, the BSI reports that 32 % of the companies surveyed were infected by ransomware in the last six months.[273] Reasons for these high deviations can be, in addition to different methodological approaches to sampling[274], also technological developments that may have protected companies more reliably from ransomware attacks in recent years. There are also high deviations from the current BSI cyber security survey with regard to (D)DoS attacks. Here the BSI reports shares of 18 %, around three times higher than in the present study.[275] Here too, the reasons for this are probably mainly due to the type of sampling. Klahr et al. come to similar conclusions in their representative study for British companies, however. Malware or spyware attacks are given a total of 33 % (here together 32.6 %) and ransomware attacks 17 % (here 12.5 %).[276]

[273] Cf. Bundesamt für Sicherheit in der Informationstechnik (2016).

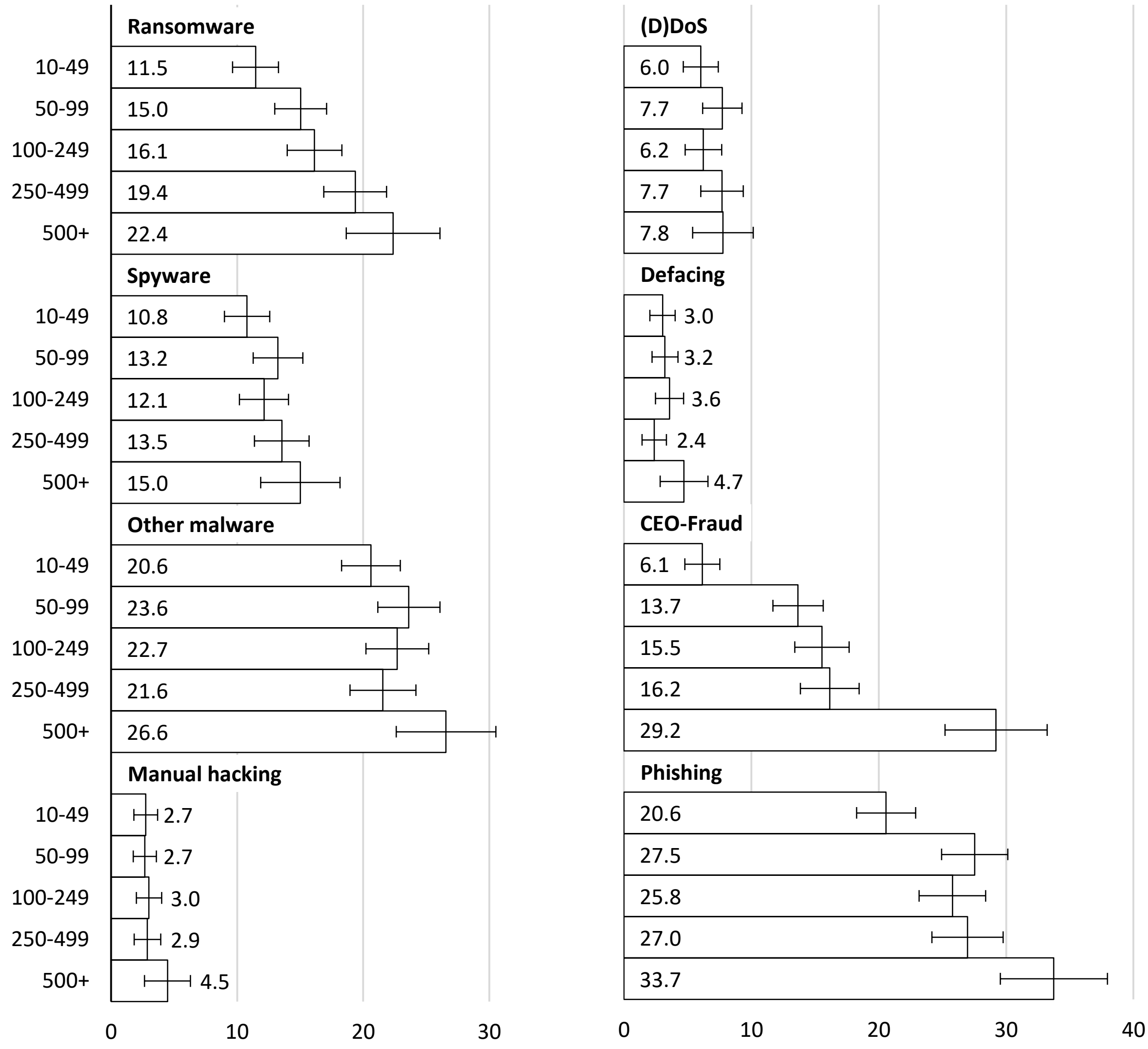
[274] For example, samples in which the participants recruit themselves do not allow any conclusions to be drawn about the population and largely rule out comparison with other studies.

[275] Cf. Bundesamt für Sicherheit in der Informationstechnik (2019b).

[276] Cf. Klahr et al. (2017).

As already shown in Figure 31, in terms of cyber-attacks, large companies (500+ employees) are much more affected than small companies (10-49 employees). When differentiating between the individual types of attack, it becomes apparent that there are not always significant differences between the employee size classes (Figure 37).

Figure 37 **Annual prevalence rates by type of attack and employee size class**
in percent; weighted data; 95 %-CI; multiple answers possible



With regard to manual hacking, (D)DoS attacks and defacing, there are at most tendential differences between small and large companies. On the other hand, the prevalence of ransomware attacks, CEO fraud and phishing differ significantly. This is surprising because these are types of attacks which, unlike spyware attacks or manual hacking, for example, quickly become apparent as a result. An obvious explanation, that large companies may detect more attacks than smaller companies due to greater resource input in the area of IT security, hardly applies to these attack types. Instead, there are indications that large companies probably offer a greater attack surface, especially for untargeted cyber-attacks, due to their higher presence on the Internet and their more extensive IT infrastructure and higher number of IT users.

In ransomware attacks, a linear increase in the prevalence rate is seen with increasing company size. While only about every ninth small company (10-49 employees: 11.5 %; N=1,161) was affected by at least one ransomware attack in the past twelve months, every fourth to fifth large company (500+ Employees: 22.4 %; N=483) was affected. One conceivable explanation here is that e-mails as typical infection paths for ransomware (e.g. applications, invitations, etc.) are received less by smaller companies in purely quantitative terms, the number of potential senders is more manageable, and they are better known. For this reason, fake e-mails may be better identified as such in small companies.

An even clearer difference between small and large companies can be seen in the CEO Fraud: 6.1 % of small (10-49 employees) but 29.2 % of large companies (500+ Employees) had to react to one or more such attacks within one year. In addition to a larger internet presence and a larger target area, more complex organisational structures could be cited as an explanation for the significantly greater impact on large companies, in so far as the associated unclear work processes, unclear responsibilities and major communication problems, as well as the anonymity among employees, which increases with the size of the company, can be exploited by the perpetrators.

Phishing attacks in the previous twelve months affected one fifth of small businesses (10-49 employees: 20.6 %) and one third of large businesses (500+ Employees: 33.7 %).

In addition to the employee size class, the WZ class affiliation could also be related to the exposure to different types of attacks. In this respect, the shading in Table 24 shows that some WZ08 classes are more heavily burdened by certain types of attack at the first level than others: For example, Manufacturing (WZ08-C) is most affected by phishing (28.0 %), but also and above all by ransomware (14.5 %), spyware (12.8 %) and other malware (22.6 %).

Table 24 shows that within the WZ08 classes there are tendencies to differ in the degree to which they are affected by certain types of attack. While the majority of the WZ08 classes are mostly affected by other malware and phishing, Agriculture, Forestry, Fishing, Arts, Entertainment and Recreation were most frequently affected by ransomware attacks.

Furthermore, it is noticeable that in the WZ08 classes P: education and M: professional, scientific and technical activities two types of attack occurred most frequently. In addition, these two WZ08 classes also contain a relatively large number of grey shaded cells (five largest shares per attack type), which indicates a comparatively high general vulnerability of these economic sectors to cyber-attacks.

Table 24 **Annual prevalence rates for cyber-attacks by type of attack and WZ08 classes**
in percent; weighted data

	Cyber-attack type							
WZ08 class (level 1)[277]	1	2	3	4	5	6	7	8
Agriculture, Forestry and Fishing (WZ08-A)	13.7	6.8	8.3	0.0	7.4	0.0	1.4	8.3
Manufacturing (WZ08-C)	14.5	12.8	22.6	2.1	6.5	3.4	8.3	**28.0**
Water Supply; Sewerage, Waste Management and Remediation Activities (WZ08-E)	8.9	7.0	13.3	0.0	4.7	2.3	6.8	11.4
Construction (WZ08-F)	9.9	9.8	20.9	1.7	3.4	0.8	4.9	18.1
Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles (WZ08-G)	14.5	13.3	24.2	5.2	5.0	3.1	9.5	22.8
Transportation and Storage (WZ08-H)	8.7	6.6	13.5	1.7	4.3	3.0	6.9	13.9
Accommodation and Food Service Activities (WZ08-I)	10.6	12.6	20.6	3.4	7.0	3.4	3.9	19.3
Information and Communication (WZ08-J)	6.7	6.7	25.0	1.3	**18.8**	4.0	5.3	24.3
Financial and Insurance Activities (WZ08-K)	4.8	8.7	16.5	0.0	2.9	1.0	5.8	22.0
Real Estate Activities (WZ08-L)	12.5	8.8	15.2	1.2	8.8	3.7	12.2	25.0
Professional, Scientific and Technical Activities (WZ08-M)	15.7	10.5	**25.2**	**5.3**	10.0	4.3	7.3	23.5
Administrative and Support Service Activities. (WZ08-N)	9.1	12.4	20.7	2.9	5.8	2.5	**17.0**	27.8
Education (WZ08-P)	**16.4**	**14.8**	21.7	2.6	8.3	5.0	7.4	16.8
Human Health and Social Work Activities (WZ08-Q)	11.8	11.7	20.9	2.1	4.2	**6.0**	12.5	23.0
Arts, Entertainment and Recreation (WZ08-R)	14.5	7.0	13.8	0.0	1.7	1.8	3.4	6.9
Other Service Activities. (WZ08-S)	3.2	5.9	16.5	0.8	8.3	0.0	12.0	19.0

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing
Highlighting: bold: largest share per type of attack; Gray background: the five largest shares per type of attack; underlined: largest share per WZ08 class

7.1.3 Threat of cyber-attacks

The companies, both affected and not affected, were asked whether they had at least been actively threatened by an attacker with one of the types of attack mentioned in the last twelve months. This was affirmed by 3.9 % (N=4,982). For 44.1 % of the companies that were threatened with a cyber-attack (N=197), the threat remained the same: they did not experience a cyber-attack during the same period.[278]

7.1.4 Non-affected companies

Companies that have not experienced a cyber-attack in the last twelve months were asked how likely they considered it was that a cyber-attack had occurred that just went unnoticed. About a third (31.1 %, N=2,876) consider this to be very unlikely and over half (57.3 %) consider it to be rather unlikely. In contrast, one in ten companies (9.8 %) considers this scenario more

[277] Classes with a case number smaller than 30 are not listed.

[278] A proportion of 55.9% (N=197) experienced at least one cyber-attack, although the survey leaves it unclear whether the threatened attack was implemented or whether another attack was experienced during the same period without a previous threat. With regard to the most severe attack, however, the question of the threat was raised again.

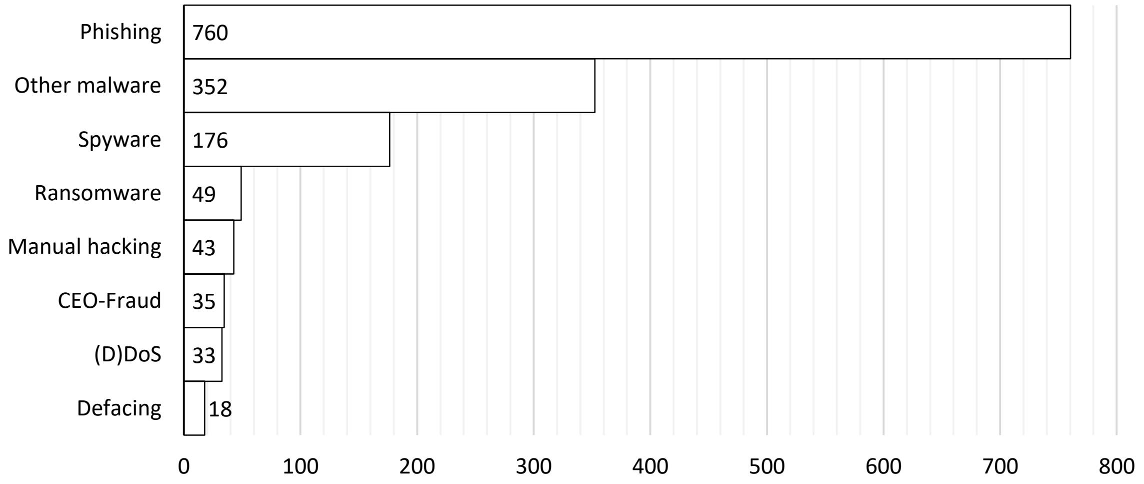
likely and a very small proportion of 1.9 % considers it very likely. The proportion of companies that consider this rather/very likely is significantly lower among those who have never experienced a cyber-attack (7.8 %, N=1,643) than among those who have been attacked at least once before the last twelve months (17.4 %, N=1,092). This indicates that risk awareness is higher among companies already affected than among those not yet affected. No other statistically significant differences in this assessment can be identified either with regard to the positions of the responding company representatives or between companies of different employee size classes.

7.2 Rate of incidence

In addition to stating whether the surveyed companies were affected by the respective type of attack at least once in the previous twelve months (prevalence), the number of cyber-attacks to which they had to respond during this period was also collected.[279] The total number of events reported by the companies for this period constitutes the so-called incidence, and the relative number of events per 100 companies constitutes the incidence rate. For example, in the last twelve months, 100 companies experienced 760 phishing attacks, 352 attacks with other malware and 176 spyware attacks, but only 49 ransomware attacks to which they had to respond (Figure 38).

Figure 38 **Incidence rates by type of attack**

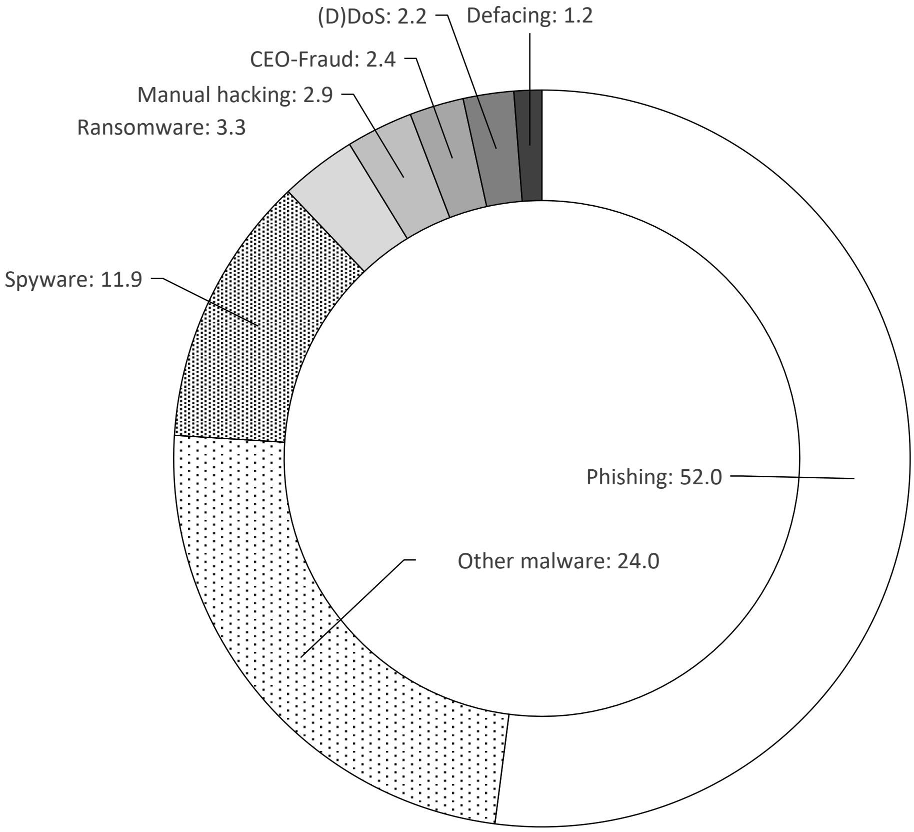
Number of cyber-attacks per 100 companies in the last 12 months; weighted data



In addition, the events summed up for each type of attack can be put in relation to the total number of all reported cyber-attacks (Figure 39). Both the incidence rates and the proportions of each type of attack in all reported cyber-attacks show a change in ranking from the annual prevalence rates (Figure 36).

[279] In order to reduce the influence of extreme values in the following evaluation, these were reset for the respective type of attack to a value calculated from the mean value added with three standard deviations (for companies from 500 employees: mean value added with four standard deviations). The difference in the calculation of the upper limit between large companies (500 incidents or more) and all others is due to the higher theoretically possible number of incidents in very large companies.

Figure 39 **Proportion of cyber-attacks experienced by type of attack**
in percent; weighted data



Phishing and other malicious software incidents (52.0 % and 24.0 % respectively) together account for more than three-quarters of all cyber-attacks experienced and remain at the forefront. In contrast to the annual prevalence rates, spyware attacks (11.9 %) account for a higher proportion of all cyber-attacks than ransomware attacks (3.3 %). In other words, compared with ransomware attacks, spyware attacks tend to be experienced by fewer companies (11.3 % vs. 12.5 %), but in a much higher number. The situation is similar with regard to manual hacking: although the number of companies that experienced such an attack within a year is lower than for all other types of attack, the number of reported incidents is proportionately higher than for CEO Fraud, (D)DoS and Defacing (2.9 % vs. 2.4 %, 2.2 % and 1.2 % respectively). This suggests that spyware attacks and manual hacking are more targeted at specific companies than the other types of attacks.

There is also a tendency for differences in the proportion of cases per type of attack to be observed between the employee size classes (Table 25). It is interesting to note that these differences do not follow a linear trend (e.g. the larger the company, the higher the proportion of phishing).

Table 25 **Proportion of cyber-attacks experienced by type of attack and employee size classes**
in percent; weighted data

	Employee size class				
Cyber-attack type	10-49	50-99	100-249	250-499	500+
Phishing	57.1	43.7	38.7	51.1	36.0
Other malware	19.0	32.5	38.0	25.4	36.5
Spyware	12.4	10.4	7.0	11.9	18.1
Ransomware	2.6	6.3	4.4	4.7	3.1
Manual hacking	4.0	0.4	1.8	0.3	0.7
CEO Fraud	1.3	4.2	5.6	3.0	4.2
(D)DoS	2.2	1.6	3.5	3.2	0.6
Defacing	1.4	1.0	1.1	0.5	0.7
Total	100.0	100.0	100.0	100.0	100.0

7.3 Risk assessment after experienced cyber-attacks

It is a general finding of darkfield research that the experience of having been a victim of a crime is associated with an increased fear of crime, including a higher risk assessment of future victimisation.[280] Based on this finding, a similar relationship between experienced cyber-attacks and the risk assessment for the company can also be expected for the corporate context.

Figure 40 **Risk assessment for untargeted cyber-attacks according to impact and employee size class**
Percentage of answers "rather/very high"; weighted data

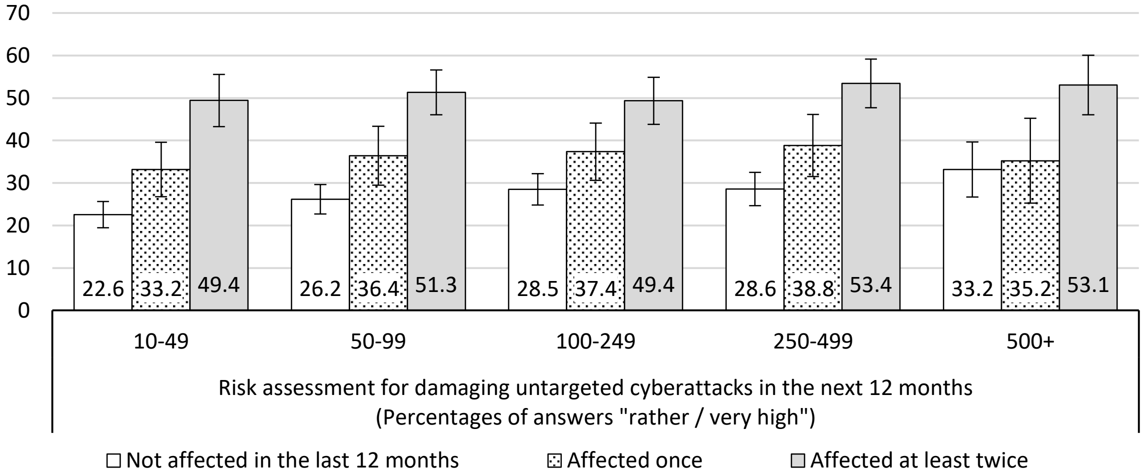


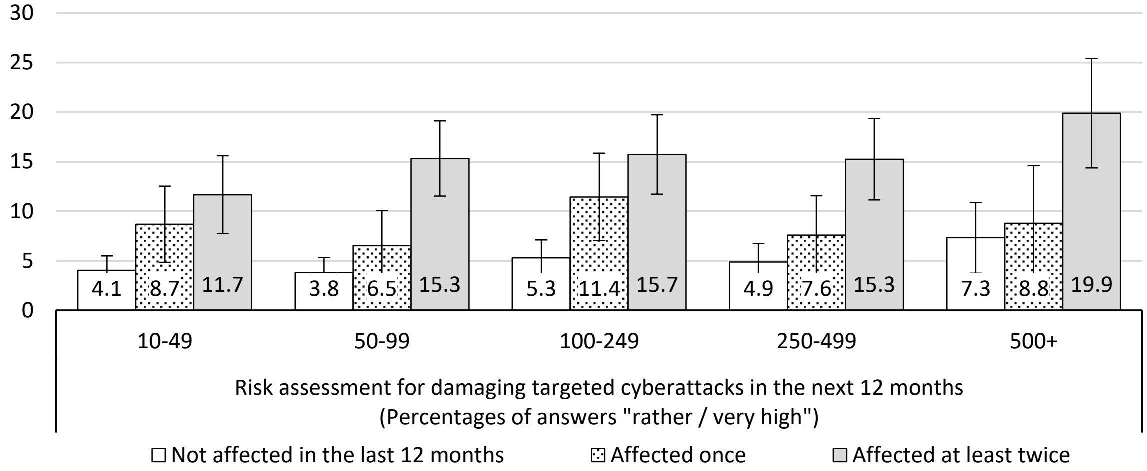
Figure 40 shows the proportions of companies for which the risk of suffering a damaging cyber-attack in the next twelve months was assessed as "very" or "rather high". In addition to the employee size class, these were also differentiated according to whether they had been affected by none, one or more types of attack in the last twelve months. As suspected, the less experience was gained with cyber-attacks in the last twelve months, the less often the risk of being targeted by cyber-attacks was assessed as "very/rather high".

A similar picture emerges with regard to risk assessments for companies regarding targeted damaging cyber-attacks (Figure 41). For companies that had to react to one or more types of

[280] On the consequences of computer-related crime among private individuals, see for example Dreißigacker & Riesner (2018).

attack in the previous year, the risk of renewed damaging attacks in the following year tended to be rated higher than for companies that were not affected.

Figure 41 **Risk assessment for targeted cyber-attacks according to impact and employee size class**
Percentage of answers "rather/very high"; weighted data



7.4 Interim summary

In this chapter, the extent to which companies have been affected by cyber-attacks was described. In total, 41.1 % of the companies stated that they had been affected by at least one of the types of attack surveyed in the last twelve months. Of these, 57.2 % of companies have experienced several different types of attacks. With regard to the so-called "lifetime prevalence", two thirds of the companies stated that they had experienced cyber-attacks in the past. Overall, it appears that smaller companies have lower prevalence rates than larger ones.

In addition to the employment size class, the sectoral affiliation is related to the prevalence rate, which ranges from 23.6 % for companies in agriculture, forestry and fishing (WZ08-A) to 48.4 % for companies in administrative and support service activities (WZ08-N). This variance also exists independently of the employment size classes and can also be found to some extent at the second level of individual WZ classes.

A large proportion of companies were hit by malware attacks: 12.5 % by at least one ransomware attack, 11.3 % by a spyware attack and 21.3 % by another malware attack. More than a fifth of companies had to react to at least one phishing attack. Every twelfth company was affected by CEO fraud, every sixteenth company by (D)DoS attacks. With shares of 3.1 % and 2.8 % affected companies, the attack types defacing, and manual hacking played a comparatively minor role in terms of distribution.

With regard to the respective types of attacks, there are further differences between the employee size classes of the companies: With regard to manual hacking, (D)DoS attacks and defacing, only tendential differences between small and large companies can be seen. In contrast, the prevalence of ransomware attacks, CEO fraud and phishing differ significantly. This is surprising because these are types of attacks which, unlike spyware attacks or manual hacking, for example, quickly become apparent as a result. An obvious explanation for this is that large companies may detect more attacks than smaller companies due to greater resource input in the area of IT security. Instead, it suggests that large companies probably offer a greater attack surface, especially for untargeted cyber-attacks, due to their greater presence on the Internet and their more extensive IT infrastructure and higher number of IT users.

In terms of attack types as a proportion of all reported cyber-attacks in the last 12 months, phishing, and other malicious software incidents (52.0 % and 24.0 % respectively) together account for over three quarters. It is also interesting to note that these percentages of spyware and manual hacking are higher than the annual prevalence rates. This means that although fewer companies have experienced these types of attacks overall, if they have, they have usually been experienced several times.

As expected, the impact of cyber-attacks in the last twelve months is also related to the assessment of the risk for the company to (re)experience a damaging cyber-attack in the next twelve months. This was evident both in relation to untargeted cyber-attacks that affect many other companies at the same time and to targeted cyber-attacks that only affect one's own company.

In the following chapter, we will show which company characteristics are positively related to the overall prevalence rate for cyber-attacks and are therefore to be considered potential risk factors.

8 POSSIBLE RISK FACTORS

As already shown in the presentation of the prevalence rates, there are statistically significant differences in the extent to which cyber-attacks affect organizations between employee size classes and sectors (WZ08 classes): Larger companies and certain sectors (e.g. WZ08-G: wholesale and retail trade; repair of motor vehicles and motorcycles or WZ08-M: professional, scientific and technical activities) are more frequently affected by cyber-attacks than others.[281] Why this is the case remains an open question for the time being.

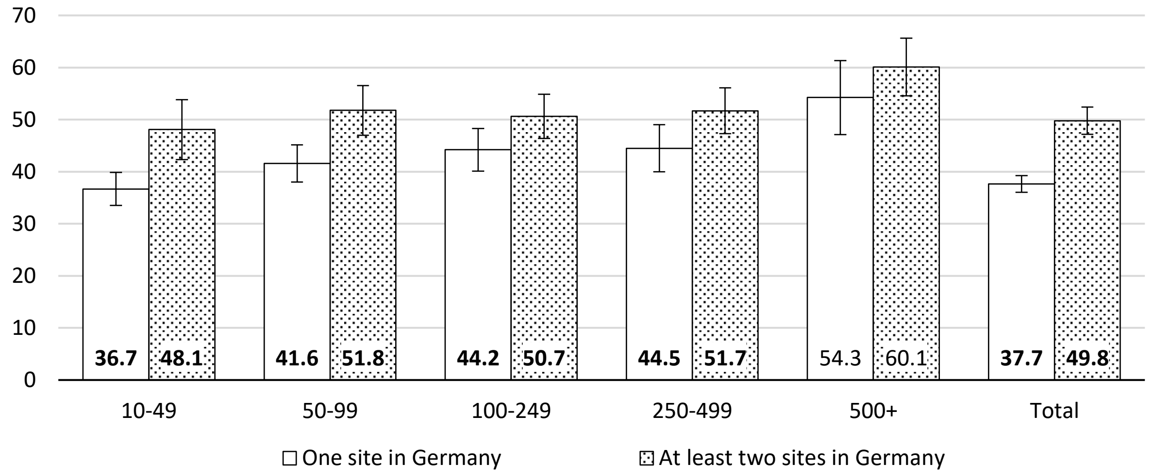
In the following, other selected company characteristics are related to the annual prevalence rate for cyber-attacks as a whole to provide an indication of which other factors increase the risk of cyber-attacks. In addition, the control of employee size classes can be used to check whether a correlation exists in all or only in individual size classes. On the other hand, the control of the considered variable can be used to check whether the above-mentioned prevalence differences between the employee size classes within the respective feature groups remain stable or are resolved. If the prevalence rates within one of these characteristic groups no longer differ between the employee size classes, the corresponding characteristic can be used as a possible explanation for this difference.

8.1 Number of locations

The number of locations with own IT infrastructure could have a positive effect on the risk of cyber-attacks via a more complex and decentralized IT structure. A comparison of the annual prevalence rates of companies with one (37.7 %; N=3,523) and companies with at least two sites in Germany (49.8 %; N=1,400) shows this expected correlation to be statistically highly significant (p<.000; Chi² test). Even if the employee size class of the companies is controlled, this correlation remains (Figure 42). Only in the case of companies with 500 or more employees, where there is a five percent probability of error, can it not be ruled out that this has come about by chance.

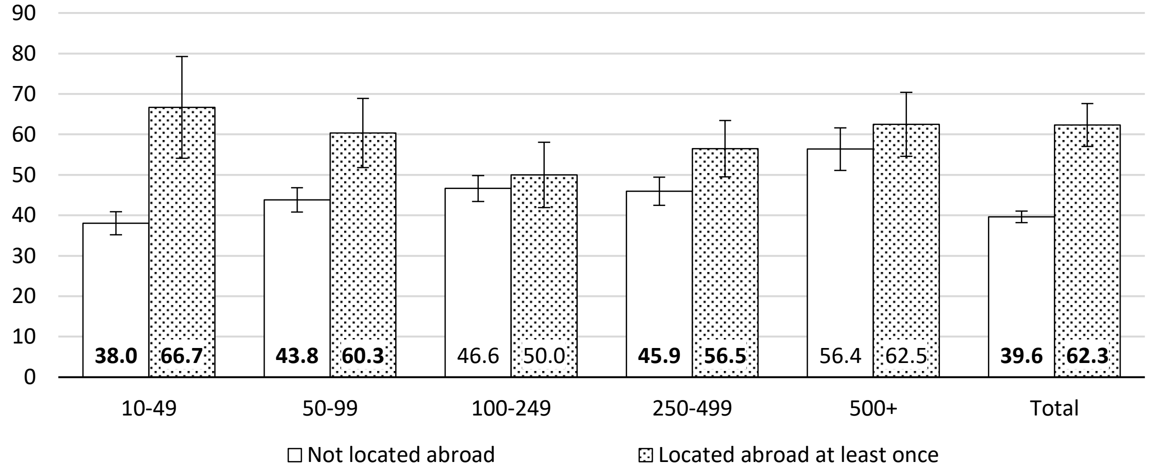
[281] See section 7.1.1.

Figure 42 **Total annual prevalence by number of sites in Germany and employee size class**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



It can also be seen that the prevalence rates of companies with at least two sites in Germany do not differ significantly with regard to their employee size class, with the exception of large companies (500+ Employees). This means that the number of sites can explain part of the relationship between company size and prevalence rate.

Figure 43 **Total annual prevalence by sites abroad and employee size class**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



In relation to the presence of at least one site abroad, a relationship to annual prevalence can also be identified. Companies with at least one site abroad were significantly more frequently affected by cyber-attacks in the last twelve months (62.3 %; N=321) than companies without sites abroad (39.6 %; N=4,609). This tends to apply to all employee size classes (Figure 43), but is most clearly the case for small companies (10-49 employees: 66.7 % vs. 38.0 %; N=54 or 1,123).

The prevalence differences in the group of companies with a foreign site(s) by employee size class are no longer statistically significant. In other words, the presence of at least one foreign site can also explain prevalence differences between the employee size classes.

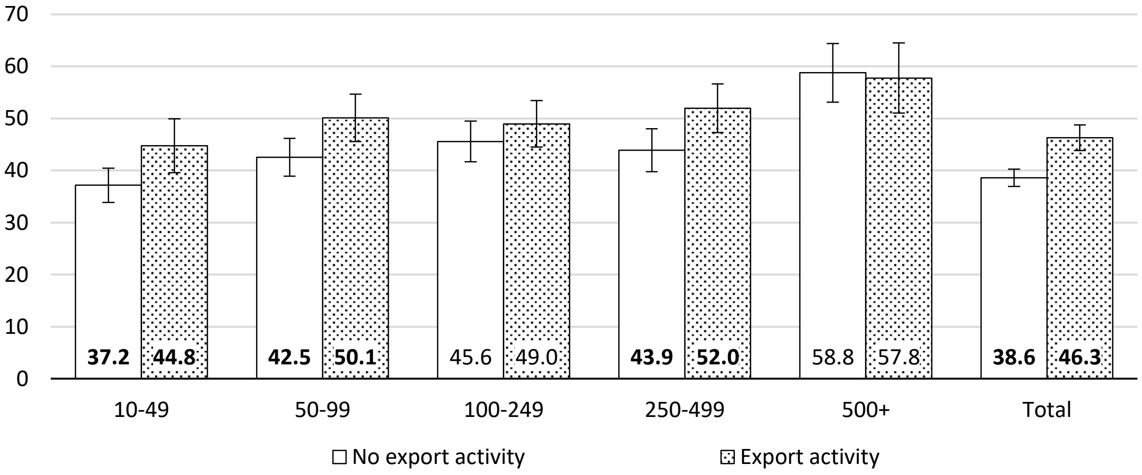
8.2 Export activity

Export activity could also have an impact on the risk of cyber-attacks, as it is likely to increase international networking and visibility.

Overall, the expected difference in annual prevalence between companies that export products or services abroad (46.3 %; N=1,607) and companies that do not (38.6 %; N=3,343) is apparent. This difference is not as marked when compared with the differences for the site abroad (Figure 44), but is significant with one exception for small and medium-sized companies (this cannot be said with the necessary certainty for companies with 100 to 249 employees). For large companies, on the other hand, export activity does not appear to have any effect on the impact of cyber-attacks.

Figure 44 **Total annual prevalence by export activity and employee size class**

in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



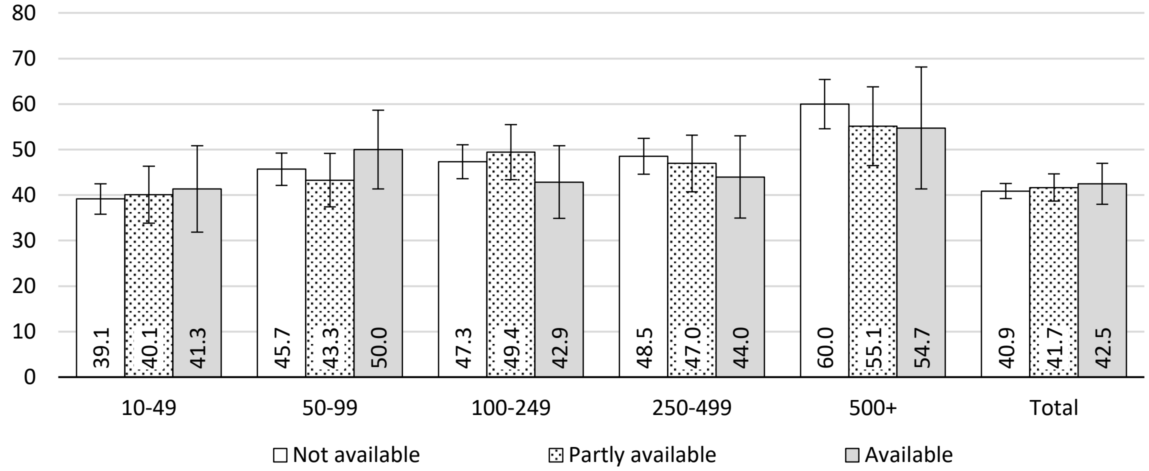
Similar to the non-exporting companies, the prevalence rates of exporting companies increase with increasing company size, indicating that export activities seem less suitable for explaining the prevalence differences between employment size classes.

8.3 Publicly available information

The publication of detailed responsibilities, contacts and job descriptions of employees could also be related to a higher incidence of cyber-attacks in the last twelve months, as this information could potentially be exploited for cyber-attacks, especially in the field of social engineering (e.g. CEO fraud).

Figure 45 Annual prevalence in total by publicly available employee information on the Internet and employee size class

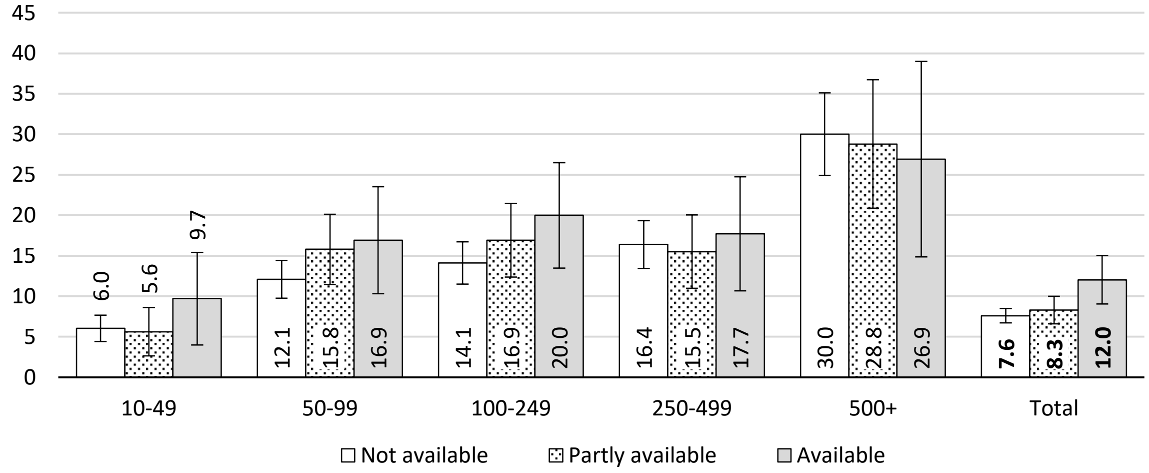
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



In terms of the overall prevalence rate of cyber-attacks, there are initially neither uniform trends nor statistically significant differences between companies that publish information online, those that do so partially and those that do not (Figure 45). If we relate this distinction to the annual prevalence of CEO Fraud cyber-attacks, the expected correlation becomes apparent (Figure 46). Overall, companies that published company information on employees on the Internet were significantly more affected by CEO fraud (12.0 %; N=457) than companies that published only partial (8.3 %; N=1,013) or inaccessible (7.6 %; N=3,410) information. Under control of the employee size class, this correlation can only be seen as a tendency, which may be due to the fact that the case numbers of the additionally differentiated comparison groups are relatively small.

Figure 46 Annual prevalence of CEO Fraud by publicly available employee information on the Internet and employee size class

in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



The fact that prevalence rates in all three groups tend to increase with the size of the workforce is an indication that the availability of certain company information on the Internet does not provide an explanation for the different prevalence rates of the employee size classes.

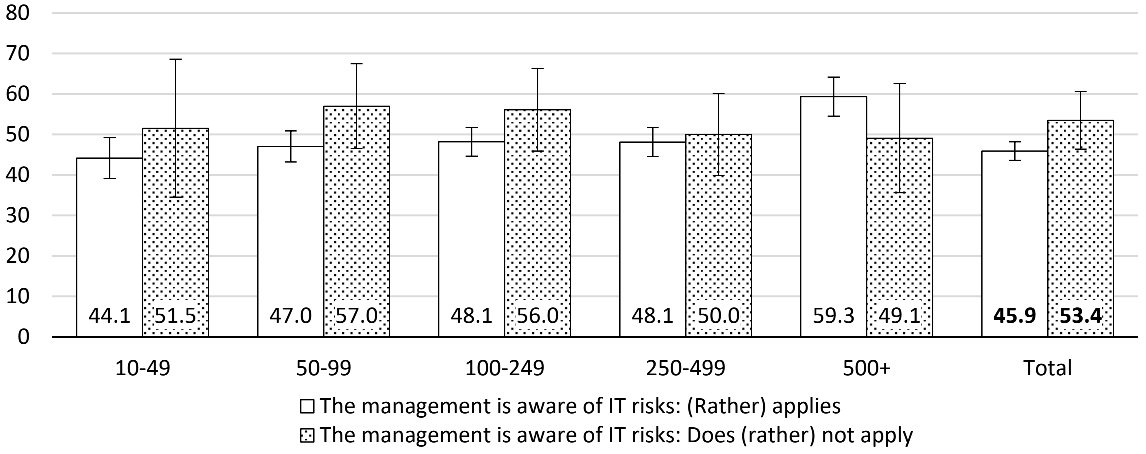
8.4 Risk awareness within the company

Whether there is awareness of IT risks within the company was only determined by the assessment of the company representatives interviewed and is therefore subjective. As shown above, this assessment is related to the position the respondents held within the company.[282] For this reason, only the statements of IT employees are used to compare the annual prevalence of cyber-attacks as a whole according to the assessment of risk awareness.[283]

In comparison, companies whose IT representatives (rather) agreed that management is aware of IT risks and complies with the guidelines have a lower overall prevalence rate for cyber-attacks (45.9 %; N=1,868) than companies whose representatives (rather) disagreed (53.4 %; N=189; Figure 47). This tends to be the case for all employee size classes, except for large companies (500 employees or more), for which a contrary but not significant correlation can be seen. This could be accidental or related to other variables that are more important for large companies.

Figure 47 **Total annual prevalence by risk awareness of business and employee size class**

in percent; weighted data; 95 %-CI; bold: differences significant at p<.05 (Chi² test); only answers from IT-Employees

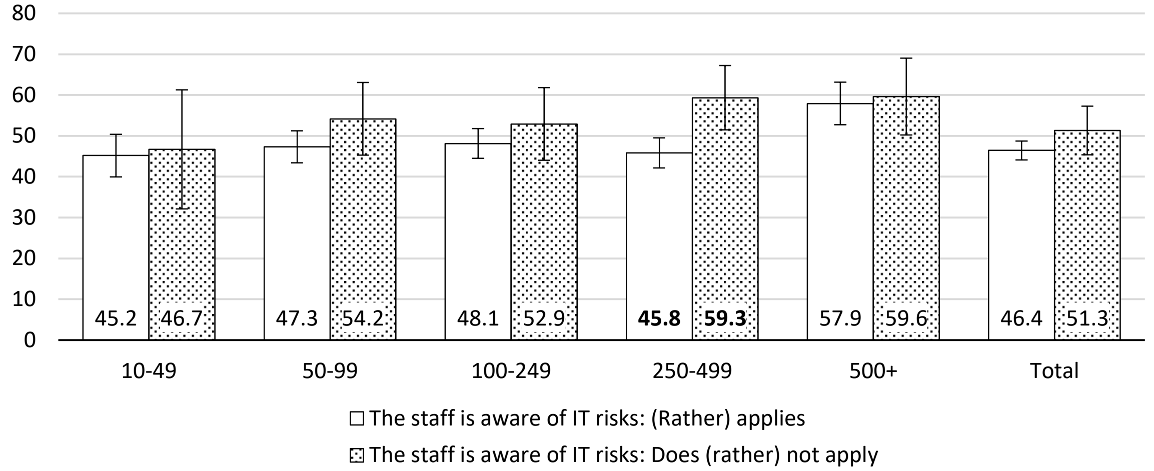


It can also be seen that the prevalence differences between the employee size classes level off both within the companies with (rather) risk-conscious management and within the companies with (rather) risk-conscious management. This is an indication that this characteristic can also be used to explain the prevalence differences between the employee size classes. In other words, if the management is not aware of IT risks, the size of the company hardly seems to play a role, because the risk is similarly high in all employee size classes. If the management is aware of the risks, the risk of cyber-attacks seems to be the same at least between small and medium-sized companies. Only large companies stand out clearly in this group. It is possible that in large companies the risk awareness of the management is more independent of other factors that play a role in the risk.

[282] See section 6.1.

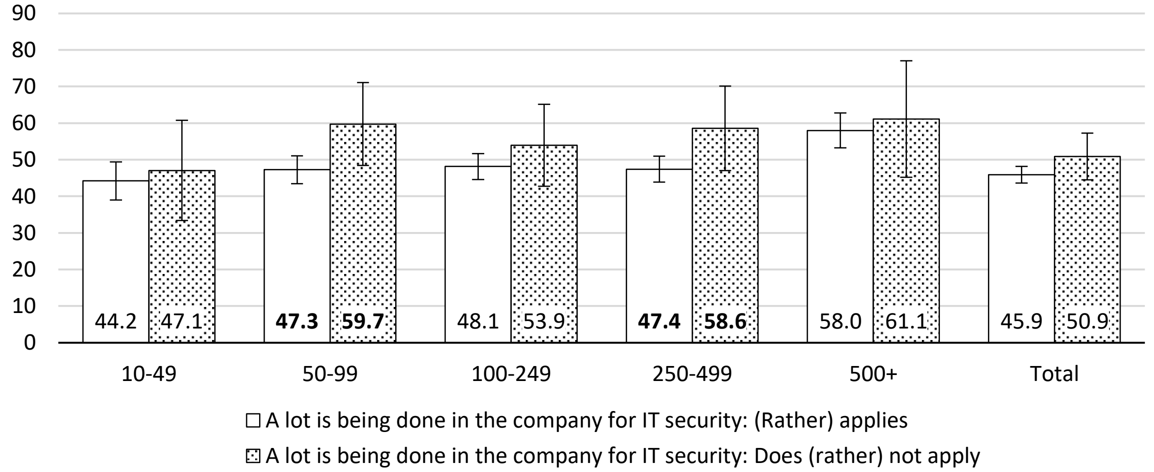
[283] This is due to the fact that IT employees represent the largest group of interviewees.

Figure 48 **Total annual prevalence by risk awareness of the workforce and employee size class**
in percent; weighted data; 95 %-CI; bold: differences significant at p<.05 (Chi² test); only answers from IT-Employees



When comparing the annual prevalence rates for cyber-attacks overall with regard to the assessment of the surveyed IT employees regarding the risk awareness of the staff, at least one uniform tendency can be seen (Figure 48): Companies in which the statement that the staff is aware of IT risks and complies with the guidelines was (rather) agreed to, are proportionally less affected than companies in which this was not (rather) agreed to. The correlation is statistically significant only in companies with 250-499 employees. An indication that the risk awareness of the staff is not suitable for explaining the prevalence differences between the employee size classes is shown by the prevalence rates in both comparison groups, which continue to tend to rise with increasing numbers of employees.

Figure 49 **Total annual prevalence by risk awareness of the workforce and employee size class**
in percent; weighted data; 95 %-CI; bold: differences significant at p<.05 (Chi² test); only answers from IT-Employees



A similar picture emerges with regard to the assessment of the statement that much is being done in the company for IT security. Companies whose IT representatives (rather) agreed with this statement tended to be less affected by cyber-attacks in general than companies whose representatives (rather) disagreed with it (Figure 49). Statistically significant differences in this respect can be seen in companies with 50 to 99 and 250-499 employees (47.3 % vs. 59.7 % and 47.4 % vs. 58.6 %).

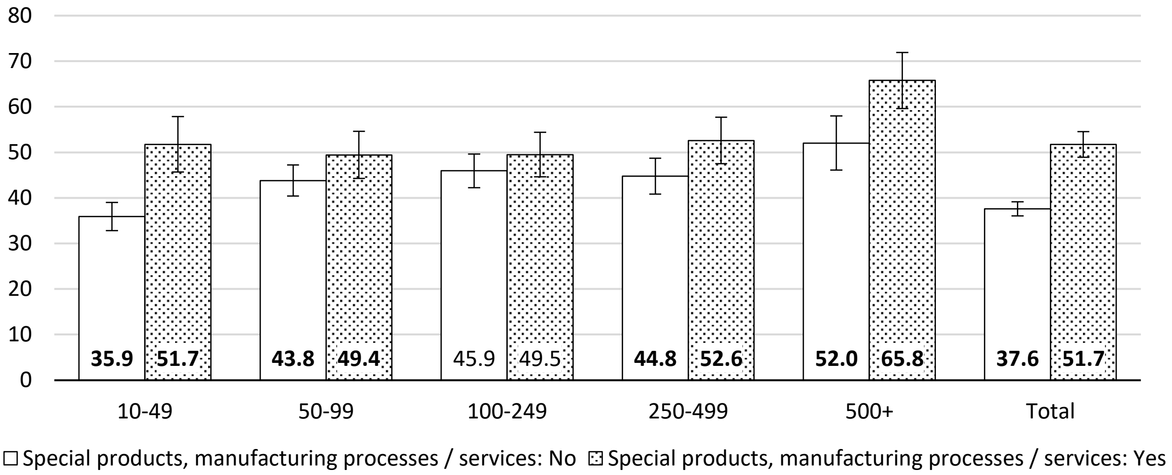
In the group of companies in which (rather) not much is done for IT security, the prevalence rates of the individual employee size classes no longer differ significantly, which could, however, be related to the small number of cases in these classes, especially since the percentage difference between the small and large companies is still 13 percentage points. This characteristic therefore seems less suitable to explain the prevalence differences between the employee size classes.

8.5 Potential targets

8.5.1 Special products, manufacturing processes or services

Insofar as some cyber-attacks are targeted at specific companies or industries, a higher risk is to be assumed for companies with potential targets such as specific products, manufacturing processes or services.[284]

Figure 50 **Total annual prevalence by potential targets (special products etc.) and employee size class**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



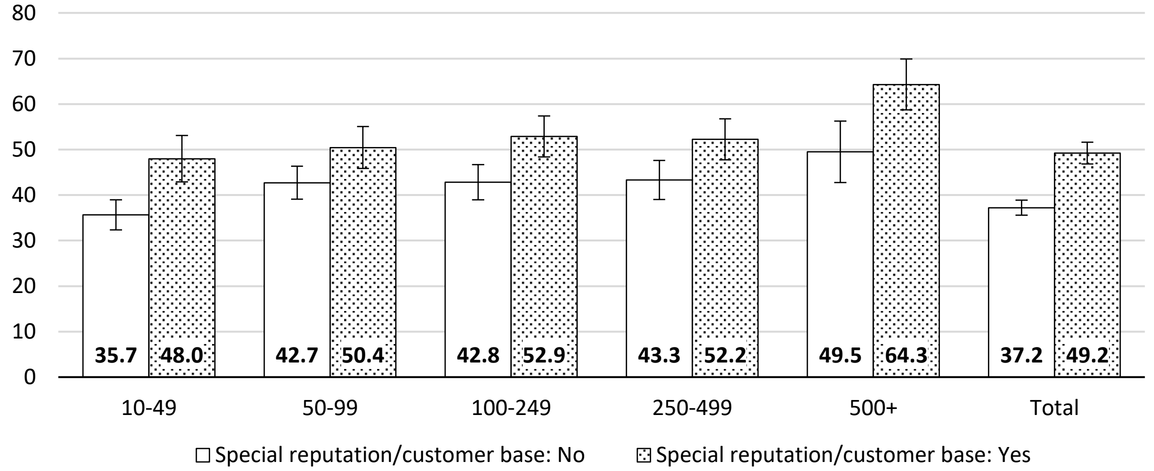
A comparison of the overall annual prevalence of cyber-attacks in companies with and without such specificities may support this assumption (Figure 50). Companies that answered the question about special products etc. were significantly more frequently affected by cyber-attacks (51.7 %; N=1,212) than companies that answered the question in the negative (37.6 %; N=3,743). With one exception (companies with 100-249 employees) this result is also confirmed in the respective employee size classes.

8.5.2 Special reputation or customer base

Another potential target for attackers was asked about their special reputation or customer base. This also shows a clear picture (Figure 51): Companies which answered this question in the affirmative, i.e. which in their own estimation have a special reputation or customer base, were significantly more frequently affected by cyber-attacks in the last twelve months (49.2 %; N=49.2 %) than those which answered in the negative (37.2 %; N=3,276). This result is maintained even under control of the employee size class in all classes.

[284] The assessment of "specificity" was the responsibility of the respondents themselves (see Section 6.3).

Figure 51 Annual prevalence in total according to potential targets (special reputation etc.) and employee size class
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



In both groups, which have special products etc. or a special reputation, the prevalence difference between small and medium-sized companies levels off. In other words, the presence of these potential targets can help explain the prevalence difference between the employee size classes.

8.6 Companies of public interest

The group of companies providing companies of general public interest[285] could also be a particular target for cyber-attacks, since their damage can have a far-reaching extent and quickly noticeable consequences for the population (e.g. for the patients of a hospital).[286] This could be exploited by potential perpetrators, for example in connection with blackmail. Against this background, such companies should be particularly protected against cyber-attacks. Although this was only confirmed with regard to three organisational IT security measures (certification of IT security, IT security training for employees, exercises or simulations for the failure of important IT systems), which were proportionally more frequent in companies of general interest than in companies of the other WZ08 classes (Figure 15 and Figure 22), this could already be associated with a higher level of protection, which would have an effect on the prevalence rate.

When comparing the existing IT security measures between companies of general interest and companies of other WZ08 classes, this suspected connection becomes at least partially apparent.

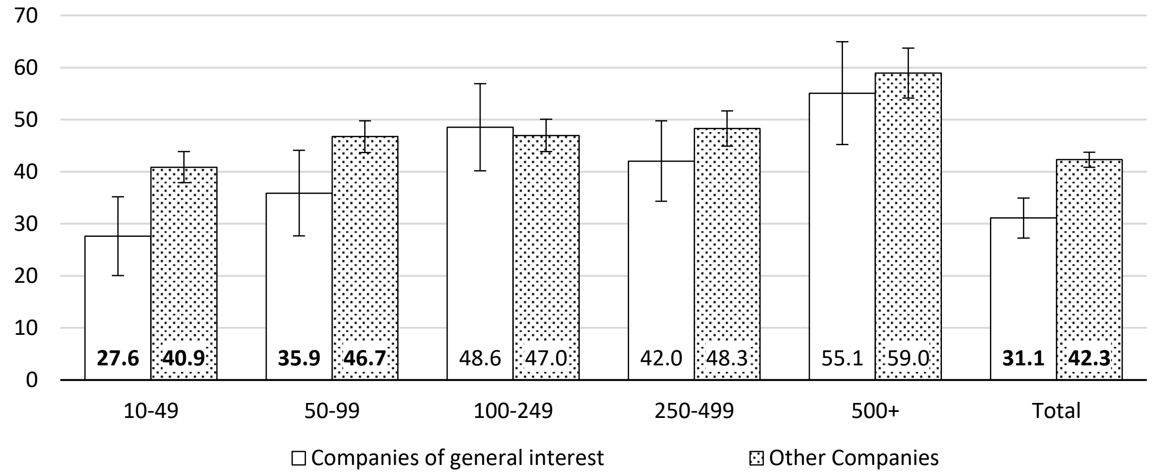
[285] See footnote 194 and the table 4 in section 3.4.1. A list of all the corresponding WZ classes can be found in the table 43 in Annex 1.

[286] Thus, the Süddeutsche Zeitung (Online) reported on 17.07.2019 of 13 hospitals affected by a ransomware attack: https://www.sueddeutsche.de/digital/krankenhaeuser-schadsoftware-ransomware-virus-drk-1.4529406 (last checked on 02.09.2019). See also Bundesamt für Sicherheit in der Informationstechnik (2019c).

Figure 52

Annual prevalence in total according to affiliation to companies of general interest

in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



Regardless of the employee size class, the share of companies affected by at least one cyber-attack in the group of companies of general interest in the previous year is significantly about eleven percentage points below the share of companies of the other WZ08 classes (31.1 % vs. 42.3 %; N=556 and 4,425, respectively; Figure 52). Differentiated by employee size class, this is particularly true for smaller companies (10-49 and 50-99 employees).

8.7 Interim summary

In summary, after these comparisons of the groups of characteristics, it can be concluded that there are other characteristics, in addition to company size and industry, that are related to the risk of cyber-attacks. Whether one of these characteristics is more decisive than others cannot be determined within the scope of this analysis. This requires further multivariate analyses, the results of which are published elsewhere. Nevertheless, even here, particularly marked differences in prevalence are already noticeable with regard to the number of sites in Germany, the existence of a foreign sites, export activity and the existence of potential targets for attackers, e.g. special products/ manufacturing processes/services or special reputation/ customer base. Companies with several sites in Germany, at least one site abroad, which are active in the export business or which offer special products etc. or have a special reputation/customer base were significantly more frequently affected by cyber-attacks than companies without these characteristics, irrespective of their size. In particular, small companies of general interest (10-99 employees) were affected by cyber-attacks significantly less frequently than companies in other sectors, which indicates a higher level of protection of general interest companies.

The results are less clear with regard to the availability of information on employees (e.g. detailed responsibilities, contacts, job descriptions) and risk awareness within companies. The latter was collected via the subjective assessment of a company representative and could be distorted as a result.

However, management risk awareness in particular appears to play an important role in explaining the differences in prevalence between companies of different employee size classes, since under control of the management risk awareness assessment, these differences largely cancel each other out. The annual prevalence rates for cyber-attacks as a whole also no longer differ significantly between employee size classes in companies with several sites in Germany or with at least one site abroad, so these features also appear to help explain the difference reported above.

9 MOST SEVERE ATTACK

Since not every cyber-attack experienced by the companies could be surveyed in detail due to the limited duration of the interview, the companies affected in the previous twelve months should only focus on the most severe cyber-attack when answering the detailed questions. The severity of these attacks remains open for the time being but can be estimated by assessing the reported damage. If only one attack was experienced, this is considered the most severe.

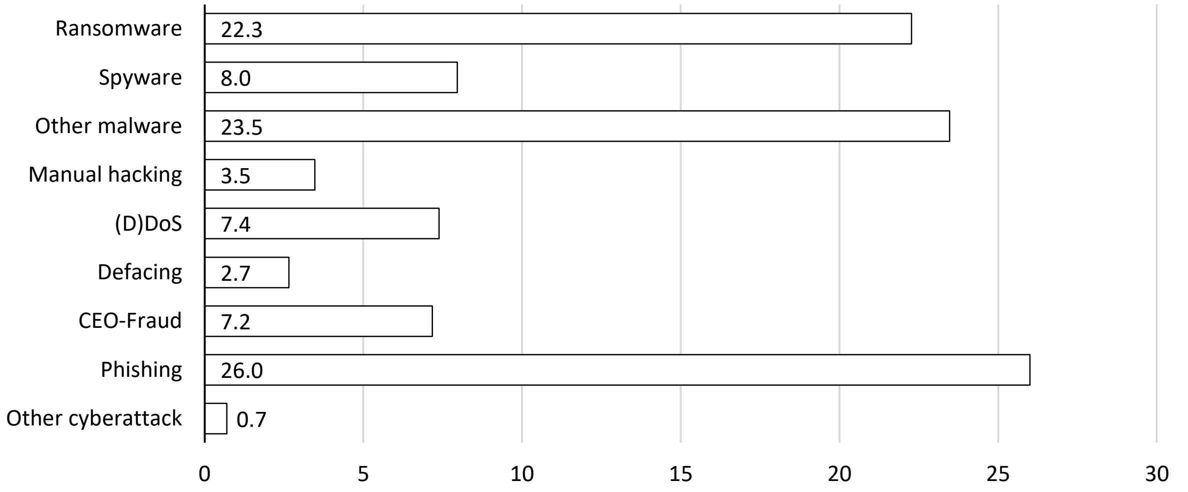
9.1 Type of attack

The most common types of attack mentioned in relation to the most severe cyber-attack of the previous twelve months (Figure 53) include phishing (26.0 %), ransomware (22.3 %) and other malware (23.4 %). Spyware (8.0 %), (D)DoS (7.4 %) and CEO Fraud (7.2 %) were named much less frequently, followed by manual hacking (3.5 %), defacing (2.7 %) and other cyber-attacks (0.7 %).[287] Only a very small percentage of 0.4% of respondents (N=1,787) answered in the affirmative to the question of whether this attack was threatened in advance.

Figure 53

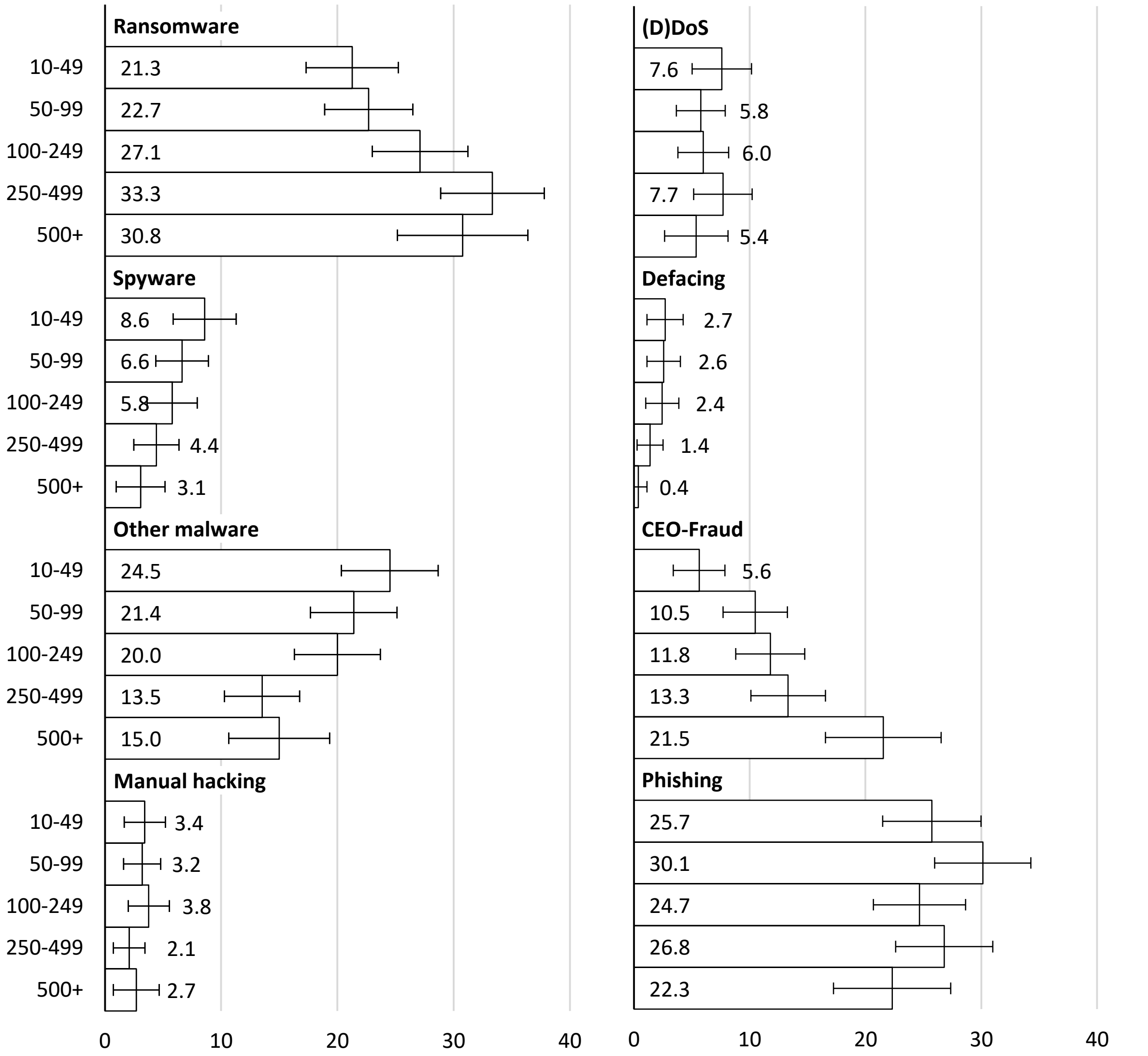
Most severe cyber-attack by attack type

in percent; weighted data; multiple answers possible; N=1,787



[287] In particular, illegal crypto-mining was mentioned here, although it remains unclear whether other companies have subsumed the use of crypto-malware under other malware.

Figure 54 **Most severe attack in the last 12 months by type of attack and employee size class**
in percent; weighted data; 95 %-CI; multiple answers possible



When comparing the most severe attacks evaluated by the companies according to attack type and employee size classes, there are sometimes significant differences (Figure 54): ransomware attacks are mentioned significantly more frequently by larger companies in connection with the most severe attack (250-499 employees: 33.3 %; 500+ employees: 30.8 %) than by small companies (10-49 employees: 21.3 %). In contrast, small companies mention other malware significantly more frequently (10-49 employees: 24.5 %) than larger companies (250-499 employees: 13.5 %; 500+ employees: 15.0 %). Further statistically relevant differences can be found in spyware and CEO fraud: While spyware was significantly more common in small companies (10-49 employees: 8.6 %) than in large companies (500+ employees: 3.1 %), CEO fraud was significantly more common in large companies (500+ employees: 21.5 %) than smaller ones. The middle employee size classes (50-99 employees: 10.5 %; 100-249 employees: 11.8 %; 250-499 employees: 13.3 %) also differing significantly from small companies (10-49 employees: 5.6 %). There are no statistically relevant differences between the employee size classes for the other types of attack and, with the exception of phishing, these were mentioned comparatively rarely in connection with the most severe cyber-attack. Phishing, on the other hand, is not only one of the most common types of attack (see Figure 36 and Figure 37), but in many cases it is also cited as the most severe attack type experienced in the last twelve months.

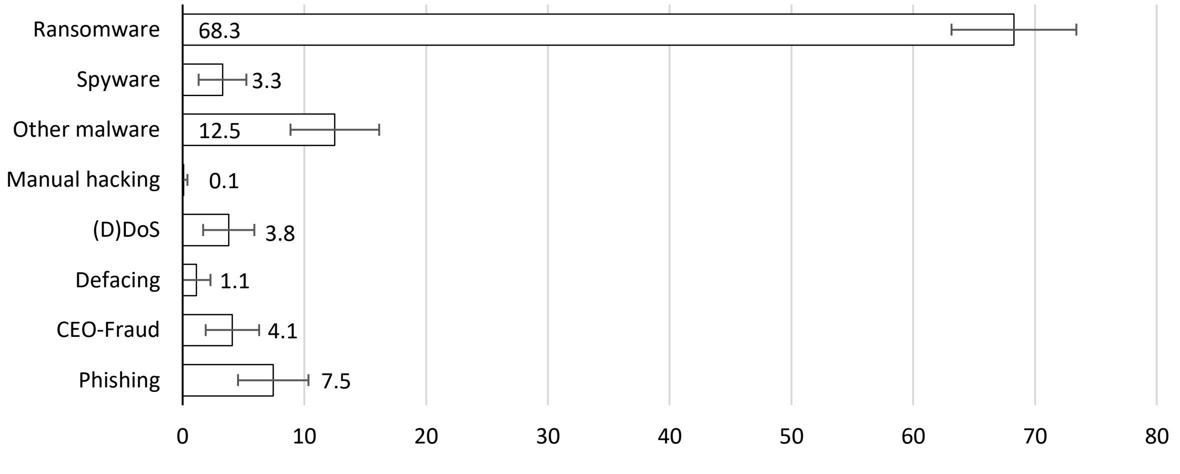
9.2 Conjecture about the perpetrators

The information on the suspected perpetrators behind the most severe crime is not particularly reliable. This is particularly evident in the fact that only one in three of the companies concerned (30.7 %, N=1,787) even expressed a corresponding assumption. Of these, 4.4 % (N=532) stated that perpetrators presumably came from among former or active employees. A share of 1.8 % suspected business partners (e.g. service providers, suppliers) behind the crime, 6.1 % competitors and 92.4 % other outsiders.[288] In summary, only 6.1 % of the companies with suspicions about the perpetrators say that, with regard to the most severe cyber-attack, they are presumed to be internal perpetrators (former/active employees or business partners). Statistically significant differences between employee size classes, sectors or types of attack cannot be identified here, not least because of the small number of cases. As a tendency, large companies (500+ Employees: 11.5 %, N=78) tend to deal with internal offenders more frequently than small companies (10-49 employees: 4.8 %, N=124).

9.3 Demand of ransom

In 18.2 % (N=1,744) of the most severe cyber-attacks reported, the perpetrators demanded a ransom. These demands were met by 2.3 % (N=317) of the companies affected, whereupon in six out of seven cases the perpetrators kept their promises (e.g. data decryption or stopping the attack).

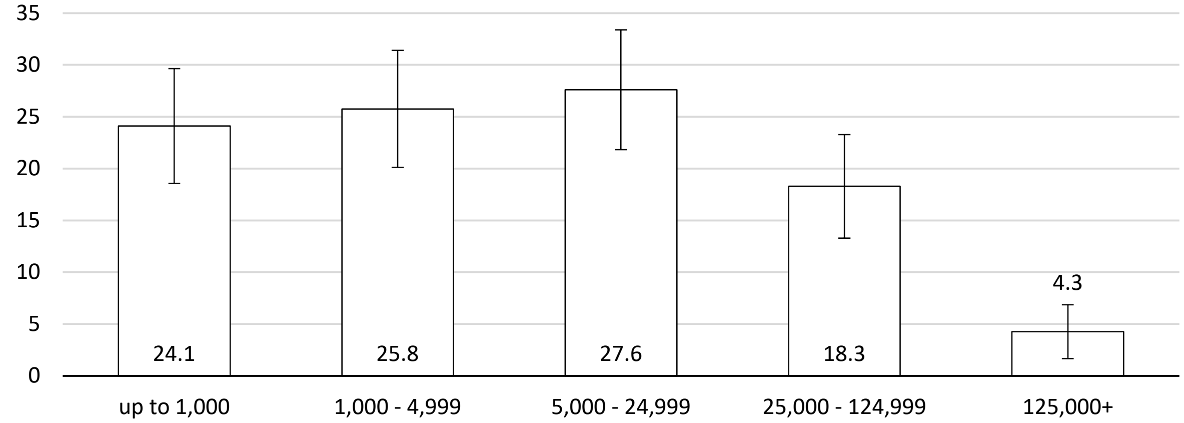
Figure 55 **Cyber-attacks with ransom demand by attack type**
in percent; weighted data; 95 % CI; multiple answers possible; N=317



As expected, ransomware attacks are the most common of the cyber-attacks associated with ransom demands, accounting for 68.3 % (Figure 55). Attacks with other malware are represented with 12.5 % and phishing with 7.5 %. The shares of other types of attacks are in the lower single-digit range (e.g. CEO Fraud: 4.1 %, (D)DoS: 3.8 % and Spyware: 3.3 %).

[288] Multiple answers were possible. Findings on perpetrators of cyber-attacks in general can be found, for example Huber et al. (2018); Huber & Pospisil (2018).

Figure 56 **Level of ransom demand in EUR (classified)**
in percent; weighted data; 95 %-CI; N=230



The amount of the ransom demands ranges very widely from EUR 100 to EUR 100 million, with half of the reported demands (median) below EUR 4,800 and the other half above (N=230).[289] The figure 56 shows classified distribution of ransom demands: In about one quarter the amount of the ransom was below EUR 1,000 (24.1 %), in another quarter between EUR 1,000 and 4,999 (25.8 %). In slightly more than a quarter of cases, the claim was between EUR 5,000 and EUR 24,999 (27.6 %), in just under a fifth between EUR 25,000 and EUR 124,999 (18.3 %) and in a small proportion of 4.3 % EUR 125,000 and more.[290]

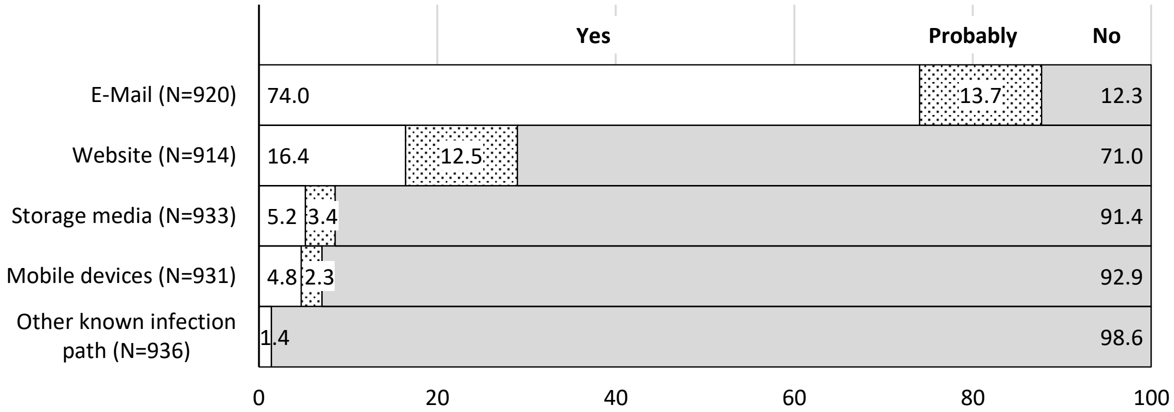
9.4 Path of infection

The companies that reported an attack by ransomware, spyware or other malicious software (hereafter summarized as malware attack) as the most severe cyber-attack of the last twelve months (N=954) were asked about the path of infection. They were able to specify for various predefined paths whether this was (probably) the case or not. A share of 74.0 % indicated that the infection occurred via e-mail (N=920) and another 13.7 % suspected this. Approximately one in eight companies (12.3 %) excludes this path of infection (Figure 57). Malware infections via a website (e.g. via active content or downloads) are much less frequently reported (yes: 16.4 %, probably: 12.5 %). The lowest percentages are those that name or suspect storage media (e.g. USB sticks, SD cards, CDs) and mobile end devices (e.g. netbooks/notebooks, tablets, smartphones) as a path of infection (yes: 5.2 % and 4.8 %, presumably: 3.4 % and 2.3 % respectively). Nine out of ten companies (91.4 % and 92.9 %) exclude this.

[289] More than a quarter (27.4%, N=317) of the companies affected by money claims could not provide any information on the amount of the ransom.

[290] If one considers exclusively the ransom demands for ransom goods attacks, the classes are similarly occupied (under 1,000: 26.2%, 1,000 - 4,999: 26.4%, 5,000 - 24,999: 25.0%, 25,000 - 124,999: 16.6%, from 125,000: 5.8%). However, the median is somewhat lower at around EUR 2,100 (N=146).

Figure 57 **Infection path for malware attacks**
in percent; weighted data

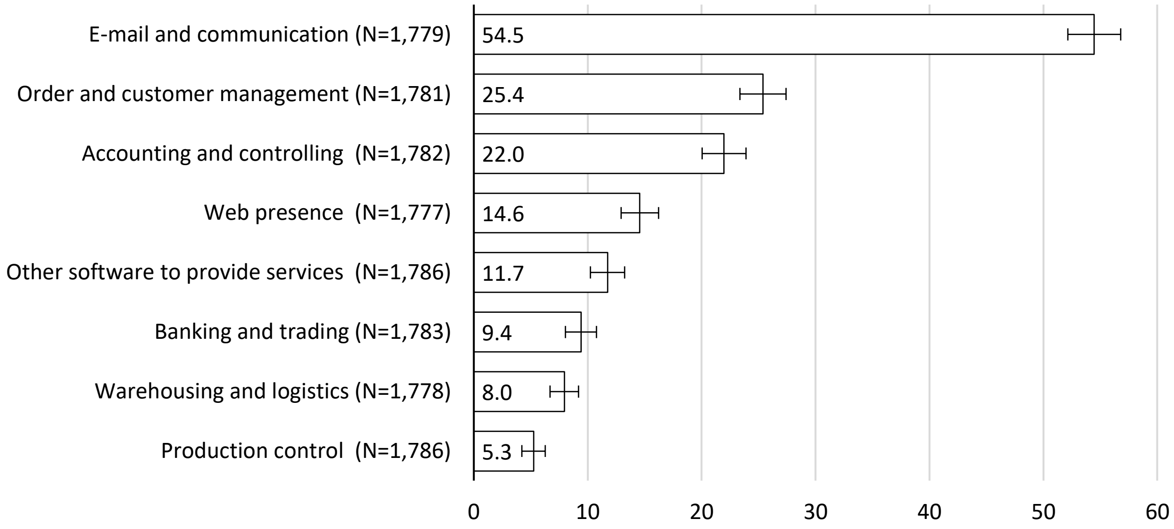


9.5 Consequences

9.5.1 Affected systems

The three most frequently mentioned IT systems affected by the most severe attack, i.e. those which could not be used or could only be used to a very limited extent as a result of the attack, are e-mail and communication (54.5 %), order and customer management (25.4 %) and accounting and controlling (22.0 %). Web presence (14.6 %) and other software for the provision of services (11.7 %) were mentioned less frequently, and IT systems in banking and trading (9.4 %), warehousing and logistics (8.0 %) and production control (5.3 %) were affected even less frequently (Figure 58).

Figure 58 **IT systems affected by the most severe cyber-attack**
in percent; weighted data; 95 %-CI; multiple answers possible



A comparison between the employee size classes shows that small companies tend to be affected more frequently by the failure or severely limited usability of the various IT systems (Table 26). These differences are statistically significant with regard to the IT systems e-mail and communication, order and customer management and web presence: while e-mail traffic and communication are either not functioning at all or only to a very limited extent in more than half of the small companies (10-49 employees: 56.9 %) as a result of the most severe cyber-attack, this is only the case in 37.7 % of the large companies (500+ Employees).

Table 26 **IT systems affected by the most severe cyber-attack by employee size class**
in percent; weighted data; bold: significant at p<.05 (Chi² test)

	Employee size class				
IT system	10-49	50-99	100-249	250-499	500+
E-mail and communication	**56.9**	**49.7**	**44.9**	**47.7**	**37.7**
Order- and customer management	**27.0**	**24.1**	**17.3**	**18.2**	**16.2**
Accounting and controlling	23.1	19.2	18.0	18.2	15.5
Web presence	**15.8**	**11.3**	**9.8**	**7.5**	**8.8**
Other software to provide services	11.8	11.8	12.4	9.6	10.9
Banking and Trading	9.8	9.0	7.6	8.9	6.9
Warehousing and logistics	8.1	8.8	7.3	5.6	5.4
Production control	5.4	4.9	6.2	4.2	2.7
N	407	465	449	427	260

Also, with regard to the WZ08 classes, clear differences can be seen in some cases (Table 27). For example, 70.3 % of accommodation and food service activities (WZ08-I) indicated that the IT system e-mail and communication was affected by the most severe attack and failed completely or partially as a result. The share of affected order and customer management systems (39.7 %) and websites (34.9 %) is also higher in the business sector WZ08-I than in other WZ08 classes. IT systems for accounting and controlling were most frequently affected in companies in human health and social work activities (WZ08-Q: 35.4 %) and the construction (WZ08-F: 32.5 %). Other software for the provision of services was comparatively frequent in the business sector education (WZ08-P: 20.5 %) and in professional, scientific and technical activities (WZ08-M: 18.7 %). Banking and trading systems were more frequent in the sector WZ08-G (wholesale and retail trade; repair of motor vehicles and motorcycles: 15.1 %), warehousing and logistics systems in the sector WZ08-H (transportation and storage: 18.2 %) and production control systems in the sector WZ08-N (administrative and support service activities: 8.8 %).[291]

[291] A further differentiation by second level WZ classes is not meaningful due to the small number of cases.

Table 27 **IT systems affected by the most severe cyber-attack according to WZ08 classes**
in percent; weighted data

	IT system affected								
WZ08 class (level 1)[292]	1	2	3	4	5	6	7	8	N
Manufacturing (WZ08-C)	52.6	22.3	18.5	6.7	6.7	6.2	8.7	7.2	389
Construction (WZ08-F)	55.9	30.1	32.5	12.1	15.0	10.6	7.2	7.2	206
Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles (WZ08-G)	56.0	29.3	28.7	17.2	10.4	**15.1**	17.1	5.3	376
Transportation and Storage (WZ08-H)	52.7	27.3	18.2	10.9	7.4	5.5	**18.2**	7.3	55
Accommodation and Food Service Activities (WZ08-I)	**70.3**	**39.7**	15.6	34.9	4.8	9.4	1.6	4.8	64
Information and Communication (WZ08-J)	41.5	12.3	7.7	**33.8**	3.1	6.2	1.5	1.5	65
Professional, Scientific and Technical Activities (WZ08-M)	55.6	22.5	17.1	15.8	18.7	3.2	2.7	3.2	187
Administrative and Support Service Activities (WZ08-N)	56.0	35.9	17.0	13.2	9.9	12.1	1.1	**8.8**	90
Education (WZ08-P)	57.0	25.6	21.3	12.4	**20.5**	7.6	3.3	4.2	121
Human Health and Social Work Activities (WZ08-Q)	55.4	16.9	**35.4**	20.7	13.3	13.4	1.2	2.4	83
Other Service Activities (WZ08-S)	50.0	5.0	9.8	15.0	17.5	5.0	13.9	0.0	40

IT system: 1: e-mail and communication, 2: order and customer management, 3: accounting and controlling, 4: web presence, 5: other software for the provision of services, 6: banking and trading, 7: warehouse and logistics, 8: production control
Emphasis: bold: largest share per IT system; Gray background: the three largest shares per IT system; underlined: largest share per WZ08 class

Table 28 **IT systems affected by the most severe cyber-attack, by attack type**
in percent; weighted data

	Cyber-attack type							
IT system	1	2	3	4	5	6	7	8
E-mail and communication	**49.2**	**66.7**	**60.2**	**45.2**	**71.2**	40.4	**43.8**	**52.6**
Order- and customer management	48.2	26.6	24.1	25.8	7.6	2.1	9.4	19.8
Accounting and controlling	37.4	19.7	16.7	40.3	3.8	0.0	18.8	20.9
Web presence	8.0	16.2	11.7	21.1	58.0	**87.5**	3.9	5.9
Other software to provide services	23.9	14.8	12.4	17.7	4.5	0.0	3.9	4.5
Banking and Trading	11.1	12.7	7.2	8.1	1.5	0.0	7.0	12.9
Warehousing and logistics	15.6	5.6	9.4	16.1	3.1	0.0	0.0	3.9
Production control	7.8	7.0	5.7	12.9	3.8	0.0	0.0	3.4
N	397	142	418	61	131	47	128	462

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing
Highlighting: bold: largest share per type of attack; Gray background: the three largest shares per type of attack; underlined: largest share per IT system

A fairly homogeneous picture can be seen when broken down according to which IT systems are most frequently affected by each type of attack (Table 28). With the exception of (D)DoS and defacing attacks, e-mail and communication systems, order and customer management systems as well as accounting and controlling systems are among the three most frequently affected IT systems, i.e. IT systems that cannot be used or can only be used to a very limited extent due

[292] Classes with a case number smaller than 30 are not listed.

to the most severe attacks. (D)DoS and defacing attacks affected not only e-mail and communication systems in accordance with their objectives, but in particular the companies' web presence. Other software used to provide services as well as warehouse and logistics systems are comparatively frequently affected by ransomware attacks and manual hacking. The latter type of attack also plays a major role in warehousing and logistics and production control systems. In contrast to the other types of attack, CEO fraud plays a special role in Table 28 insofar as forms of social engineering generally do not have a direct damaging effect on IT systems. The fact that the systems mentioned are affected by CEO fraud should be seen here more as a means of attack.

Looking at the largest shares per IT system, it is noticeable that accounting and controlling systems are relatively often affected by manual hacking. This also tends to apply to warehouse and logistics systems as well as production control systems.

Table 29 **Downtimes of affected IT systems that are (rather) important for the companies**

weighted data; only data on the most severe cyber-attack

		of which (rather) important (%)	Downtime of (rather) important classified IT systems					
IT system	Affected (%)		Median (h)	Ø (h)	SD (h)	Min (h)	Max. (h)	Max. (d)
E-mail and communication	54.5 (N=1,779)	92.7	24 (N=705)	64.8	201.0	1	2,160	90
Order- and customer management	25.4 (N=1,781)	95.3	24 (N=393)	76.0	172.1	1	1,440	60
Accounting and controlling	22.0 (N=1,782)	93.4	24 (N=310)	73.3	169.4	1	1,440	60
Web presence	14.6 (N=1,777)	68.0	12 (N=161)	337.2	1,463.2	1	8,760	365
Other software to provide services	11.7 (N=1,786)	87.7	24 (N=172)	88.7	166.6	1	720	30
Banking and Trading	9.4 (N=1,783)	92.6	24 (N=117)	43.9	110.2	1	2,160	90
Warehousing and logistics	8.0 (N=1,778)	85.3	24 (N=103)	72.9	151.7	1	720	30
Production control	5.3 (N=1,786)	94.1	48 (N=82)	65.3	63.4	1	480	20

(h): hours
(d): days

If the IT systems mentioned above were affected by the most severe cyber-attack, companies could also indicate whether the IT system was (rather) important or (rather) unimportant for the company[293] and how long the system could not be used or could only be used to a limited extent.

A large proportion of the IT systems affected by the most severe cyber-attacks of the last twelve months are (rather) important for companies. With the smallest share of 68.0 %, the web presence is less (rather) important than order and customer management, at the upper end with a share of 95.3 % (Table 29). With regard to the downtimes of the IT systems ("not or only to a very limited extent usable"), very wide ranges can be seen, ranging from one hour to one year

[293] The background to this question is the consideration that the failure of certain IT systems has different degrees of severity for companies. For example, the failure of the web presence of a retail trade that does its main business locally is likely to have less severe consequences than for an online mail order business whose existence depends on the functioning of its web presence.

(website: 8,760 hours or 365 days[294]). For this reason, the median, which is more robust compared to extreme values, appears to be the more suitable location parameter for describing the distribution compared to the arithmetic mean. In a comparison of the affected (rather) important IT systems, this lies between 12 hours for web presence and 48 hours for production control. In other words, in 50.0 % of the companies affected, the (rather) important web presences took no more than half a day and the (rather) important production control systems took no more than two days. The other 50.0 % had to cope with correspondingly higher downtimes. In relation to the other IT systems, the median downtime is 24 hours. It is also noticeable that production control systems are the least affected, at 5.3 %, but when this is the case, they show the highest downtime (median: 48 hours). At the same time, they also have the lowest maximum downtime at 480 hours, which may indicate that in the event of an attack, companies will restore these systems to an operational state with a high priority.

Table 30 **Downtime of (rather) importantly classified IT systems by cyber-attack type**

Median in hours; weighted data; only data on the most severe cyber-attack

	Cyber-attack type								
IT system	1	2	3	4	5	6	7	8	9
E-mail and communication	24 (N=163)	48 (N=77)	24 (N=182)	3 (N=20)	6 (N=80)	6 (N=19)	1 (N=30)	12 (N=145)	24 (N=705)
Order- and customer management	48 (N=163)	34 (N=36)	48 (N=94)	2 (N=15)	11 (N=9)		1 (N=6)	6 (N=76)	24 (N=393)
Accounting and controlling	48 (N=138)	25 (N=20)	48 (N=59)	10 (N=20)			1 (N=17)	24 (N=58)	24 (N=310)
Web presence	48 (N=22)	24 (N=20)	24 (N=34)		5 (N=54)	45 (N=21)		12 (N=11)	12 (N=161)
Other software to provide services	48 (N=92)	48 (N=17)	24 (N=34)	168 (N=6)				1 (N=17)	24 (N=172)
Banking and Trading	36 (N=38)	43 (N=17)	24 (N=28)					24 (N=29)	24 (N=117)
Warehousing and logistics	36 (N=42)		48 (N=29)	49 (N=10)				24 (N=15)	24 (N=103)
Production control	72 (N=26)	48 (N=9)	48 (N=24)	168 (N=7)				24 (N=15)	48 (N=82)

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing, 9: cyber-attacks in total.

The average downtimes (median in hours) of the individual IT systems classified as (rather) important (Table 30), differentiated according to the type of cyber-attack, can only be interpreted to a limited extent due to the sometimes very small number of cases: Longer downtimes for production control systems and for other software for the provision of services appear to occur particularly as a result of manual hacking (median: 168 hours in each case). If IT systems for production control are affected by ransomware attacks, the downtimes here also appear to be comparatively long (median: 72 hours). Since the CEO-fraud attack type is usually less designed to damage IT systems, one possible explanation would be that these were variants of the CEO-fraud, such as the initiation of unauthorised changes to master data, creation of contact

[294] The value of 365 days of downtime for a website classified as (rather) important seems very high. Further background information could unfortunately not be requested due to time constraints. It would be conceivable, for example, that the downtime was bridged by a parallel web presence.

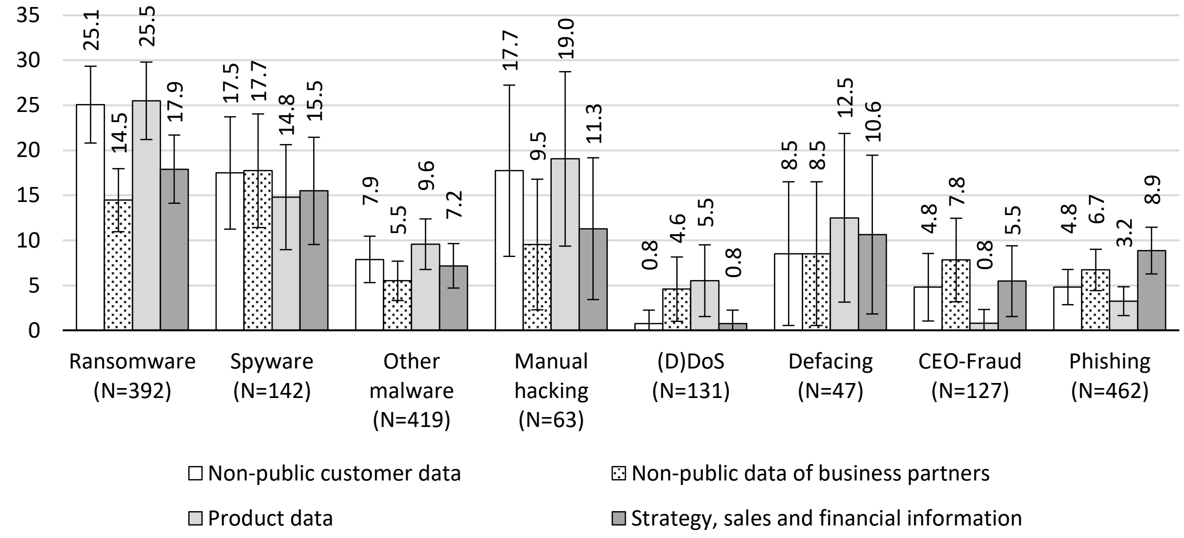
information or creditors/debitors by using social engineering. However, it is also possible that, for example, the duration of forensic measures or system maintenance as a result of the attack was subsumed under this.

9.5.2 Affected data

The data affected by the respective types of attack were collected differentiated according to non-public data of customers (e.g. access data, bank data, addresses, patient data)[295], non-public data of business partners (e.g. access data, bank data, addresses), product data (e.g. construction plans, recipes, source codes) as well as strategy, sales, and financial information (e.g. price lists, reorganisation plans, acquisitions, financial and accounting data). In around a quarter of the companies, the most severe cyber-attack in the previous year affected such data (25.2 %; N=1,783), i.e. it was unauthorizedly deleted, manipulated, stolen/copied or encrypted.

As far as their impact is concerned, no statistically relevant differences can be found either between the different types of data or between companies of different employee size classes.

Figure 59 **Proportion of affected companies by data and attack type**
in percent; weighted data; 95 % CI; only data on the most severe cyber-attack



On the other hand, significant differences within and between the types of attack are in some cases discernible (Figure 59): For example, companies reporting a ransomware attack as the most severe cyber-attack are particularly affected by non-public customer data (25.1 %) and product data (25.5 %) and less by non-public data from business partners (14.5 %) and strategic, sales, and financial information (17.9 %). At the same time, as expected, this type of attack generally affects data more than a (D)DoS or phishing attack. It is also not apparent that spyware attacks are particularly targeted at specific data, e.g. product or strategy information, in order to carry out targeted espionage.

[295] The first category, customer data, is therefore personal data within the meaning of the European Data Protection Regulation. In the case of the second category, data of business partners, it may also be personal data. However, this could not be collected individually due to time and complexity reasons.

According to the different degrees to which companies of different WZ08 classes are affected by cyber-attacks, the proportion of data affected by the most severe cyber-attack also varies between the WZ08 classes.

Table 31 **Share of Companies with affected data by data type and WZ08 classes**

in percent; weighted data

	Data type					
WZ08 classes (level 1; short name; only if N≥30)	1	2	3	4	5.	N
Manufacturing (WZ08-C)	25.2	10.5	7.2	10.5	11.5	388
Construction (WZ08-F)	20.3	5.3	9.7	7.7	5.3	207
Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles (WZ08-G)	32.2	14.9	**15.1**	**20.2**	11.7	375
Transportation and Storage (WZ08-H)	18.5	12.7	1.9	9.1	7.4	54
Accommodation and Food Service Activities (WZ08-I)	17.2	14.3	11.1	1.6	1.6	63
Information and Communication (WZ08-J)	3.1	1.5	1.5	1.5	1.5	65
Professional, Scientific and Technical Activities (WZ08-M)	25.7	9.8	9.3	16.0	13.4	185
Administrative and Support Service Activities (WZ08-N)	33.0	**16.1**	11.0	4.4	14.3	90
Education (WZ08-P)	22.3	10.7	3.3	11.6	9.1	121
Human Health and Social Work Activities (WZ08-Q)	**36.1**	13.4	8.5	4.8	**22.0**	82
Other Service Activities (WZ08-S)	10.0	2.6	2.5	2.8	5.0	39

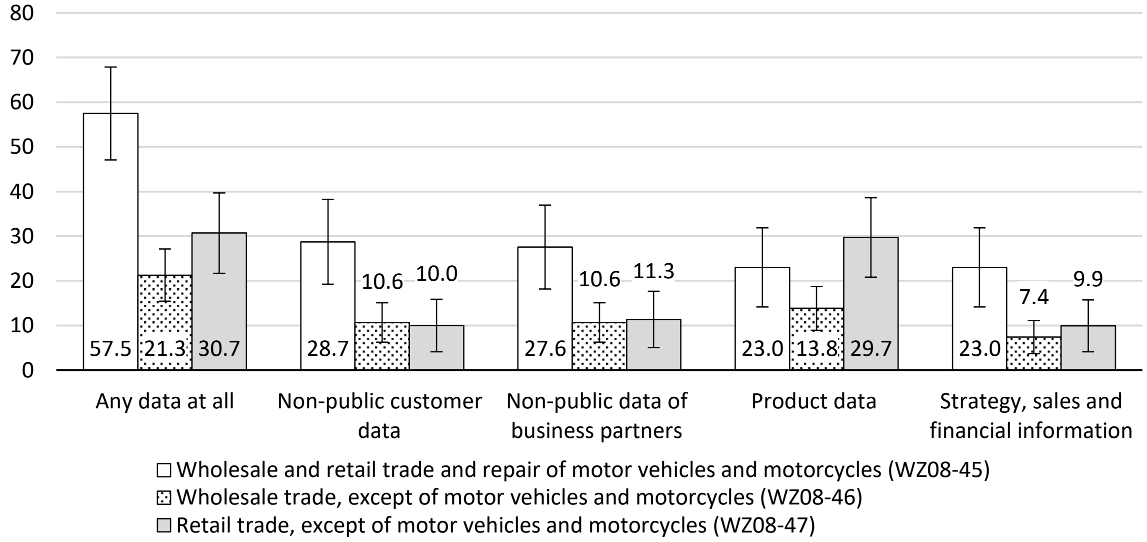
Data type: 1: Data in total, 2: non-public customer data, 3: non-public data of business partners, 4: Product data, 5: Strategy, sales and financial information.

Highlighting: bold: largest share per data type; grey background: the three largest shares per data type

The WZ08 class G (trade; maintenance and repair of motor vehicles), for example, was relatively frequently affected by attacks with malware (ransomware, spyware and other malicious software)[296] and, as expected, counts WZ08 classes whose companies are more frequently affected by data (data in total: 32.2 %). This is particularly product data and non-public data of business partners.

Figure 60 **Affected data by WZ08 classes**

in percent; weighted data; 95 % CI; multiple answers possible



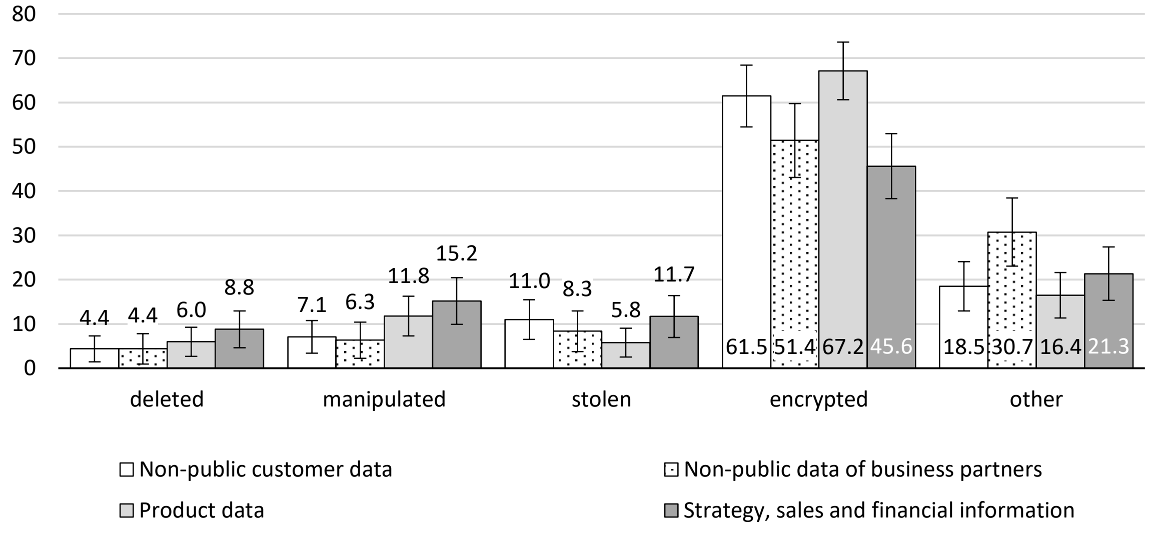
[296] See section 7.1.2 Table 24.

As far as the second level of the WZ08 classes is concerned, wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45), is particularly affected (Figure 60). Only in terms of product data, retail trade, except of motor vehicles and motorcycles (WZ08-47) is at least tending to be more affected. With regard to affected strategy, sales and financial information, manufacturing of machinery and equipment (WZ08-28) have the highest share (30.4 %).[297]

In addition to the fact that the data were affected, the question was asked what happened to these data. Possible answers were: "deleted", "manipulated", "stolen", and "encrypted".[298]

In most cases, the data concerned was encrypted, and this was particularly true for product data (67.2 %) compared to non-public data of business partners (51.4 %) and strategy, sales and financial information (45.6 %) (Figure 61). In contrast, product data was manipulated significantly more frequently (15.2 %) than non-public data from customers (7.1 %) and business partners (6.3 %).

Figure 61 **Consequences for the affected data by data type**
in percent; weighted data; 95 % CI; multiple answers possible



9.5.3 *Cost items*

Whether costs were incurred as a result of the most severe cyber-attack of the last twelve months, the following cost items were inquired: costs for external advice & support (e.g. legal advice, emergency management), defence & investigation, fines & compensation payments, drain off financial means, business interruption/revenue loss and costs for recovery & replacement. For almost one third of the companies (30.0 %; N=1,772), the most severe cyber-attack did not incur such costs. 28.6 % reported costs for one of these six items, 24.7 % for two and

[297] As can be seen from these examples, such differences and anomalies at the second level of the WZ08 classes are not always reflected at the first level. A more differentiated comparison is therefore worthwhile (see Table 52 in Annex 1).

[298] In the survey, the survey institute added the category "other" because the respondents perceived the answer options as not being exhaustive. This could be due, for example, to the fact that the category "stolen" was misunderstood in that the theft was associated with the simultaneous loss of the data. In future surveys, the term "unauthorised copy/use/view" or similar could be used instead.

the remaining 16.7 % for three or more items. The amount of the costs is not taken into account for the time being.

Table 32 **Proportion of companies with costs resulting from the most severe cyber-attack**
in percent; weighted data; multiple answers possible; bold: significant at p<.05 (Chi² test)

		Employee size class				
Cost item	Total	10-49	50-99	100-249	250-499	500+
External advice & support	30.3	**31.9**	**28.2**	**23.3**	**21.2**	**14.3**
Defence & investigation	39.9	**41.4**	**36.6**	**33.6**	**33.8**	**41.7**
Fines & compensation	1.4	1.5	1.1	2.0	0.5	1.2
Drain off financial means	2.2	2.0	3.4	2.5	1.2	3.5
Business interruption	25.7	26.6	24.1	23.5	23.8	17.1
Replacement & recovery	33.0	**34.9**	**29.7**	**24.0**	**23.5**	**26.5**
Costs incurred for at least one item	70.0	**72.3**	**65.7**	**60.4**	**62.6**	**64.5**
N	1,772	404	467	447	425	259

For the most frequently cited items, costs were incurred as a result of the most severe cyber-attack (defence & investigation: 39.9 %; replacement & recovery: 33.0 % and external advice & support: 30.3 %), there are statistically significant differences between the employee size classes (Table 32): small companies thus incurred costs for external advice & support and replacement & recovery much more frequently (10-49 employees: 31.9 % and 34.9 % respectively) than for large companies (50 or more employees: 14.3 % and 26.5 % respectively). Costs for defence & investigation were most frequently incurred in small and large companies (10-49 employees: 41.4 %; 500+ Employees: 41.7 %) and least frequently in companies with 100-249 employees (33.6 %) and 250-499 employees (33.8 %). Costs of business interruption also tended to be more common in small companies than in large companies (10-49 employees: 26.6 %; 500 employees and over: 17.1 %), while costs of fines & compensation and drain off financial means were similarly low in all sizes of company and were only in the low single-digit percentage range.

Differentiated by type of attack (Table 33), it can be seen that the companies that identified ransomware, spyware and manual hacking as the most severe attacks incurred costs significantly more frequently (85.9 %, 86.6 %, and 80.6 % respectively) than the other types of attack (e.g. CEO fraud: 46.0 %). Looking at the largest shares per cost item, it can be seen, for example, that contrary to the obvious assumption, drain off financial means due to manual hacking (20.6 %) plays a proportionately greater role than, for example, in the case of the CEO Fraud (6.3 %).

Looking at which cost items were most frequently mentioned for the respective types of attack, further differences become apparent: For ransomware and manual hacking, replacement & recovery is the most frequently mentioned cost item (52.4 % and 50.0 %, respectively), while for all other types of attack, although with varying frequency, the item is defence & investigation.

Table 33 **Percentage of companies with costs resulting from the most severe cyber-attack by type of attack**
in percent; weighted data; multiple answers possible

	Cyber-attack type							
Cost item	1	2	3	4	5	6	7	8
External advice & support	37.6	45.8	36.9	35.5	21.2	37.5	20.3	17.6
Defence & investigation	45.7	**49.0**	**44.0**	43.5	**35.6**	**42.6**	**26.8**	**33.2**
Fines & compensation	1.5	0.0	2.6	8.1	0.8	0.0	0.0	0.6
Drain off financial means	1.5	0.0	0.2	20.6	0.0	0.0	6.3	2.6
Business interruption	42.0	34.8	28.6	29.5	19.7	17.0	9.3	13.7
Replacement & recovery	**52.4**	34.3	34.6	**50.0**	25.0	38.3	5.6	20.9
Costs incurred for at least one item	85.9	86.6	78.1	80.6	61.8	72.3	46.0	50.8
N	398	142	415	62	131	47	124	459

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing
Highlighting: bold: largest share per type of attack; underlined: largest share per cost item

Costs for external advice & support and for defence & investigation were most common after spyware attacks (45.8 % and 49.0 % respectively). Fines & compensation payments and drain off financial means were most frequently reported for manual hacking (8.1 % and 20.6 %, respectively). Costs resulting from business interruption and replacement & recovery were most common after ransomware attacks (42.0 % and 52.4 %).

9.5.4 Amount of costs

In general, reliable studies on the damage caused by cyber-attacks are rare. This rarity is also due, among other things, to the difficulty of operationalization, the moderate willingness of companies to provide information and the fact that only a few companies actually determine and track the costs incurred.[299] Indirect costs such as damage to the company's reputation, loss of orders or competitive disadvantages, which can occur with a significant time lag from the cyber-attack, can hardly be realistically quantified.

Looking at direct costs caused by the most severe cyber-attack of the last twelve months, it should therefore be taken into account that the figures are often approximates. The total costs across all the cost items surveyed above were therefore only calculated if valid responses for all cost items were available. Non-valid values in this case are the answers "Not specified" or "I do not know". Of the 70.0 % of companies that stated that costs were incurred for at least one of the items (N=1,772), no total costs could be calculated for 30.9 % (N=1,240) due to missing information on the approximate cost amount of single items. This means that only "secured" and complete information on direct total costs was included and cases with unclear cost items or cost amounts were not taken into account in order to determine the most realistic possible indication of the total direct costs incurred.

For those companies where costs were incurred, and all relevant information was available, total costs ranged from EUR 10 to EUR 2 million and averaged around EUR 16,900 (N=857).

[299] Also, Klahr et al. (2017) report that it is unusual for companies to identify and track financial costs of cybersecurity incidents.

The average costs tended to be higher in larger companies than in smaller ones, and when comparing the cost items, drain off financial means were found to have the highest average costs of around EUR 27,900 (Table 34).

Table 34 **Average costs by cost item and employee size class**

in EUR; rounded; weighted data; multiple answers possible; only companies with costs

		Employee size class				
Cost item	Total	10-49	50-99	100-249	250-499	500+
External advice & support	1,900 (N=412)	1,600 (N=99)	2,000 (N=104)	5,300 (N=78)	4,800 (N=69)	3,900* (N=25)
Defence & investigation	8,800 (N=559)	7,200 (N=136)	15,200 (N=122)	8,500 (N=103)	13,500 (N=102)	33,200 (N=73)
Fines & compensation	4,200* (N=23)	2,700* (N=6)	1,000* (N=3)	12,200* (N=6)	50,000* (N=1)	31,600* (N=3)
Drain off financial means	27,900 (N=30)	24,700* (N=7)	48,700* (N=9)	6,700* (N=5)	16,900* (N=3)	47,700* (N=7)
Business interruption	12,000 (N=283)	10,700 (N=70)	10,000 (N=55)	22,600 (N=49)	48,100 (N=53)	12,200* (N=20)
Replacement & recovery	13,100 (N=487)	13,100 (N=121)	11,900 (N=107)	20,100 (N=77)	2,500 (N=76)	7,800 (N=53)
Total costs	16,900 (N=857)	15,900 (N=208)	18,500 (N=194)	19,500 (N=158)	22,900 (N=167)	31,200 (N=98)

*) very low number of cases (N < 30)

Since average values can be strongly influenced by extreme values, the median, which is more robust in comparison, is also given, dividing the distribution into two equally large halves. The median of the total costs across all cost items is EUR 1,000, i.e. if costs were caused by the most severe cyber-attack, they were up to EUR 1,000 in one half of the companies and over EUR 1,000 in the other half, with no significant differences between the employee size classes. But, small companies tend to have lower costs more often than large ones (Table 35). However, it should be borne in mind that there are sometimes significant differences between the employee size classes with regard to the prevalence of the various types of cyber-attacks.

Differentiated according to single cost items, it is noticeable that the medians of the costs of external advice & support and for defence & investigation are significantly lower (EUR 870 and EUR 800 respectively) than the medians of the costs incurred by drain of financial means and business interruptions (EUR 2,000 each).

Table 35 **Median costs by cost item and employee size class**

in EUR; rounded; weighted data; multiple answers possible; only companies with costs

	Employee size class					
Cost item	Total	10-49	50-99	100-249	250-499	500+
External advice & support	870 (N=412)	790 (N=99)	1,000 (N=104)	1,000 (N=78)	1,000 (N=69)	2,000* (N=25)
Defence & investigation	800 (N=559)	600 (N=136)	1,000 (N=122)	1,000 (N=103)	1,000 (N=102)	1,500 (N=73)
Fines & compensation	910* (N=23)	670* (N=6)	850* (N=3)	8,550* (N=6)	50,000* (N=1)	11,110* (N=3)
Drain off financial means	2,000 (N=30)	2,760* (N=7)	2,000* (N=9)	3,620* (N=5)	15,700* (N=3)	31,250* (N=7)
Business interruption	2,000 (N=283)	2,000 (N=70)	3,000 (N=55)	5,000 (N=49)	2,810 (N=53)	5,000* (N=20)
Replacement & recovery	1,000 (N=487)	1,000 (N=121)	800 (N=107)	1,000 (N=77)	800 (N=76)	1,100 (N=53)
Total costs	1,000 (N=857)	1,000 (N=208)	1,200 (N=194)	1,500 (N=158)	1,500 (N=167)	1,470 (N=98)

*) very low number of cases (N < 30)

Table 36 **Average costs by cost item and cyber-attack type**

in EUR; rounded; weighted data; multiple answers possible; only companies with costs

	Cyber-attack type							
Cost item	1	2	3	4	5	6	7	8
External advice & support	1,900 (N=93)	1,200 (N=56)	1,600 (N=126)	6,800* (N=18)	2,100* (N=24)	1,700 (N=11)	1,900* (N=24)	1,700 (N=61)
Defence & investigation	20,100 (N=133)	5,500 (N=52)	3,000 (N=146)	4,000* (N=23)	14,400 (N=41)	1,600* (N=18)	2,600 (N=30)	6,500 (N=111)
Fines & compensation	2,900* (N=5)		1,300* (N=10)	10,300* (N=5)	100* (N=1)			10,700* (N=2)
Drain off financial means	800* (N=5)			39,900* (N=12)			22,900* (N=2)	28,000* (N=10)
Business interruption	11,900 (N=85)	1,600 (N=30)	9,600 (N=81)	65,100 (N=13)	19,300 (N=16)		32,100 (N=6)	3,600 (N=49)
Replacement & recovery	20,400 (N=172)	1,200 (N=37)	6,600 (N=119)	10,900* (N=26)	27,000 (N=31)	1,200* (N=13)	2,900* (N=6)	7,100 (N=76)
Total costs	32,200 (N=201)	4,700 (N=92)	8,200 (N=230)	43,700 (N=35)	25,600 (N=66)	2,600* (N=21)	8,600 (N=40)	9,300 (N=166)

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing

*) very low number of cases (N < 30)

Further differences can be found when comparing the total direct costs by type of attack (Table 36 and Table 37): For example, the average costs across all items for ransomware attacks and manual hacking are 32,200 EUR and 43,700 EUR (median: 1,300 and EUR 2,800) are significantly higher than the costs of the other types of attack, especially the direct costs of spyware attacks, other malware attacks and defacing (average: EUR 4,700, EUR 8,200 and EUR 2,600 respectively; median: EUR 750, EUR 790 and EUR 990 respectively).

Table 37 **Median costs by cost item and cyber-attack type**

in EUR; rounded; weighted data; multiple answers possible; only companies with costs

	Cyber-attack type							
Cost item	1	2	3	4	5	6	7	8
External advice & support	1,500 (N=93)	550 (N=56)	500 (N=126)	2,000* (N=18)	1,000* (N=24)	100 (N=11)	1,460* (N=24)	500 (N=61)
Defence & investigation	1,000 (N=133)	750 (N=52)	500 (N=146)	2,000* (N=23)	1,000 (N=41)	990* (N=18)	500 (N=30)	1,000 (N=111)
Fines & compensation	100* (N=5)		990* (N=10)	10,000* (N=5)				
Drain off financial means	500* (N=5)			5,000* (N=12)			19,700* (N=2)	2,000* (N=10)
Business interruption	2,000 (N=85)	1,500 (N=30)	2,000 (N=81)	100,000* (N=13)	10,000* (N=16)		500* (N=6)	740 (N=49)
Replacement & recovery	1,000 (N=172)	400 (N=37)	1,000 (N=119)	4210* (N=26)	1,000 (N=31)	950* (N=13)	1,000* (N=6)	500 (N=76)
Total costs	1,300 (N=201)	750 (N=92)	790 (N=230)	2,800 (N=35)	1,090 (N=66)	990* (N=21)	1,000 (N=40)	1,000 (N=166)

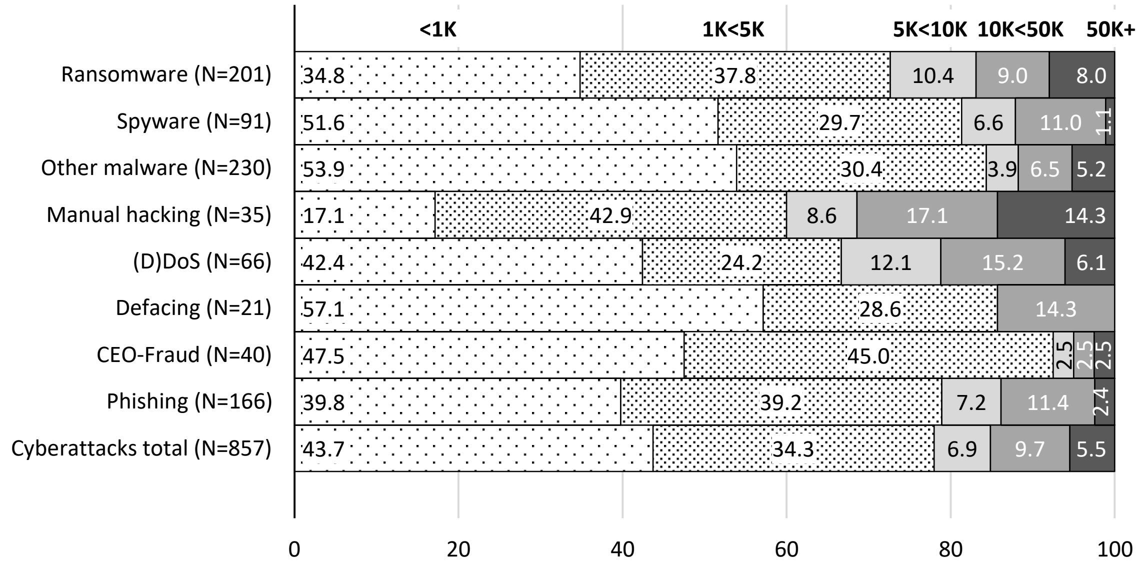
Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing

*) very low number of cases (N < 30)

With the restriction that the underlying case numbers are in part very small, it can be shown with all due caution that the relatively rare manual hacking caused relatively high costs in all positions, but especially with regard to business interruption as well as fines & compensations, in the median comparison and on average. The higher median cost of business interruption due to manual hacking is also consistent with the longer average downtime of production control systems and other software for this type of attack, as shown in Table 30 above.

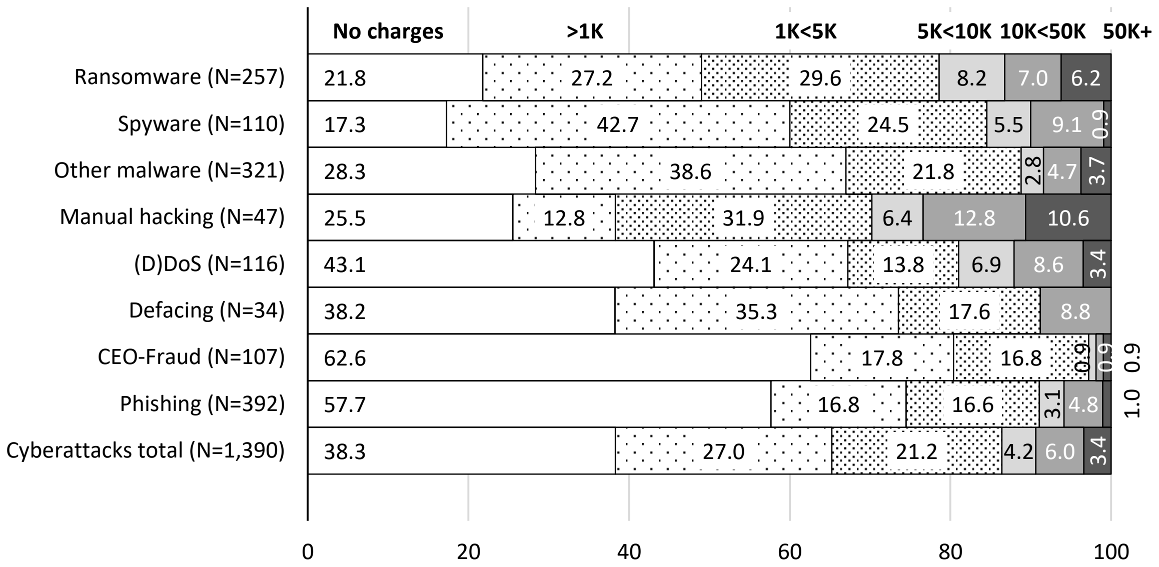
Figure 62 **Classified total costs by cyber-attack type**

in percent; classes in thousand EUR; weighted data; only companies with costs



More generally, it can also be noted that the costs resulting from the different types of attacks were in most cases relatively low (Figure 62): 78.0 % of the most severe cyber-attacks reported had total costs below EUR 5,000 calculated over the cost items surveyed. In 6.9 %, costs of between EUR 5,000 and EUR 10,000 were incurred, in 9.7 % between EUR 10,000 and EUR 50,000, and in a small proportion of cases (5.5 %) the total costs were EUR 50,000 or more.

Figure 63 **Classified total costs by cyber-attack type**
in percent; classes in EUR thousand; weighted data



If the companies that have not incurred any costs from the most severe cyber-attack in the last 12 months are included as a further class (Figure 63), it becomes even clearer that only a relatively small proportion had to deal with major direct costs: in relation to all cyber-attacks as a whole, the proportion of companies that have either not incurred any costs or have incurred costs of less than EUR 5,000 is 86.4 %. It is also noticeable that the proportion of companies without costs differs between the types of cyber-attack. More than half of the companies that reported CEO fraud or phishing in connection with the most severe cyber-attack did not have to pay any of the costs surveyed (62.6 % and 57.7 respectively). In contrast, this proportion is significantly lower for malware attacks (spyware: 17.3 %, ransomware: 21.8 %, other malware: 28.3 %) and manual hacking (25.5 %).

With regard to comparable literature, it is noticeable that, apart from the limitations mentioned at the beginning of the section, it is above all the object of consideration of the most severe attack that leads to the fact that direct comparisons are hardly possible. The vast majority of studies to date estimate the costs of cyber-attacks over a certain period of time[300] (e.g. the last 12 months) and not for a specific incident.[301]

The British insurance group Hiscox, on the other hand, gives estimated average costs for the largest cybersecurity incident in the last 12 months (survey period: autumn 2017). According to the survey, German companies are even more affected than Dutch, Spanish, British and US companies and have average costs of USD 11,918 (up to 249 employees), USD 86,834 (250 to 999 employees) and USD 150,891 (more than 1,000 employees). Although the exact cost components and other structural characteristics are not disclosed, overall the cost estimates appear

[300] See for example Klahr et al. (2017); Rantala (2008); Vanson Bourne (2014).

[301] A reference to the most severe attack is made, for example, in Paoli et al. (2018), but only as a cost category, without specifying the average total cost in EUR (e.g. median).

to be higher than the results of this study.[302] Klahr et al. also refer, among other things, to the most severe attack of the last 12 months: If direct costs were incurred in these, they were estimated at an average of GBP 1,320 (median: GBP 150).[303] These cost figures are thus lower than those in this study.[304] This is also true when it is taken into account that the sample of Klahr et al. includes micro-companies with less than ten employees.[305]

It remains completely undisputed that cyber-attacks in general can result in high costs for companies and that extreme events can actually occur. According to the available results of the self-disclosure-based estimates of the interviewed persons, however, only a few companies seem to be affected by extremely high direct costs caused by cyber-attacks.

9.6 Information and police reporting behaviour

9.6.1 Information of non-governmental bodies

Regarding the most severe attack, the company representatives were asked which non-governmental body were informed about the incident. They were given a choice of possible answers: Customers, business partners, insurers, company owners and the public. The way in which the information was obtained (about the company itself or by other means) was left out.

Table 38 **Non-governmental body which has learned of the incident, by employee size class**
in percent; weighted data; multiple answers possible; bold: significant at p<.05 (Chi² test)

		Size classes of persons employed				
Non-governmental body	Total	10-49	50-99	100-249	250-499	500+
Customers	15.5	**16.8**	**11.1**	**11.9**	**10.4**	**11.9**
Business Partner	21.4	**23.1**	**16.2**	**16.0**	**13.6**	**13.8**
Insurer	9.1	9.2	9.1	8.4	9.7	9.2
Owners of the company	91.5	**93.4**	**88.5**	**85.8**	**85.9**	**76.0**
Public	4.0	4.4	3.1	2.5	2.1	1.9
N	1,769	406	455	442	424	258

In most cases, the owners were informed about the most severe cyber-attacks (91.5 %), although this was significantly more common in small companies (10-49 employees: 93.4 %) than in large companies (500+ employees: 76.0 %; table 38). As a rule, this will be due to the fact that the owners of small companies also play an active role in the management of the company more often than in large companies. About one-fifth (21.4 %) of the most severe attacks reported were reported to the companies' business partners, and 15.5 % to customers. Here, too, there are statistically relevant differences between the employee size classes, in that business partners and customers were informed more often in small companies than in large ones (10-

[302] Cf. Hiscox (2018). At the current exchange rate of USD 1.11 per EUR, the average total costs for companies with ten or more employees where costs have been incurred are around USD 18,700 in this study.

[303] Cf. Klahr et al. (2017).

[304] At the current exchange rate of GBP 0.86 per EUR, the average total costs for companies with 10 or more employees where costs have been incurred are around GBP 14,500 in this study. The median is then GBP 860.

[305] For large companies with 250 or more employees, for example, direct average costs are reported as GBP 4,270 (median: GBP 870). In comparison, for companies with 250-499 employees, these costs are converted to GBP 19,700 (median: GBP 1,290) in this study.

49 employees: 23.1 % and 16.8 % respectively; 500 employees and over: 13.8 % and 11.9 % respectively). In 9.1 % of cases, insurers obtained information about the most severe attack, and only in 4.0 % of cases did the public obtain information. Even if the differences between the employee size classes are statistically insignificant in this respect, it is at least tending to be apparent with regard to the public that the public is more likely to be informed about incidents involving small companies than the larger ones.

Differentiated according to cyber-attack types, manual hacking and defacing attacks are particularly striking, of which non-governmental bodies became aware relatively frequently (Table 39). The types of cyber-attacks of which information reached these offices relatively rarely include CEO fraud, phishing and attacks with other malicious software: With regard to the most severe cyber-attacks, business partners, for example, only 10.9 % and 14.9 % of the companies affected by CEO fraud and phishing, respectively, received information from more than a third of the companies affected by (D)DoS (37.1 %).

Table 39 **Non-governmental entity that learned of the incident, by cyber-attack type**
in percent; weighted data; multiple answers possible

	Cyber-attack type							
Non-governmental body	1	2	3	4	5	6	7	8
Customers	16.7	23.2	10.1	29.0	35.2	**52.4**	6.3	9.9
Business Partner	27.0	23.2	18.1	30.6	**37.1**	31.9	10.9	14.9
Insurer	14.1	9.2	7.7	**25.8**	12.2	6.4	3.3	5.5
Owners of the companies	96.0	95.8	89.9	96.8	84.0	**100.0**	84.4	90.3
Public	3.5	4.9	3.6	22.6	5.3	**26.2**	0.8	1.1
N	395	142	413	62	131	45	127	462

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing
Highlighting: bold: largest share per non-governmental body; grey background: the three largest shares per non-governmental body

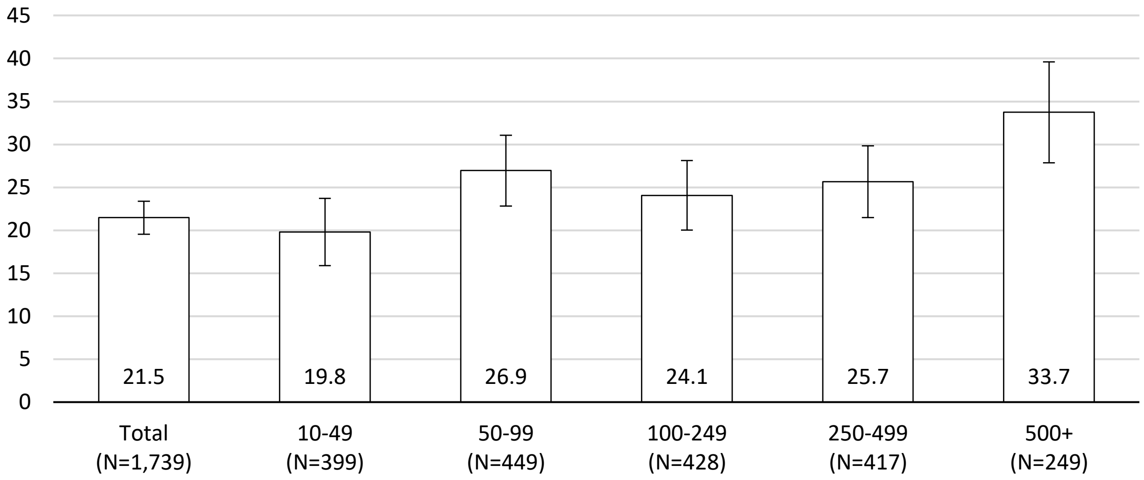
9.6.2 Contact with government agencies

In addition, in relation to the most severe cyber-attack of the last twelve months, company representatives were asked where the company had turned to about this incident. The following possible answers were given: nearest police station, police station specialising in cybercrime, Office for the Protection of the Constitution, Federal Office for Information Security (BSI), State Data Protection Commissioner and others.[306] Initially, it is not taken into account whether the companies have filed criminal charges or not.[307]

[306] The category "other" was not surveyed in free text in the survey for reasons of time economy.

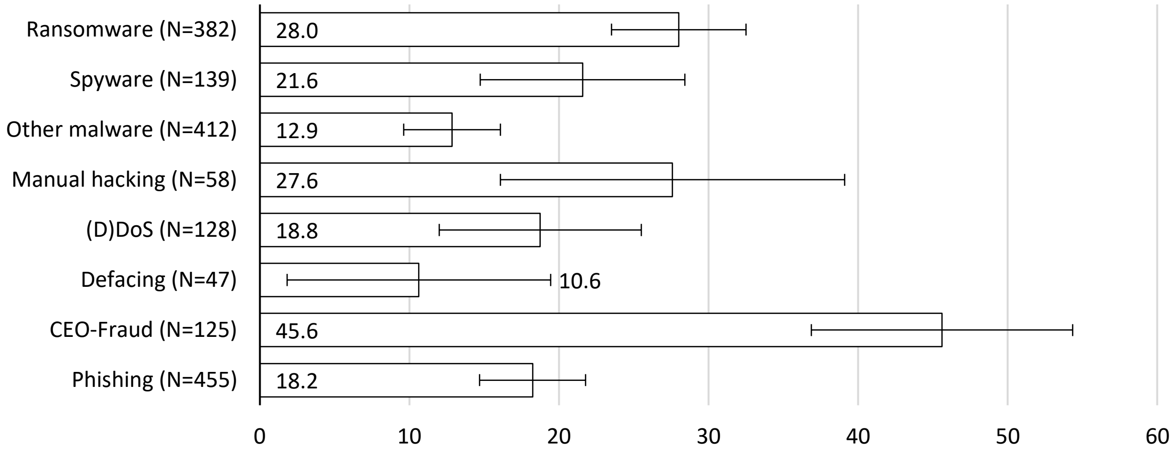
[307] Cybercrime offences often fall within the scope of official offences, i.e. they must be prosecuted ex officio by law enforcement authorities as soon as they become aware of them. In the case of offences such as data modification according to § 303a StGB or data spying according to § 202a StGB, on the other hand, a criminal complaint by the reporting company is required so that the prosecuting authorities can begin the investigation or begin and advance the criminal proceedings. The BSI, the Office for the Protection of the Constitution and the State Data Protection Commissioner are not among the criminal prosecution authorities.

Figure 64 **Affected companies with contact to public authorities by employee size class**
in percent; weighted data; 95 % CI; only data on the most severe cyber-attack



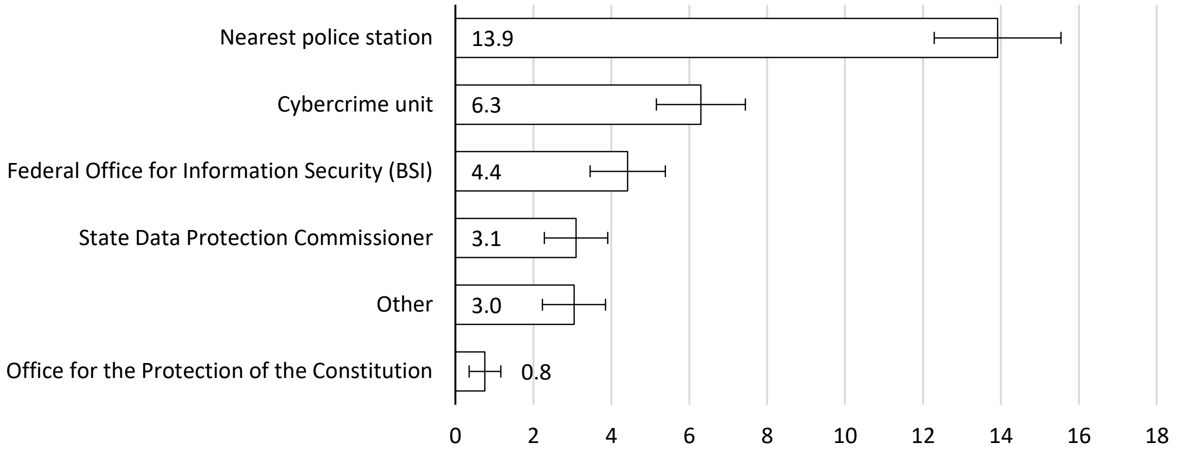
At least one of these public authorities has been contacted by a good fifth of the companies affected by cyber-attacks (21.5 %), with the proportion being significantly higher for large companies (500+ employees: 33.7 %) than for small companies (10-49 employees: 19.8 %; Figure 64).

Figure 65 **Affected companies with contact to authorities by cyber-attack type**
in percent; weighted data; 95 % CI; only data on the most severe cyber-attack



Almost half (45.6 %) of companies affected by CEO fraud turned to at least one government agency (Figure 65). Companies were the least likely to turn to the authorities as a result of a defacing attack (10.6 %) or an attack with other malware (12.9 %).

Figure 66 **Affected companies with contact to public authorities by public authorities**
in percent; weighted data; 95 %-CI; multiple entries possible; N=1,739



When broken down by the various agencies, the companies concerned most frequently contacted the nearest police station, accounting for 13.9 % of the total (Figure 66). This is followed by police departments specialising in cybercrime (6.3 %), the BSI (4.4 %), the State Data Protection Commissioner (3.1 %), others (3.0 %) and the Office for the Protection of the Constitution (0.8 %). There are no statistically relevant differences between the employee size classes, which is probably also due to the relatively small number of cases. However, large companies tend to use (cybercrime specialised) police departments, the BSI and the Office for the Protection of the Constitution more frequently than small companies.

Table 40 **Affected companies with government contact by government agencies and cyber-attack type**
in percent; weighted data; multiple answers possible

	Cyber-attack type							
State agency	1	2	3	4	5	6	7	8
Nearest police station	21.5	11.5	8.5	19.3	4.7	6.3	**34.4**	9.2
Cybercrime unit	7.9	10.8	2.2	1.7	8.6	0.0	**16.0**	4.4
Office for the Protection of the Constitution	1.8	**3.6**	0.0	0.0	0.0	0.0	0.0	0.2
Federal Office for Information Security (BSI)	6.5	5.0	2.9	**17.5**	2.3	0.0	4.8	2.9
State Data Protection Commissioner	4.2	2.9	1.7	**17.2**	0.8	4.3	2.4	2.6
Other	2.9	3.6	2.4	5.2	**7.0**	0.0	3.2	3.3
N	382	139	412	58	128	48	125	455

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing
Highlighting: bold: largest share per government agency; grey background: the three largest shares per government agency

Table 40 shows the proportions of companies, broken down by the type of most severe cyber-attack, that have turned to the various government agencies as a result of these attacks. The nearest police stations were, for example, more frequently contacted by those affected by a CEO fraud attack (34.4 %), a ransomware attack (21.5 %) or manual hacking (19.3 %), but comparatively rarely by (D)DoS attacks (4.7 %). Police departments specialising in cybercrime were also most likely to be contacted by CEO Fraud victims (16.0 %), the Office for the Protection of the Constitution by spyware victims (3.6 %) and the BSI and the State Data Protection

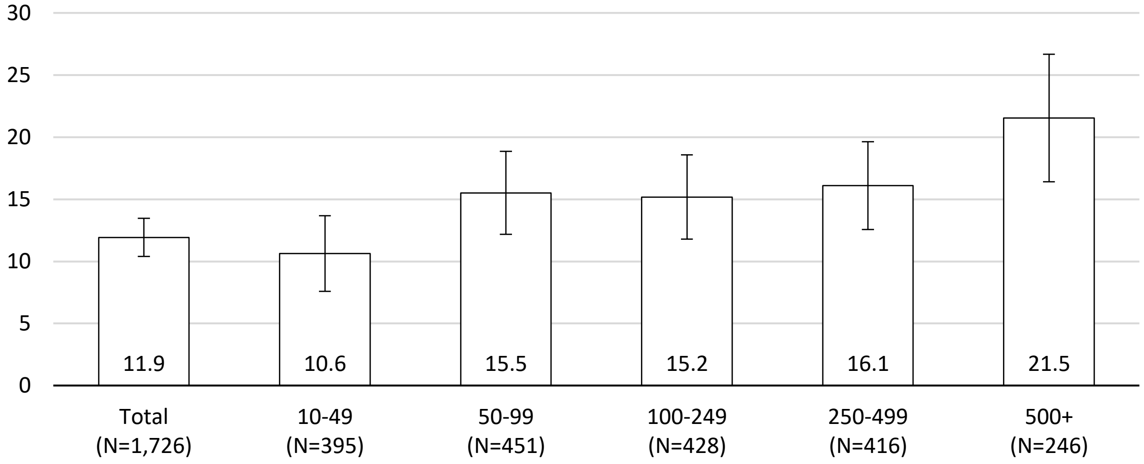
Commissioner by victims of manual hacking (17.5 % and 17.2 % respectively). With regard to the not yet mentioned cyber-attacks of other malware, defacing and phishing, affected companies were most likely to turn to the nearest police station (8.5 %, 6.3 % and 9.2 % respectively).

9.6.3 Reporting to the police

The question of whether the most severe cyber-attack of the last twelve months was reported to the police was affirmed by 11.9 % (Figure 67). This confirms the assumption that there is a high number of non-registered crimes in the area of cybercrime against companies.[308] At 21.5 %, the reporting rate of large companies (500+ Employees) is about twice as high as that of small companies (10-49 employees: 10.6 %). One reason for this could be that, in addition to different attack types experienced by larger organizations, there are also differences in the police reporting behaviour between the different types of cyber-attacks (Figure 68): For example, CEO-fraud, which affects large companies significantly more frequently (Figure 37, p. 104), was the most frequently reported type of cyber-attack with a share of 24.6 %.[309] In addition to CEO fraud, spyware and ransomware attacks (19.7 % and 15.7 % respectively) and manual hacking (19.4 %) are also reported comparatively frequently to the police. The number of non-registered crimes seems to be largest in relation to attacks with other malware and in relation to defacing with police reporting rates of 4.4 % and 6.4 % respectively.

Figure 67 **Police reporting rate by employee size class**

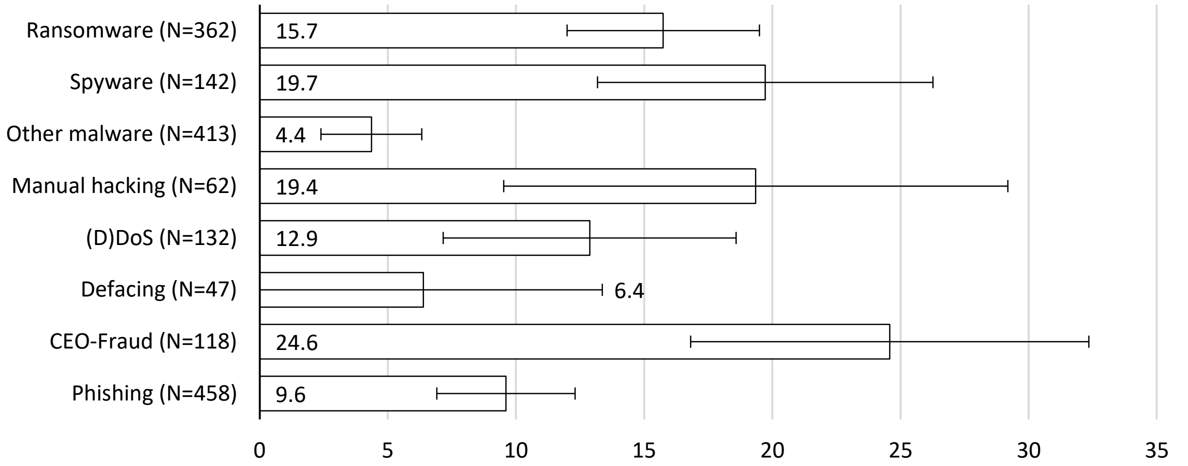
in percent; weighted data; 95 % CI; only data on the most severe cyber-attack



[308] There is also a possibility that the 11.9% police reporting rate is still overestimated, as it relates only to the most severe attacks and less severe incidents are presumably even less likely to be reported.

[309] Why this is so, however, remains open and can only be guessed at this point. Possible explanatory factors could be, for example, the type of data involved, the amount of costs incurred, the existence of cyber insurance or any suspicions about the perpetrators. For factors that influence the police reporting behaviour of private individuals in the context of cybercrime, see van de Weijer et al. (2019).

Figure 68 **Police reporting rate by cyber-attack type**
in percent; weighted data; 95 % CI; only data on the most severe cyber-attack



The differences in the police reporting rates between the employee size classes, differentiated by type of attack, are not statistically significant for the more common attack types ransomware and phishing. Due to the small number of cases, especially in the subgroups of the less frequently occurring attack types, no further comparison is possible.

9.6.4 Reasons for not reporting to the police

If the most severe cyber-attack was not reported to the police, the company representatives were able to give the main reasons for this. Among the possible answers given were: "Because there was a risk of damage to the company's image", "Because there was a risk of disruption to work", "Because authorities might demand access to confidential data", "Low chance of success in the investigation", "I didn't know who to turn to for this" and "Other reasons".[310]

Table 41 **Reasons for not reporting to the police by employee size class**
in percent; weighted data; multiple answers possible; bold: differences significant at p<.05 (Chi² test)

		Position within the company			Employee size class				
Why didn't you file a reporting to the police?	Total	Manage-ment	IT	Other-wise.	10-49	50-99	100-249	250-499	500+
Because there was a risk of damage to the company's image	3.0	**4.9**	**1.6**	**1.1**	2.5	3.8	3.6	8.5	2.5
Because there was a risk of disruption to work	11.3	**18.4**	**7.5**	**2.1**	11.9	12.6	10.8	6.7	3.7
Because authorities might demand access to confidential data	5.0	**8.5**	**2.9**	**1.1**	5.1	4.9	2.4	6.1	2.5
Low chance of success in the investigation	72.0	**77.7**	**74.3**	**47.9**	72.3	75.3	70.1	71.2	67.9
I didn't know who to turn to for this	20.7	**29.9**	**10.7**	**25.5**	**22.6**	**22.5**	**15.6**	**12.3**	**6.1**
Other reasons	30.1	**23.9**	**30.6**	**46.8**	28.9	31.7	32.5	36.8	35.8
N	686	284	308	94	159	183	167	164	82

[310] For reasons of economy of time, the category "other" was not included in the free text of this question. Moreover, for precisely these reasons, a split-half method was used, according to which only half of the participating companies were asked this question (see Section 5.4).

Only 3.0 % of the company representatives stated that fears of damage to the company's image were a reason for not reporting to the police (Table 41). Fears that authorities might ask for access to confidential data were also rarely mentioned (5.0 %). In one in nine companies that did not report the most severe cyber-attack to the police, there were concerns that the investigation would disrupt work in the company (11.3 %). About one-fifth said they did not know who to report cyber-attacks to (20.7 %) and almost three-quarters said that the investigations did have low chances of success (72.0 %). The category "other" was also mentioned comparatively frequently (30.1 %). Here it can be assumed that an increased workload for the report, which is offset by a low expected benefit, was included. This was not given as a single answer option in the telephone interviews.

There are only statistically relevant differences between the employee size classes in terms of not knowing exactly who to turn to for a report to the police: this answer was given significantly more often by small companies than by large companies (10-49 employees: 22.6 % and 50-99 employees: 22.5 % vs. 6.1 % for 500+ employees). This could be related to the positions of the company representatives, insofar as the lack of knowledge in management seems to be more pronounced in this respect than among IT employees (29.9 % vs. 10.7 %) and management was surveyed above all in small companies. With the exception of the lack of prospect of success of the investigation, which is given about equally often by management and IT employees as the reason for not reporting the case, management and IT employees give all other reasons more frequently than IT employees. In particular, the fear of work impediments seems to have a relatively high influence on the decision for or against a report in this group.

Table 42 **Reasons for not reporting to the police by cyber-attack type**
in percent; weighted data; multiple answers possible

	Cyber-attack type							
Reason for not reporting to the police	1	2	3	4	5	6*	7	8
Because there was a risk of damage to the company's image	4.4	12.2	0.6	6.5	0.0	0/18	2.6	3.2
Because there was a risk of disruption to work	13.1	12.5	5.2	19.4	13.7	1/18	16.2	11.8
Because authorities might demand access to confidential data	4.4	10.4	0.6	32.3	0.0	0/18	0.0	5.9
Low chance of success in the investigation	**82.5**	**75.0**	**64.4**	**96.8**	**72.0**	**13/18**	**60.5**	**68.3**
I didn't know who to turn to for this	21.2	27.1	21.3	16.1	29.4	2/18	18.4	18.3
Other reasons	35.8	8.3	40.2	19.4	18.0	6/18	31.6	27.4
N	137	48	174	31	51	18	38	186

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing
*) Due to the small number of cases, indication in absolute numbers
Highlighting: bold: largest share per cyber-attack type; grey background: the three largest shares per cyber-attack type

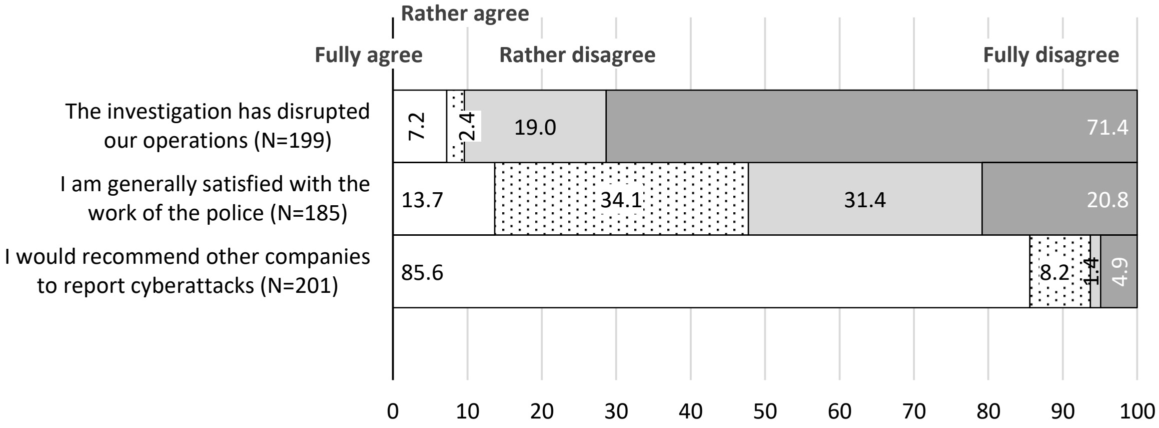
When comparing the reasons for not reporting by cyber-attack type, it is first of all striking that the lack of any prospect of success in the investigation prevented many companies from reporting the most severe attack of the last twelve months (Table 42). However, this seems to be more the case for manual hacking and ransomware attacks (96.8 % and 82.5 % respectively) than for other malware or CEO fraud (64.4 % and 60.5 % respectively). With regard to manual hacking, a significantly higher proportion of respondents were concerned that the authorities might demand access to confidential data (32.3 %) than for companies affected by other types of attack. On the other hand, not knowing who to contact for reports seems to be less important in the case of manual hacking (16.1 %) than in the case of other types of attack, especially (D)DoS attacks (29.4 %). The frequently mentioned category "other" (e.g. in context of ransomware attacks or attacks with other malware: 35.8 % and 40.2 %), refers to further reasons that play a role in the decision not to report cyber-attacks and that should be taken into account in future research.

9.7 Assessment of law enforcement agencies

For the evaluation of the work of the police or law enforcement agencies in cases where the most severe cyber-attack of the last twelve months was reported, respondents were able to rate on a four-point scale from 1 "fully agree" to 4 "fully disagree" the following statements: "Our operations were disrupted by the investigation", "I am overall satisfied with the work of the police" and "I would recommend other companies to report cyber-attacks".

Figure 69 **Evaluation of the work of law enforcement agencies**

in percent; weighted data; only companies that reported the most severe incident



Only one tenth of the reporting companies (9.6 %) rather/fully agreed with the statement that the investigations had disrupted operations (Figure 69). More than two thirds fully disagreed (71.4 %) and another fifth rather disagreed (19.0 %). Almost half (47.7 %) were fully or rather satisfied with the work of the police. Nevertheless, 93.7 % of those reporting would recommend other companies to report cyber-attacks to the police. Only a small proportion of 4.9 % would not do so at all.

With one exception, there are no statistically significant differences in these questions, neither between the employee size classes nor between the positions of the company representatives interviewed. This is partly due to the small number of cases, which also makes it impossible to differentiate the answers according to the type of cyber-attack. The exception concerns the agreement to the recommendation to report cyber-attacks to the police: While almost all employees in the IT & information security sector (98.0 %; N=101) would (rather) recommend other companies to report cyber-attacks, the figure within management is slightly lower at 87.3 % (N=79).[311]

When asked whether the perpetrators of this most severe cyber-attack could be identified, a small percentage of 7.7 % (N=201) answered "yes". In most cases (92.3 %) the investigation was unsuccessful.

9.8 Interim summary

The details of the most severe cyber-attack of the last twelve months can be summarised as follows: Attacks using ransomware, other malware and phishing attacks were most frequently reported as the most severe cyber-attacks. In one quarter of companies, the most severe cyber-attack affected different digital data insofar as it was deleted, manipulated, stolen/copied or encrypted. Direct costs as a result of this attack were incurred by 70.0 % of the companies, particularly in connection with defence & investigation, replacement & recovery, and external advice & support. In contrast, reports of fines & compensations and drain off financial means were relatively rare.

The range of reported total direct costs resulting from the most severe cyber-attacks is very wide, from EUR 10 to EUR 2 million, with an average of around EUR 16,900. However, for more than three quarters of the companies (78.0 %) the total costs calculated were below EUR 5,000 and only very rarely EUR 50,000 or more (3.4 %). For a total cost value of EUR 1,000, the distribution can be divided into two equally large halves (median). Cost items with a comparatively high median of EUR 2,000 include drain of financial means and business interruption. The attack types that have caused the highest median costs include ransomware attacks (1,300 EUR) and manual hacking (2,800 EUR).[312]

Only 11.9 % of companies reported the most severe cyber-attack to the police, with larger companies reporting more often than smaller ones (500+ employees: 21.5 % vs. 10-49 employees: 10.6 %). The most commonly reported attack types include CEO fraud (24.6 %), spyware (19.7 %) and manual hacking (19.4 %). In contrast, attacks with other malware and defacing were reported relatively rarely (4.4 % and 6.4 % respectively).

The most common reasons for not reporting are low chances of success in the investigation (72.0 %) and uncertainty about who exactly to report to (20.7 %). In addition, 30.1 % of respondents gave other reasons, which probably include the often only minor damages and associated direct costs. However, fears of damage to the company's image, access to confidential data or work disruptions hardly seem to play a role.

Of the companies that have filed a complaint, only just under half (47.8 %) are (rather) satisfied with the police work overall. This is probably due to the fact that only 7.7 % of the reports to the police led to the identification of offenders. Nevertheless, the majority of 93.8 % would recommend other companies to report cyber-attacks to the police. Only ten out of 100 companies experienced disruptions in their operations during the investigation (9.6 %).

[311] The company representatives in other positions all agreed with the statement (21 out of 21).

[312] Damage and costs due to loss of reputation or indirect or highly delayed effects, such as loss of market share due to stolen construction plans and counterfeit products, were not examined in this study.

In addition to these detailed questions on the most severe cyber-attack of the last twelve months, the respondents were asked to classify the existence of the IT security measures described in Section 5.3 and to state whether an IT security measure in use was already in place before or only after the most severe attack. On this basis, the following chapter will examine whether these previously existing measures had a protective effect.

10 POSSIBLE PROTECTION FACTORS

While Chapter 8 analysed company characteristics that are associated with a more frequent occurrence of cyber-attacks in the last twelve months and can therefore be considered potential risk factors,[313] this chapter aims to identify for IT security measures that are associated with a lower occurrence of cyber-attacks in the last twelve months and can therefore be considered potential protection factors.

When comparing the amount of affected companies based on existing IT security measures, it must be taken into account that these may have been implemented only after a damaging event. For this reason, the survey also asked whether the specified IT security measures were already in place before or just after the cyber-attack.

As this chronological classification of IT security measures could not be recorded for all cyber-attacks experienced in the last twelve months, but only for the incident reported as the most severe cyber-attack, the following evaluation does not refer to the annual prevalence, unlike the potential risk factors. Instead, only the amount of affected companies with regard to existing IT security measures that have answered the detailed questions on the most severe cyber-attack can be compared (37.8 %; N=4,723).[314]

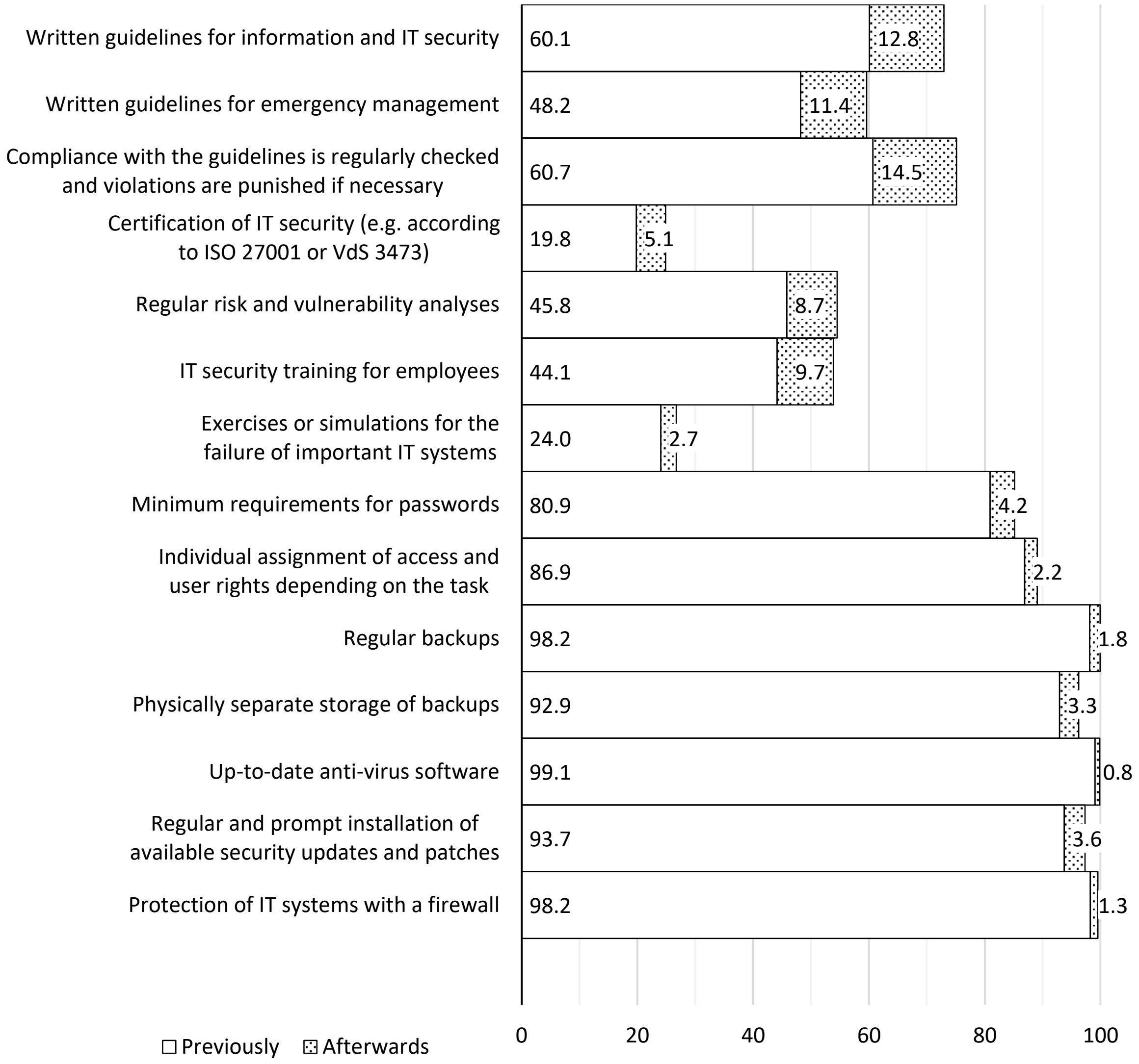
Companies that introduced certain IT security measures only after the most severe attack were counted among the affected companies without this measure, which was more often the case with organisational IT security measures than with technical ones: For example, 12.8 % of the affected companies introduced written guidelines on information or IT security only after the most severe cyber-attack was reported (Figure 70).

Similar to the search for potential risk factors, the existence of IT security measures is related to the proportion of companies affected, and the employee size class is controlled. In this way it can be checked whether a correlation exists in all or only in individual size classes. If the share of affected companies with a certain IT security measure is significantly smaller than the share of affected companies without it, this indicates its preventive effect.

[313] In addition to the size of the staff and the sector, these include the number of locations in Germany, the existence of at least one foreign location, export activity and the existence of special products/manufacturing processes/services or special reputation/customer groups.

[314] Companies that have experienced at least one cyber-attack in the last twelve months but failed to answer detailed questions about the most severe attack were excluded from this comparison. As a result, the underlying case number, and the proportion of those affected were reduced compared to the annual prevalence rate for the cyber-attacks surveyed overall.

Figure 70 **Existing IT security measures before or only after the most severe cyber-attack**
in percent; weighted data; only affected companies

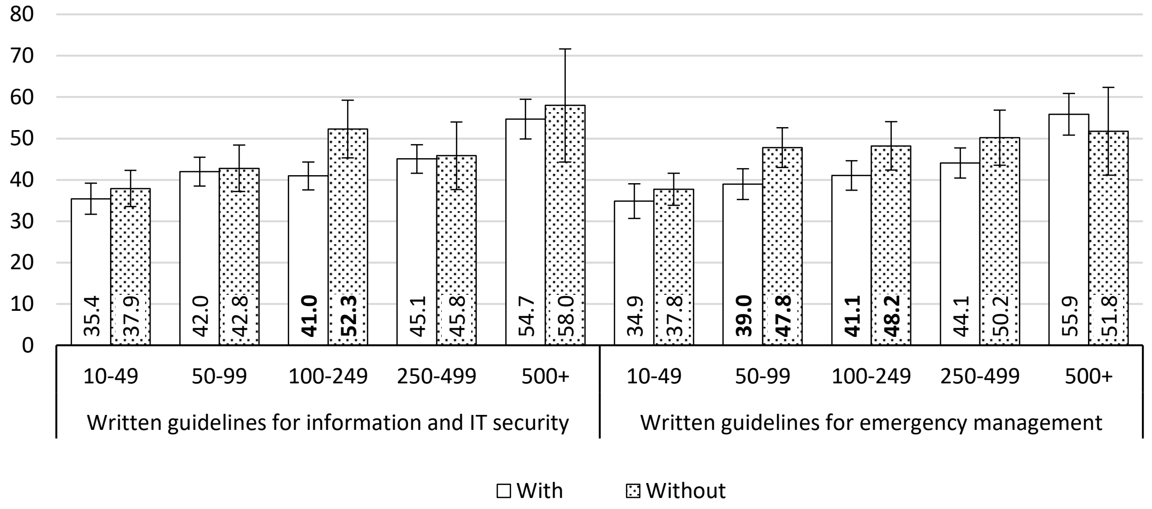


10.1 Organizational measures

Even if written guidelines on information/IT security or emergency management cannot have a preventive effect by their mere existence, they represent a discussion of the topic within the companies and at least partly for a lived practice that could make a difference.

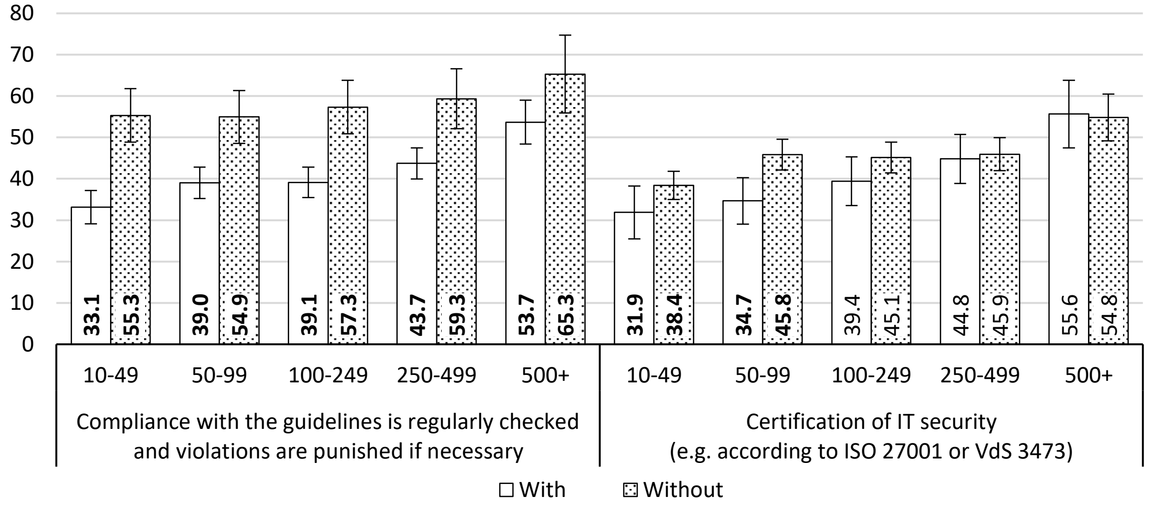
As expected, the shares of affected companies with such policies tend to be lower than the shares of companies that did not have them or only after the most severe cyber-attack (Figure 71). The correlation is statistically significant with regard to information or IT security policies for companies with 100 to 249 employees and with regard to emergency management policies for companies with 50 to 99 and 100 to 249 employees: while about half of companies without such policies were affected by at least one incident, the proportion of companies with policies is around two-fifths.

Figure 71 **Proportion of those affected with and without guidelines on IT security or emergency management**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



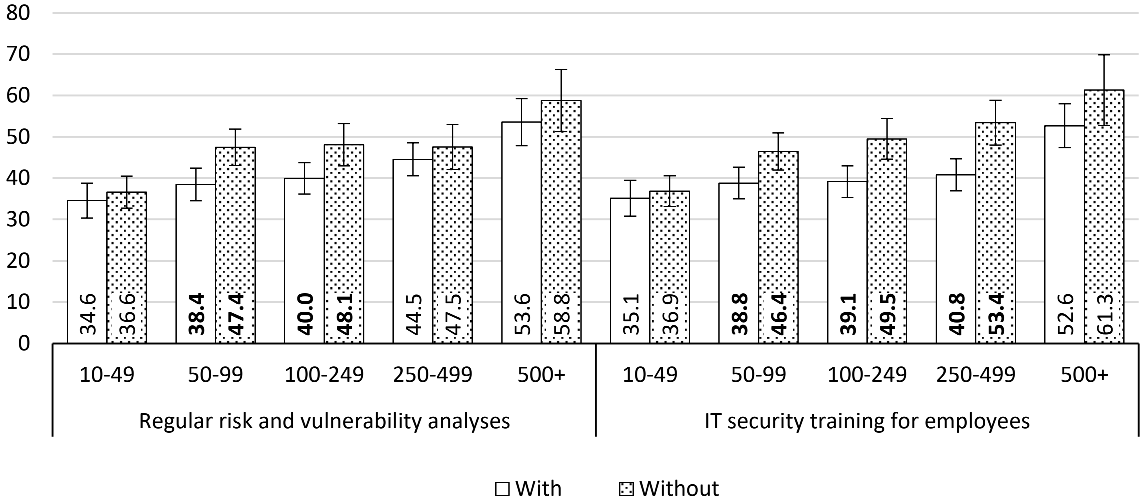
The fact that it is important to implement such guidelines and "live" them in the company is shown by the significantly lower proportion of affected companies in all employee size classes. These companies regularly review these guidelines and sanction violations if necessary (Figure 72). The difference to companies that did not do so is most obvious in the group of small companies (10-49 employees: 33.1 % vs. 55.3 %). The certification of IT security is also negatively related to the extent to which it is affected and proves to be statistically significant among smaller companies (10-49 employees: 31.9 % vs. 38.4 % and 50-99 employees: 34.7 % vs. 45.8 % affected).

Figure 72 **Proportion of those affected with and without guideline checks or certification**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



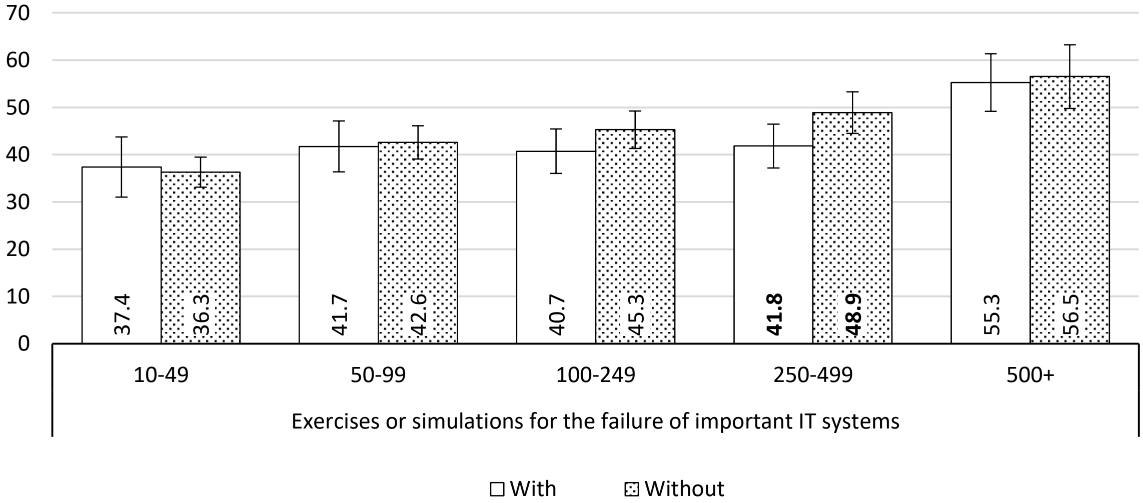
Regular risk and vulnerability analyses are also associated with lower percentages of companies being affected and can therefore make a preventive contribution through the measures associated with them (Figure 73). This tends to be the case in all employee size classes and is statistically significant in the groups with 50 to 99 and 100 to 249 employees (38.4 % vs. 47.4 % and 40.0 % vs. 48.1 % affected persons). The influence of IT security training for employees appears to be even somewhat greater, and is statistically significant in medium-sized companies (50-99, 100-249 and 250-499 employees): In the class 250 to 499 employees, for example, a share of 40.8 % with and 53.4 % without training measures was affected by at least one cyber-attack in the previous year.

Figure 73 **Percentage of those affected with and without risk/vulnerability analyses or training**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



Exercises or simulations about the failure of important IT systems have a negative correlation with the extent to which companies with 250 to 499 employees are affected, insofar as the proportion of affected companies that carry out exercises and simulations is about 8 percentage points below the proportion of companies that do not provide for them (41.8 % vs. 48.9 %; Figure 74).

Figure 74 **Percentage of those affected with and without exercises/simulations for the failure of important IT systems**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



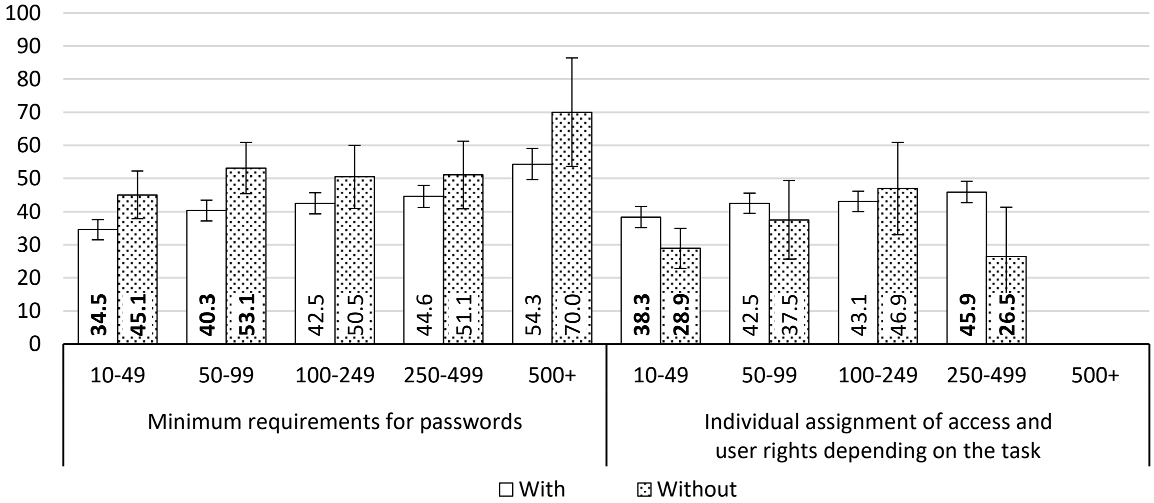
10.2 Technical measures

The influence of technical IT security measures can hardly be shown in comparison to the organisational ones, because the variance of the answers of the companies was often too small. As already described, almost all companies stated that they regularly and promptly install available security updates and patches, carry out backups and have firewall or anti-virus protection.

The group of companies that have not implemented these measures is often too small for a valid comparison, especially when other variables such as employee size class are controlled.

With regard to the existence of minimum password requirements,[315] the comparison can still be made across all employee size classes and shows that companies with minimum password requirements were less frequently affected by cyber-attacks in the previous year (Figure 75). The difference seems significant in the group of companies with 10 to 49 employees (34.5 % vs. 45.1 %) and with 50-99 employees (40.3 % vs. 53.1 %). A clearly visible difference can also be seen in the large companies (500 and more employees: 54.3 % vs. 70.0 %), but since the group without minimum requirements is very small (N=30) in this size class, it cannot be ruled out that this difference was caused by random sampling, given a statistical error probability of 5 %.

Figure 75 Proportion of those affected with and without minimum requirements for PW or individual access/user rights
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)

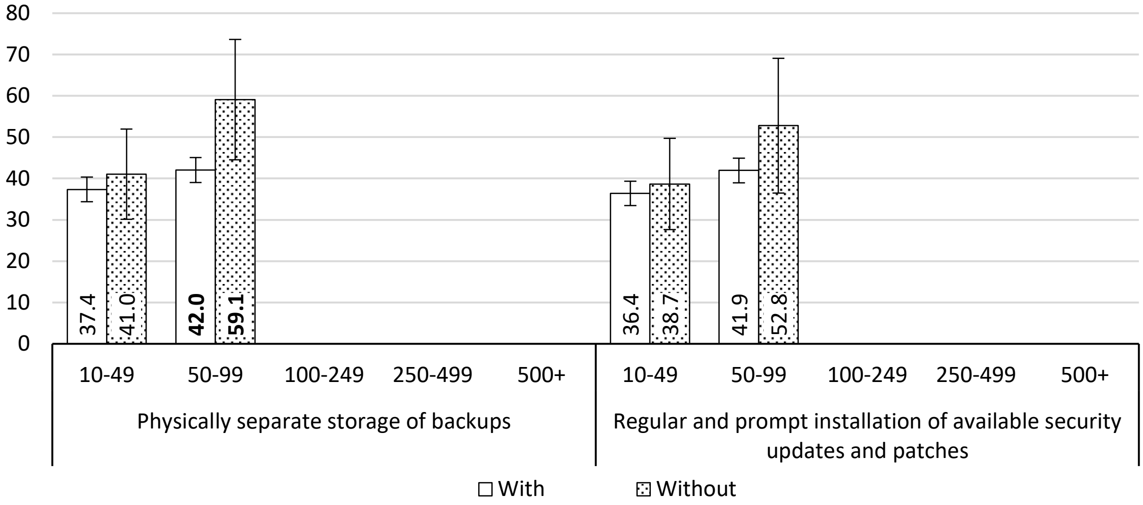


A counter-intuitive result can be seen with regard to the individual assignment of access and user rights depending on the task of the employees (Figure 75). This measure, which is intended to restrict the unhindered access of all employees to all areas of the company's IT system and thus make it more difficult for internal and external attackers, for example, to move within the network and access relevant data, is significantly positively related to affect companies with 10 to 49 and 250 to 499 employees. In the context of small numbers of cases in companies without individual rights allocation, this difference could be explained by a lower degree of digitization, which reduces the risk of cyber-attacks in these companies regardless of IT security measures. On the other hand, differences in the types of cyber-attacks can be identified, especially in the companies concerned with 250 to 499 employees: Those companies in this size category who had granted individual access and user rights before the most severe cyber-attack were more frequently affected by attacks in the area of social engineering (CEO fraud and phishing), against which limited access and user rights can hardly have a preventive effect. In this respect, there is much to suggest a spurious relationship between individual rights allocation and a higher impact rate, which is caused by other variables that are not considered.

[315] See footnote 235.

As the group of companies without physically separated storage of back-ups is also very small, only the impact rates of the lower two employment size classes can be meaningfully compared, with a significant difference in the size class 50 to 99 employees (Figure 76): companies with physically separated back-ups are thus less affected by cyber-attacks than companies not implementing this measure (42.0 % vs. 59.1 %). Since backups and their storage are mainly damage control measures[316] and not attack prevention measures, other related preventive measures are likely to be responsible for the described correlation.

Figure 76 **Proportion of those affected with and without physically separate backups or regular updates/patches**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



With regard to the lower two employee size classes, the impact rates of companies with and without the regular and timely installation of available security updates and patches can be compared, whereby at best only tendential differences in the expected direction are visible (Figure 76).

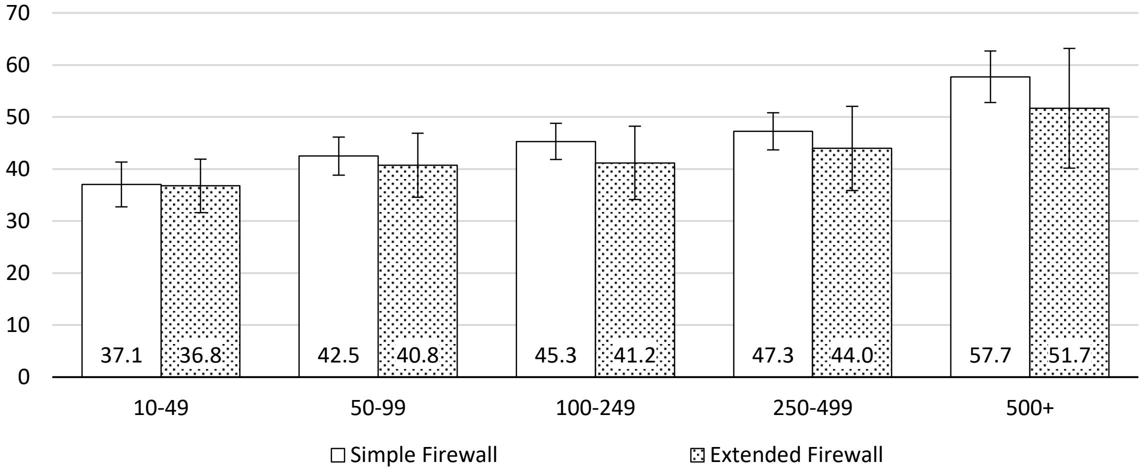
As already indicated, the remaining technical IT security measures (up-to-date anti-virus software, regular backups and protection of the IT systems with a firewall) cannot be meaningfully correlated with the rate of affection due to the lack of variance.

With regard to firewall protection, it was differentiated whether it is a simple firewall, i.e. packet filtering by source and destination address by software firewall or router at network level, or an advanced firewall, i.e. additional monitoring and filtering by packet content at application level. Even though the proportion of respondents who did not know what to do with this distinction is relatively large,[317] these two groups of companies can be compared with each other in terms of the impact rate. It can be expected that companies with an enhanced firewall will be less likely to be affected by cyber-attacks that require active response due to the higher level of technical protection.

[316] In addition to regular backups and their physically separate storage, in the event of damage it is crucial that the recovery of data works promptly.

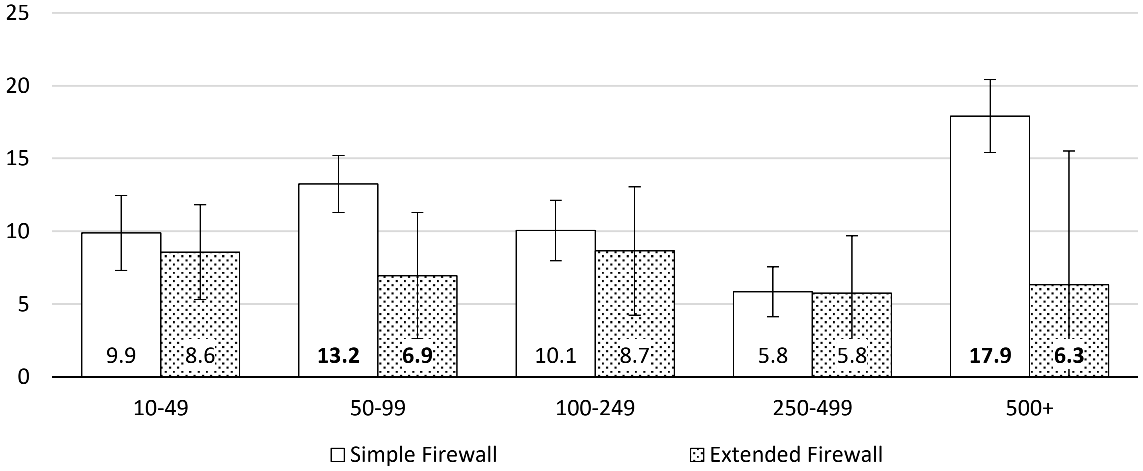
[317] See figure 21 in section 5.3.2.

Figure 77 **Proportion of affected persons by type of firewall**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



In relation to all cyber-attacks as a whole, there are small differences in the expected direction, but these are not statistically significant (Figure 77). Since such a technical measure can hardly have any effect on attacks in the area of social engineering, the group comparison is again carried out in relation to malware attacks.

Figure 78 **Percentage of persons affected by other malware by firewall type**
in percent; weighted data; 95 % CI; bold: differences significant at p<.05 (Chi² test)



In this comparison, significant differences can be seen in some cases (Figure 78): Companies with 50 to 99 employees and 500 or more employees who had already used an advanced firewall before the most severe cyber-attack were less frequently affected by attacks with other malware than corresponding companies with a simple firewall (6.9 % vs. 13.2 % and 6.3 % vs. 17.9 %). This indicates that the quality and maturity of technical protection measures played a significant role. The reason why this correlation is not so clear in the other employee size classes could be related to the fact that other factors such as proper implementation and application as well as regular maintenance have an impact that cannot be controlled here.

10.3 Interim summary

In summary, after these comparisons of the shares of affected companies with and without the respective IT security measures, it can be stated that a preventive effect seems to emanate primarily from individual organizational measures and that the human factor plays an important role in the prevention of cyber-attacks. Above all, the review of guidelines and their compliance as well as the training of employees in IT security had the effect of reducing the percentage of those affected.

However, these organisational measures require other organisational and technical IT security measures, which contribute their part to the preventive effect.[318] Even if only a few bivariate connections between technical measures and the proportion of companies affected were found, it should therefore not be concluded that they are ineffective. This is even more true since only their existence was inquired and qualitative differences were largely ignored. In addition, almost all companies answered these questions about the existence of technical measures affirmatively, which can certainly be seen as positive, but also raises questions about qualitative differences in their design and implementation (e.g. the degree of maturity or the appropriate configuration of an existing firewall). In future studies, technical IT security measures should therefore be examined in more detail with regard to their degree of maturity and their professional implementation, maintenance and cyclicality.[319] In addition, the question of the design and usability of technical measures in everyday work[320] as well as the interaction of all IT security measures should also be taken into account.[321]

In order to be able to make more precise statements about the interaction of individual technical and organisational measures and their partial influence on the probability of a cyber-attack against the background of different types of attack and company characteristics, further multivariate analyses are planned which are based on these results.

[318] For example, guidelines for handling passwords can only be checked if there is a corresponding guideline and password protection is technically provided.

[319] For example, with regard to backups, it could be asked whether the system recovery from a backup (backup restoring) is tested. With regard to password protection, the use of a two-factor authentication could be inquired about, and with regard to security updates, whether software is used without manufacturer support, which no longer receives updates and patches, etc.

[320] For example, can the rules of conduct associated with technical measures be observed or meaningfully integrated into the respective working practice without causing unintended side effects such as reactance and problematic evasive behaviour among users? On the topic of "Usable Security" see e.g. Adams & Sasse (1999); Nurse et al. (2011); Sasse et al. (2001).

[321] Connolly & Wall (2019) point out that against the background of complex threats such as ransomware attacks, the interaction of socio-technical measures, committed managers and active support from company management is crucial (p. 14).

11 SUMMARY OF KEY FINDINGS

Decisions on securing IT systems are becoming increasingly important for companies in the context of rapid digitalisation and the associated risks of cyber-attacks of various types. In order to be able to make such decisions in a well-founded and evidence-based manner, independent scientific research results are necessary, which are largely lacking in the area of cyber-attacks against companies in Germany and beyond.

In this context, the Criminological Research Institute of Lower Saxony together with the Research Centre L3S of the Leibniz University Hannover is conducting the research project "Cyber-attacks against Companies", in which differentiated knowledge on the types of attacks, the frequency of cyber-attacks, the spread of prevention measures and IT security standards as well as risk and protection factors is to be developed. A further goal of this project is to process the knowledge gained in a practical manner and to transfer it to companies in order to support small and medium-sized companies with limited human and material resources in improving their IT security. For this purpose, an additional practice-relevant summary will be prepared on the basis of the present research report, which addresses significant differences between SMEs and large companies, especially with regard to possible risk and protection factors in a manner appropriate to the target group.

The project runs for three years from December 2017 to November 2020, is funded as part of the "IT-Sicherheit in der Wirtschaft” (EN: IT-security in the economy) initiative of the German Federal Ministry for Economic Affairs and Energy (BMWi) and receives additional support from PricewaterhouseCoopers Germany and the VHV Foundation. In addition to expert interviews and various field studies with IT employees in small and medium-sized companies, a CATI survey of 5,000 German-based companies with ten or more employees was conducted on the basis of a disproportionately stratified random sample.

The results of the survey are the content of this research report and are summarised again below, structured according to the main research questions in Section 1.2. Subsequently, methodological restrictions are pointed out and an outlook with regard to further research steps is given.

1) **What IT security measures against cyber-attacks have companies established?**

   In the IT security structure, a distinction was made between organisational and technical IT security measures. In general, it can be stated that technical measures seem to be very widespread and that there are, at best, only minor quantitative differences between the employee size classes and WZ08 classes, whereas organisational measures are less common and more likely to be used in larger companies and certain WZ08 classes.

   Organizational measures

   For all of the organizational measures surveyed, there were significant differences in their distribution: For example, in small companies (10-49 employees), written guidelines on information and IT security (62.6 %) and on emergency management (50.6 %), which show the presence and a more intensive discussion about the topic within the companies, were found less often than for large companies (500+ employees: 92.0 % and 84.4 % respectively) Also, e.g. within construction (WZ08-F: 48.9 % and 33.8 %) they are less common than for financial & insurance service providers (WZ08-K: 94.3 % and 89.3 % respectively). Most of the companies that have introduced such guidelines regularly verify their compliance to them and sanction, if appropriate, any violations (76.7 %). Differences between the employee size classes and WZ08 classes are relatively small in this respect, which suggests that such guidelines are often not only available on paper but they are used as guidance for action. As a further example of organisational measures, IT security training for employees is carried out by more than three-quarters of large companies (500+ employees: 76.2 %) but by less than half of small companies (10-49 employees: 46.5 %). The differences between companies in the construction sector and financial & insurance service providers were even more distinct (14.3 % vs. 77.1 %).

Technical measures

In contrast to the organisational measures, the proportion of companies that have minimum requirements for passwords, assign access and user rights individually and according to the corresponding task, carry out regular backups, keep them physically separate, use anti-virus software and firewall and regularly install security updates and patches is over 80 % and in most cases even over 90 % in all employee size classes. The fewmajor differences between the employee size classes were the minimum requirements for passwords and the individual assignment of access and user rights depending on the task: the amount ofsmall companies (10-49 employees: 85.4 % and 82.0 %) with such minimum requirements or with a corresponding allocation of rights are ten and fourteen percentage points below those of large companies (500+ employees: 95.4 % and 96.4 % respectively).

Since the technical IT security measures surveyed appear to be already very widespread in quantitative terms, further research will have to look for the qualitative differences that may be associated with the risk of cyber-attacks in order to be able to advise companies sensibly in this respect and to support them in their implementation. With regard to organisational measures, the results of this survey can also be used to derive the need for support for their dissemination, which affects small and medium-sized companies in particular.

Assessments of IT risks

According to the assessments of the company representatives interviewed, the majority of the company's management and staff are aware of IT risks. Only 8.0 % and 11.3 % respectively stated that their company's management and staff were not aware of IT risks. A high proportion of 84.9 % (rather) agreed with the statement that a lot is done for IT security in their company.

Based on this result, it is not surprising that the risk of one's own company being affected by a targeted cyber-attack in the next twelve months is predominantly assessed as very/ rather low (93.0 %). The representatives surveyed, who agree to this in terms of non-targeted cyber-attacks is somewhat lower at 68.5 %, but still relatively high. Only about one third of the company representatives estimate the opposite. The relation between risk assessment and the existence of potential targets in the company (e.g. special products or a special customer base) is interesting. This relation also exists with regard to untargeted cyber-attacks: In companies in which, in the opinion of the representatives surveyed, there are no potential targets, the risk of both targeted and non-targeted cyber-attacks is assessed as significantly lower than in companies with potential targets. This means that, in particular, the companies without potential targets are exposed to the risk of underestimating the risk of untargeted cyber-attacks.

2) What types of cyber-attacks have companies had to respond to in the last twelve months?

More than two-fifths (41.1 %) of the companies surveyed have experienced at least one cyber-attack in the previous twelve months that required a response, i.e. attacks that were thwarted automatically (e.g. via the firewall's spam filter or anti-virus software) or not detected at all (e.g. spyware attacks) are not included. With an annual prevalence rate of 58.2 %, large companies (500+ employees) are significantly more frequently affected than medium-sized (between 45.6 and 47.3 %) and small companies (10-49 employees: 39.4 %). This tends to reflect the different risk assessments of employee size classes, according to which small companies estimate the risk of a future cyber-attack to be lower than larger ones. However, the proportions of companies affected by at least one cyber-attack in all employment size classes in the previous year are higher than the proportions of companies that assess the risk of such attacks in the next 12 months as rather/very high. This indicates a general underestimation of the corresponding company risk.

Types of attack[322]

Attacks using malware are a focal point in terms of the spread of the different types of cyber-attacks, alongside phishing attacks: one in eight companies (12.5 %) was affected by a ransomware in the last twelve months, one in nine (11.3 %) by a spyware and approximately one in five (21.3 %) by other malware attacks.

Phishing also accounted for more than one fifth (22.0 %) of the companies affected. On the other hand, companies reported less CEO fraud (8.1 %) and (D)DoS attacks (6.4 %) and only a small proportion were affected by manual hacking (2.8 %) or defacing attacks (3.1 %).

Looking at the types of cyber-attacks by the number of incidents experienced that needed to be responded to, phishing attacks are the most common with 52.0 % of all reported incidents, followed by other malware attacks (24.0 %) and spyware attacks (11.9 %). Ransomware attacks accounted for only 3.3 % of all reported incidents, so while this type of attack is relatively widespread (11.3 % of companies were affected), the number of such incidents

[322] The following types of attack were distinguished:
Ransomware: encryption of company data (usually combined with blackmail);
Spyware: spying on user activities or other data within IT systems;
Other malware: infection of IT systems with viruses, worms or Trojans etc.
Manual hacking: Manipulation of hardware and software without the use of special malware;
Denial of Service Attack ((D)DoS): Overloading of web or e-mail servers with the aim of causing them to fail;
Defacing: Unauthorised modification of company web content;
CEO fraud: Feigning a company executive to manipulate employees;
Phishing: Faking e-mails or websites to obtain sensitive company data etc.

reported by affected companies is relatively small. The number of incidents of manual hacking, CEO fraud, (D)DoS and defacing are proportionately in the lower single-digit range (2.9 %, 2.4 %, 2.2 % and 1.2 % respectively).

Possible risk factors

In general, it can be said that larger companies are more affected by cyber-attacks than smaller ones. This is especially true for ransomware attacks, CEO fraud and phishing attacks. In contrast, the employee size class seems to play at best a small role for other types of attacks.

When comparing the rates of affectedness by sector, further significant differences can be observed: For example, wholesale and retail trade; repair of motor vehicles and motorcycles or professional, scientific and technical activities are more frequently affected by cyber-attacks than water supply; sewerage, waste management and remediation activities; or agriculture, forestry and fishing.

In addition, the number of company sites, the export of services and goods and the existence of potential targets such as special products, manufacturing processes or services and a special reputation or customer base are also associated with a higher level of affectedness. Public access to detailed information on employees appears to play a risk-increasing role, particularly in the case of the CEO fraud attack.

On the other hand, companies providing services of general interest were affected less frequently (31.1 %) than companies in other sectors (42.3 %). In particular, smaller companies in this group appear to be better protected than in the other sectors of the economy.

Extent and consequences of cyber-attacks

Among the IT systems most frequently affected by the most severe cyber-attacks are e-mail and communications, order and customer management, and accounting and controlling. These were evaluated as (rather) important to the business by over 90 % of companies. The length of time these systems could not be used at all or only to a very limited extent as a result of the cyber-attack ranged from one hour to 90 days, with a median of 24 hours in each case. Production control was the least affected, but with a median of 48 hours it was longer affected than other systems.

For one quarter of companies (25.2 %), the most severe cyber-attack affected different digital data, i.e. it was deleted, manipulated, stolen/copied or encrypted. 70.0 % had direct costs to the business as a result of the attack. These included in particular costs in connection with defence & investigation, replacement & recovery costs and costs for external advice & support. Very few reports of fees & compensation payments and drain off financial means were made.

The range of reported total direct costs resulting from the most severe cyber-attacks is between EUR 10 and EUR 2 million, which might put, in particular smaller companies, in an existence-threatening situation. However, where costs were incurred, it can also be seen that the vast majority (78.0 %) were below EUR 5,000 and very rarely EUR 50,000 or more (3.4 %). The average of the reported total costs is around EUR 16,900, the median is EUR

1,000. Cost items with a comparatively high median of EUR 2,000 include drain off financial means and business interruption. The attack types that have caused the highest median costs include ransomware attacks (1,300 EUR) and manual hacking (2,800 EUR).

3) What is the reporting behaviour of affected companies?

A share of 11.9 % of companies that reported a most severe cyber-attack reported it to the police. Thus, it can generally be assumed that there is a large number of officially non-registered cyber-attacks against companies. In addition, it was found that larger companies reported more frequently than smaller ones (500+ employees: 21.5 % vs. 10-49 employees: 10.6 %) and that there were significant differences between the types of attack. CEO fraud, spyware and manual hacking were reported comparatively frequently (24.6 %, 19.7 % and 19.4 % respectively), while other malware and defacing attacks came to the attention of the police only very rarely (4.4 % and 6.4 % respectively).

The most frequently mentioned reasons for not reporting to the police were the low chances of success of investigations (72.0 %) and other reasons (30.1 %), probably including the low costs incurred facing a certain reporting effort. In third place, non-reporting companies said that they did not know who to turn to for this purpose (20.7 %). Conversely, fears of damage to their image, access to confidential data or work disabilities seem to play a rather minor role in the decision to (non-)report to the police.

Assessment of law enforcement agencies

More than half of the companies that reported the most severe attack expressed (rather) dissatisfaction with the work of the police (52.2 %) and one tenth (rather) agreed that the investigations disrupted operations (9.6 %). And even if only for7.7 % of the most severe cyber-attacks reported the corresponding perpetrators could be identified, 93.8 % of companies would recommend that others report cyber-attacks. Their motivation is therefore probably less likely be the prospect of a successful investigation by the police rather than in the police registration of crimes or in information and advice provided by the police to protect against future cyber-attacks.

4) Is there a correlation between the frequency of cyber-attacks and the existence of certain IT security measures?

In order to identify potential protection factors against cyber-attacks, group comparisons were made between companies with and without the various IT security measures in terms of how they were affected. Summarizing these comparisons, it can be stated that mainly different organizational measures seem to have a preventive effect and the human factor plays an important role in the prevention of cyber-attacks. In particular, the review of guidelines and their compliance as well as the training of employees in IT security had the effect of reducing the percentage of companies affected.

Due to the fact that the technical IT security measures, as surveyed, were available in almost all companies, there was often no sufficiently large comparison group. An exception, where the expected correlation was found, is the minimum requirements for passwords. Companies that have not implemented this measure so far were more frequently affected by cyber-attacks than the others. This was shown statistically significant for the smaller companies with up to 99 employees.

Even if hardly any bivariate connections between technical measures and the proportion of companies affected could be found, it is not possible to conclude that they are ineffective. This is all the more true because only their existence was queried, qualitative differences were largely ignored and organisational measures require many of the technical IT security measures to be implemented. In future studies, therefore, technical IT security measures should be examined in much greater detail with regard to their maturity, quality and usability as well as in interaction with organisational measures and users.

Every research is associated with various restrictions that limit the validity of the results and which must be taken into account when interpreting the results. In connection with the results presented above, this concerns the following points in particular: The sampling was carried out from a selected population and not directly from the basic population. Even though the sample largely corresponds to the population with regard to the distribution of all controlled characteristics and there are no indications of systematic bias and it can therefore be considered representative for companies with ten employees or more in Germany, there is still uncertainty regarding the coverage problem, as companies that were not included in the sample database had no chance of being included in the sample. In addition, such company surveys are limited to the fact that only one person can be interviewed as a company representative. Apart from the problem of selecting suitable representatives, their answers always reflect the current state of knowledge and are partly only subjective assessments. In addition, questions about cyber-attacks have been asked retrospectively, which can lead to distortions, e.g. if the events in question are not remembered at all or in reality are longer ago than in the memory of the respondents. A further limitation already mentioned is that for pragmatic research reasons, on the one hand, only the existence of certain characteristics and measures could be inquired about and therefore no statements on qualitative differences can be made. On the other hand, detailed questions about, among other things, the extent and consequences of cyber-attacks could only be asked about one attack. As soon as several attacks took place in the last twelve months, the answers refer to the cyber-attack determined as the "most severe attack".

Despite these limitations, the results of this study allow a very differentiated view of the phenomenon of cyber-attacks against companies in Germany with more than nine employees. For example, it could be shown that a large proportion of these companies were affected by cyber-attacks in the last twelve months, which is not reflected in the official crime statistics due to a very low reporting rate. It was also shown that the range of damage caused by cyber-attacks is very wide, although the direct costs incurred remained manageable in the majority of cases. In particular, organisational measures affecting the human factor appear to make a difference in the prevention of cyber-attacks and should therefore be promoted with a view to their spread, especially among small and medium-sized companies. It also became clear, however, that there will be no easy answers to the cyber-attack risk and corresponding protective measures. This is partly due to the complexity of the cyber-attacks and attack vectors as well as the sometimes very complex IT structure of the companies, which can only be roughly determined in a quantitative survey.

Even though the evaluations of the company survey have not yet been completed with this report and further multivariate analyses and results are still to come, e.g. on risk and protection factors in connection with cyber-attacks and the extent of damage, not all open question about this phenomenon can be answered within this research project. In addition to differentiations of IT security measures according to maturity level, e.g. the interaction of employees and available IT security measures, the discovery of different types of attack and their routes of attack or the developments in the area of attack types remain underexposed.

It is therefore desirable that further research be conducted in the future on the phenomenon of cybercrime, and especially cybercrime against companies, which is likely to grow with digitization. In order to be able to investigate the development within one year in this area, a second survey is planned within the framework of this project with the companies and their representatives who have signalled their willingness to participate in the first survey and whom we would like to thank at this point!

ANNEX 1: ADDITIONAL TABLES

Table 43 **WZ08 classes of companies of general interest companies**

WZ08 classes		
Level 1	Level 4	Designation
WZ08-D Electricity, Gas, Steam and Air Conditioning Supply	35.11.1	Production of electricity without distribution
	35.11.2	Production of electricity incl. purchases from other suppliers for distribution
	35.11.3	Production of electricity excl. purchases from other suppliers for distribution
	35.12.0	Transmission of electricity
	35.13.0	Distribution of electricity
	35.14.0	Trade of electricity
	35.21.1	Manufacture of gas without distribution
	35.21.2	Manufacture of gas incl. purchases from other suppliers for distribution
	35.21.3	Manufacture of gas excl. purchases from other suppliers for distribution
	35.22.0	Distribution of gaseous fuels through mains
	35.23.0	Trade of gas through mains
	35.30.0	Steam and air conditioning supply
WZ08-E Water Supply; Sewerage, Waste Management and Remediation Activities	36.00.1	Collection and purification of water incl. purchases from other suppliers for distribution
	36.00.2	Collection and purification of water excl. purchases from other suppliers for distribution
	36.00.3	Distribution of water without collection and purification
	37.00.1	Operation of sewer systems
	37.00.2	Operation of sewage treatment facilities
	38.11.0	Collection of non-hazardous waste
	38.12.0	Collection of hazardous waste
	38.21.0	Treatment and disposal of non-hazardous waste
	38.22.0	Treatment and disposal of hazardous waste
	38.31.0	Dismantling of wrecks
	38.32.0	Recovery of sorted materials
	39.00.0	Remediation activities and other waste management services
WZ08-H Transportation and Storage	49.10.0	Passenger rail transport, interurban
	49.20.0	Freight rail transport
	49.31.0	Urban and suburban passenger land transport
	49.39.1	Scheduled long-distance passenger transport by motor bus
	49.39.2	Non-scheduled passenger transport by motor bus
	49.39.9	Land passenger transport N.E.C.
	49.41.0	Freight transport by road
	49.50.0	Transport via pipeline
	50.10.0	Sea and coastal passenger water transport
	50.20.0	Sea and coastal freight water transport
	50.30.0	Inland passenger water transport
	50.40.0	Inland freight water transport
	51.10.0	Passenger air transport
	51.21.0	Freight air transport
	52.10.0	Warehousing and storage

	52.21.2	Operation of road infrastructure
	52.21.3	Operation of railroad infrastructure
	52.21.4	Operation of terminal facilities for passenger transport, including bus stations
	52.21.5	Operation of stations for the handling of goods carried by rail or road (except cargo handling
	52.21.9	Service activities incidental to land transportation N.E.C.
	52.22.1	Operation of waterway infrastructure
	52.22.2	Operation of ports, harbours and piers
	52.22.3	Navigation, pilotage and berthing activitie
	52.22.9	Service activities incidental to water transportation n.e.c
	52.23.1	Operation of airports and airfields
	52.23.9	Service activities incidental to air transportation N.E.C.
	52.24.0	Cargo handling
	53.10.0	Postal activities under universal service obligation
	53.20.0	Other postal and courier activities
WZ08-J Information and Communication	61.10.0	Wired telecommunications activities
	61.20.0	Wireless telecommunications activities
	61.30.0	Satellite telecommunications activities
	61.90.1	Internet service providers
WZ08-K Financial and Insurance Activities	64.11.0	Central banking
	64.19.2	Activities of savings banks
	64.19.3	Activities of cooperatives
WZ08-L Real Estate Activities	68.10.1	Buying and selling of own residential real estate
	68.20.1	Renting and operating of own or leased residential real estate
	68.31.1	Activities of real estate agencies relating to residential real estate
	68.32.1	Management of residential real estate on a fee or contract basis
WZ08-O Public Administration and Defence; Compulsory Social Security	84.21.0	Foreign affairs
	84.22.0	Defence activities
	84.23.0	Justice and judicial activities
	84.24.0	Public order and safety activities
	84.25.0	Fire service activities
	84.30.0	Compulsory social security activities
WZ08-P Education	85.42.1	Universities
	85.42.2	Universities of applied sciences
	85.42.3	Colleges of public administration
	85.42.4	Vocational academies, specialised academies, schools for nurses, midwives etc.
WZ08-Q Human Health and Social Work Activities	86.10.1	Hospital activities (excluding university hospitals, preventive care and rehabilitation centres
	86.10.2	Activities of university hospitals
	86.10.3	Activities of preventive care and rehabilitation centres

Table 44 **Sample by WZ08 classes**

WZ08 classes (short name)		unweighted		weighted
Level 1	Level 2	Quantity	Percent	Percent
WZ08-A Agriculture, forestry and fishing	Crop and animal production, hunting and related service activities (WZ08-01)	38	0.8	1.4
	Forestry and logging (WZ08-02)	1	0.0	0.0
WZ08-B Mining and Quarrying	Other mining and quarrying (WZ08-08)	15	0.3	0.3
	Mining support service activities (WZ08-09)	2	0.0	0.0
WZ08-C Manufacturing	Manufacture of food products (WZ08-10)	95	1.9	1.5
	Manufacture of beverages (WZ08-11)	17	0.3	0.2
	Manufacture of tobacco products (WZ08-12)	3	0.1	0.0
	Weaving of textiles (WZ08-13)	36	0.7	0.5
	Manufacture of wearing apparel (WZ08-14)	11	0.2	0.2
	Manufacture of leather and related product (WZ08-15)	5	0.1	0.1
	Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials (WZ08-16)	48	1.0	1.2
	Manufacture of paper and paper product (WZ08-17)	31	0.6	0.2
	Printing and reproduction of recorded media (WZ08-18)	37	0.7	1.0
	Manufacture of coke and refined petroleum products (WZ08-19)	1	0.0	0.0
	Manufacture of chemicals and chemical products (WZ08-20)	50	1.0	0.8
	Manufacture of basic pharmaceutical products and pharmaceutical preparations (WZ08-21)	13	0.3	0.1
	Manufacture of rubber and plastic products (WZ08-22)	93	1.9	1.0
	Manufacture of other non-metallic mineral products (WZ08-23)	60	1.2	1.2
	Manufacture of basic metal (WZ08-24)	51	1.0	0.7
	Manufacture of fabricated metal products, except machinery and equipment (WZ08-25)	231	4.6	3.9
	Manufacture of computer, electronic and optical products (WZ08-26)	96	1.9	1.1
	Manufacture of electrical equipment (WZ08-27)	75	1.5	1.6
	Manufacture of machinery and equipment N.E.C. (WZ08-28)	200	4.0	2.4
	Manufacture of motor vehicles, trailers and semi-trailers (WZ08-29)	34	0.7	0.4
	Manufacture of other transport equipment (WZ08-30)	9	0.2	0.0
	Manufacture of furniture (WZ08-31)	38	0.8	1.0
	Other manufacturing (WZ08-32)	71	1.4	1.1
	Repair and installation of machinery and equipment (WZ08-33)	23	0.5	0.6
WZ08-D Electricity, Gas, Steam and Air Conditioning Supply	Electricity, gas, steam and air conditioning supply (WZ08-35)	68	1.4	0.5
WZ08-E Water Supply; Sewerage, Waste Management and Remediation Activities	Water collection, treatment and supply (WZ08-36)	16	0.3	0.1
	Sewerage (WZ08-37)	7	0.1	0.1
	Waste collection, treatment and disposal activities; materials recovery (WZ08-38)	62	1.2	0.7
	Remediation activities and other waste management services (WZ08-39)	4	0.1	0.0
WZ08-F Construction	Construction of buildings (WZ08-41)	70	1.4	2.6
	Civil engineering (WZ08-42)	53	1.1	1.3
	Specialised construction activities (WZ08-43)	187	3.7	9.0
WZ08-G Wholesale and Retail Trade; Repair of Motor	Wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45)	124	2.5	4.1
	Wholesale trade, except of motor vehicles and motorcycles (WZ08-46)	331	6.6	8.3

Vehicles and Motorcycles	Retail trade, except of motor vehicles and motorcycles (WZ08-47)	152	3.0	5.5
WZ08-H Transportation and Storage	Land transport and transport via pipeline (WZ08-49)	185	3.7	2.9
	Water transport (WZ08-50)	19	0.4	0.4
	Air transport (WZ08-51)	5	0.1	0.1
	Warehousing and support activities for transportation (WZ08-52)	104	2.1	1.2
	Postal and courier activities (WZ08-53)	16	0.3	0.2
WZ08-I Accommodation and Food Service Activities	Accommodation (WZ08-55)	91	1.8	2.7
	Food and beverage service activities (WZ08-56)	39	0.8	1.4
WZ08-J Information and Communication	Publishing activities (WZ08-58)	36	0.7	0.6
	Motion picture, video and television programme production, sound recording and music publishing activities (WZ08-59)	5	0.1	0.1
	Programming and broadcasting activities (WZ08-60)	5	0.1	0.0
	Telecommunications (WZ08-61)	6	0.1	0.3
	Computer programming, consultancy and related activities (WZ08-62)	90	1.8	1.8
	Information service activities (WZ08-63)	10	0.2	0.2
WZ08-K Financial and Insurance Activities	Financial service activities, except insurance and pension funding (WZ08-64)	170	3.4	1.7
	Insurance, reinsurance and pension funding, except compulsory social security (WZ08-65)	14	0.3	0.0
	Activities auxiliary to financial services and insurance activities (WZ08-66)	25	0.5	0.4
WZ08-L Real Estate Activities	Real Estate Activities (WZ08-68)	105	2.1	1.6
WZ08-M Professional, Scientific and Technical Activities	Legal and accounting activities (WZ08-69)	75	1.5	2.1
	Activities of head offices; management consultancy activities (WZ08-70)	146	2.9	1.7
	Architectural and engineering activities; technical testing and analysis (WZ08-71)	142	2.8	3.9
	Scientific research and development (WZ08-72)	30	0.6	0.2
	Advertising and market research (WZ08-73)	30	0.6	0.7
	Other professional, scientific and technical activities (WZ08-74)	9	0.2	0.4
	Veterinary activities (WZ08-75)	2	0.0	0.2
WZ08-N Administrative and Support Service Activities	Rental and leasing activities (WZ08-77)	11	0.2	0.3
	Employment activities (WZ08-78)	59	1.2	0.5
	Travel agency, tour operator and other reservation service and related activities (WZ08-79)	25	0.5	1.0
	Security and investigation activities (WZ08-80)	16	0.3	0.2
	Services to buildings and landscape activities (WZ08-81)	70	1.4	1.3
	Office administrative, office support and other business support activities (WZ08-82)	54	1.1	0.9
WZ08-O Public Administration and Defence; Compulsory Social Security	Public administration and defence; compulsory social security (WZ08-84)	19	0.4	0.4
WZ08-P Education	Education (WZ08-85)	274	5.5	6.4
WZ08-Q Human Health and Social Work Activities	Human health activities (WZ08-86)	169	3.4	1.9
	Residential care activities (WZ08-87)	116	2.3	1.5
	Social work activities without accommodation (WZ08-88)	151	3.0	2.4
WZ08-R	Creative, arts and entertainment activities (WZ08-90)	17	0.3	0.1

Arts, Entertainment and Recreation	Libraries, archives, museums and other cultural activities (WZ08-91)	9	0.2	0.2
	Gambling and betting activities (WZ08-92)	7	0.1	0.0
	Sports activities and amusement and recreation activities (WZ08-93)	31	0.6	0.8
WZ08-S Other Service Activities	Activities of membership organisations (WZ08-94)	104	2.1	1.0
	Repair of computers and personal and household goods (WZ08-95)	5	0.1	0.1
	Other personal service activities (WZ08-96)	46	0.9	1.4
	Total	5,000	100.0	100.0

Table 45 **Organizational IT security measures by first-level WZ08 classes**

in percent; weighted data

	IT security measure						
WZ08 classes (level 1; short name; only if N≥30)	1	2	3*	4	5	6	7
Agriculture, forestry and fishing (WZ08-A)	35.3	31.5	92.0	20.4	56.9	38.4	20.8
Manufacturing (WZ08-C)	63.6	54.6	73.2	16.9	46.9	48.1	24.1
Water Supply; Sewerage, Waste Management and Remediation Activities (WZ08-E)	63.0	58.7	75.8	30.8	59.1	52.2	24.4
Construction (WZ08-F)	48.9	33.8	73.0	**15.4**	44.4	**30.4**	**14.3**
Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles (WZ08-G)	68.1	58.6	81.4	27.7	50.1	50.5	26.9
Transportation and Storage (WZ08-H)	47.0	40.2	70.7	23.0	45.8	40.3	21.0
Accommodation and Food Service Activities (WZ08-I)	62.9	50.5	82.8	33.9	40.6	41.3	22.9
Information and Communication (WZ08-J)	76.7	67.1	70.0	33.3	62.7	72.5	47.7
Financial and Insurance Activities (WZ08-K)	94.3	89.3	99.0	63.8	89.8	89.5	77.1
Real Estate Activities (WZ08-L)	72.5	63.0	78.0	28.0	51.9	53.1	28.0
Professional, Scientific and Technical Activities (WZ08-M)	79.4	66.9	70.1	29.5	55.5	55.3	26.2
Administrative and Support Service Activities (WZ08-N)	68.9	56.5	82.6	29.6	62.8	50.2	25.1
Education (WZ08-P)	77.6	60.5	78.5	22.3	51.3	60.6	23.9
Human Health and Social Work Activities (WZ08-Q)	79.2	64.2	80.3	27.9	65.1	60.4	17.3
Arts, Entertainment and Recreation (WZ08-R)	71.9	50.9	**64.3**	35.8	**36.2**	37.9	20.0
Other Service Activities (WZ08-S)	62.4	50.4	73.6	20.8	62.0	58.7	31.0

IT security measure: 1: written guidelines for information or IT security, 2: written guidelines for emergency management, 3: Compliance with the directive is regularly checked and violations are punished if necessary, 4: Certification of IT security, 5: Regular risk and vulnerability analyses, 6: Exercises/simulations for the failure of important IT systems, 7: Training courses for IT security for the entire IT system, 7: Training courses for IT security for the entire IT system, 7: Training courses for IT security for the entire IT system employees

*) only companies with guidelines (1 and/or 2)

Highlighting: bold: smallest share per IT security measure; grey background: the three smallest shares per IT security measure.

Table 46 **Technical IT security measures by first-level WZ08 classes**

in percent; weighted data

	IT security measure						
WZ08 classes (level 1; short name; only if N≥30)	8	9	10	11	12	13	14
Agriculture, forestry and fishing (WZ08-A)	79.5	80.6	100.0	100.0	**93.2**	93.1	100.0
Manufacturing (WZ08-C)	79.7	83.1	98.9	95.2	98.5	95.0	99.0
Water Supply; Sewerage, Waste Management and Remediation Activities (WZ08-E)	80.4	91.3	97.8	95.3	100.0	95.6	100.0
Construction (WZ08-F)	86.8	70.9	97.0	94.2	100.0	94.4	96.9
Wholesale and Retail Trade; Repair of Motor Vehicles and Motorcycles (WZ08-G)	87.2	88.4	99.4	93.1	98.9	96.5	98.3
Transportation and Storage (WZ08-H)	**77.4**	**68.2**	96.6	**91.0**	97.8	**89.3**	94.3
Accommodation and Food Service Activities (WZ08-I)	83.7	74.0	**96.1**	94.1	96.2	91.6	93.1
Information and Communication (WZ08-J)	92.2	95.4	100.0	98.0	100.0	98.0	100.0
Provision of Financial and Insurance Activities (WZ08-K)	97.1	94.2	100.0	96.8	100.0	100.0	100.0
Real Estate Activities (WZ08-L)	89.0	92.7	100.0	97.5	100.0	97.6	100.0
Professional, Scientific and Technical Activities (WZ08-M)	89.5	94.8	100.0	98.0	98.9	98.9	98.0
Administrative and Support Service Activities (WZ08-N)	91.5	86.3	100.0	97.1	100.0	99.1	99.5
Education (WZ08-P)	90.3	92.1	98.4	94.2	97.4	98.1	100.0
Human Health and Social Work Activities (WZ08-Q)	87.5	90.6	99.7	95.8	98.3	91.3	97.9
Arts, Entertainment and Recreation (WZ08-R)	94.7	94.7	100.0	91.2	100.0	94.7	100.0
Other Service Activities (WZ08-S)	98.3	85.7	100.0	95.2	100.0	99.2	**92.9**

IT security measure: 8: Minimum requirements for passwords., 9: individual assignment of access and user rights 10: regular backups, 11: physically separate storage of backups, 12: up-to-date anti-virus software, 13: regular and prompt installation available security updates and patches, 14: protection of the data IT systems with firewall

Highlighting: bold: smallest share per IT security measure; grey background: the three smallest shares per IT security measure.

Table 47 **Organizational IT security measures according to WZ08 classes of the second level**

in percent; weighted data

	IT security measure						
WZ08 classes (level 2; short name; only if N≥30)	1	2	3	4	5	6	7
Crop and animal production, hunting and related service activities (WZ08-01)	**35.3**	31.5		20.4	56.9	38.4	20.8
Manufacture of food products (WZ08-10)	60.3	50.0	69.0	14.0	37.3	43.8	15.3
Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials (WZ08-16)	41.2	36.4		4.0	32.7	25.0	7.1
Printing and reproduction of recorded media (WZ08-18)	69.4	67.3	84.6	20.4	65.3	44.9	12.2
Manufacture of chemicals and chemical products (WZ08-20)	60.5	71.1		21.2	44.7	84.6	23.7
Manufacture of rubber and plastic products (WZ08-22)	86.3	56.9	72.7	10.6	39.2	49.0	23.1
Manufacture of other non-metallic mineral products (WZ08-23)	44.3	27.1	**54.8**	13.0	35.0	26.7	8.2
Manufacture of basic metal (WZ08-24)	50.0	46.9			32.3	34.4	9.7
Manufacture of fabricated metal products, except machinery and equipment (WZ08-25)	64.8	54.7	78.5	18.8	55.2	47.7	37.8
Manufacture of computer, electronic and optical products (WZ08-26)	68.5	63.0	57.1	18.9	57.4	70.4	31.5
Manufacture of electrical equipment (WZ08-27)	66.7	59.5	87.0	19.1	43.2	53.8	38.0
Manufacture of machinery and equipment N.E.C. (WZ08-28)	74.6	61.5	76.3	17.3	55.7	49.2	27.6
Manufacture of furniture (WZ08-31)	51.0	30.6		**2.0**	**16.3**	38.8	22.4
Other manufacturing (WZ08-32)	62.5	69.6	75.6	32.6	66.1	59.6	17.5
Waste collection, treatment and disposal activities; materials recovery (WZ08-38)	55.9	55.9			59.4	51.5	24.2
Construction of buildings (WZ08-41)	61.8	47.1	72.3	10.6	50.0	42.6	13.3
Civil engineering (WZ08-42)	37.7	**26.7**		21.7	53.3	**21.3**	29.5
Specialised construction activities (WZ08-43)	46.8	31.1	72.8	16.1	41.3	28.3	12.5
Wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45)	68.5	57.9	79.6	25.4	48.2	43.6	22.1
Wholesale trade, except of motor vehicles and motorcycles (WZ08-46)	71.4	60.0	81.6	25.1	51.0	56.2	24.4
Retail trade, except of motor vehicles and motorcycles (WZ08-47)	62.7	57.4	82.5	33.3	50.2	47.3	34.3
Land transport and transport via pipeline (WZ08-49)	42.4	34.5	71.6	18.7	42.9	31.3	17.1
Warehousing and support activities for transportation (WZ08-52)	52.6	56.1	66.7	32.7	42.1	50.9	28.1
Accommodation (WZ08-55)	60.2	49.6	80.6	36.1	41.5	43.1	28.5
Food and beverage service activities (WZ08-56)	67.6	52.2	85.4	28.6	38.0	38.0	11.8
Publishing activities (WZ08-58)	54.8	64.5		30.0	61.3	54.8	22.6
Computer programming, consultancy and related activities (WZ08-62)	92.0	79.5	80.5	38.3	73.0	84.3	61.8
Financial service activities, except insurance and pension funding (WZ08-64)	97.6	95.2	98.8	71.2	92.5	92.9	85.7
Real Estate Activities (WZ08-68)	72.5	63.0	78.0	28.0	51.9	53.1	28.0
Legal and accounting activities (WZ08-69)	78.8	61.1	75.6	47.7	46.9	68.3	24.0
Activities of head offices; management consultancy activities (WZ08-70)	87.1	69.4	85.1	27.8	56.5	55.3	31.0
Architectural and engineering activities; technical testing and analysis (WZ08-71)	79.8	67.4	64.1	21.3	54.1	44.8	25.0
Advertising and market research (WZ08-73)	69.7	69.7		18.8	81.8	81.8	33.3
Travel agency, tour operator and other reservation service and related activities (WZ08-79)	77.1	77.1	90.0	52.3	66.7	58.3	33.3
Services to buildings and landscape activities (WZ08-81)	69.2	39.4	71.4	10.6	53.2	24.2	**6.0**
Office administrative, office support and other business support activities (WZ08-82)	68.9	60.0	81.3	28.2	58.7	69.6	46.7
Education (WZ08-85)	77.6	60.5	78.5	22.3	51.3	60.6	23.9

Human health activities (WZ08-86)	75.8	66.7	86.7	40.0	54.8	64.6	13.5
Residential care activities (WZ08-87)	80.0	62.9	77.2	22.6	76.8	48.6	24.3
Social work activities without accommodation (WZ08-88)	80.7	64.0	77.5	21.5	66.7	63.9	16.1
Sports activities and amusement and recreation activities (WZ08-93)	66.7	39.0		32.4	31.0	33.3	15.4
Activities of membership organisations (WZ08-94)	66.7	70.8	75.7	25.5	61.5	75.0	36.5
Other personal service activities (WZ08-96)	55.6	39.7	79.2	18.5	59.4	44.1	29.0

IT security measure: 1: written guidelines for information or IT security, 2: written guidelines for emergency management, 3: Compliance with the directive is regularly checked and violations are punished if necessary, 4: Certification of IT security, 5: Regular risk and vulnerability analyses, 6: Exercises/simulations for the failure of important IT systems, 7: Training courses for IT security for the entire IT system, 7: Training courses for IT security for the entire IT system, 7: Training courses for IT security for the entire IT system employees

Highlighting: bold: smallest share per IT security measure; grey background: the five smallest shares per IT security measure.

Table 48 **Technical IT security measures by WZ08 second-level classes**

in percent; weighted data

	IT security measure						
WZ08 classes (level 2; short name; only if N≥30)	8	9	10	11	12	13	14
Crop and animal production, hunting and related service activities (WZ08-01)	79.5	80.6	100.0	100.0	93.2	93.1	100.0
Manufacture of food products (WZ08-10)	**52.9**	59.7	92.6	91.4	100.0	91.7	100.0
Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials (WZ08-16)	80.4	82.1	100.0	98.2	100.0	100.0	100.0
Printing and reproduction of recorded media (WZ08-18)	98.0	100.0	100.0	**81.3**	100.0	100.0	100.0
Manufacture of chemicals and chemical products (WZ08-20)	84.2	100.0	100.0	100.0	100.0	100.0	100.0
Manufacture of rubber and plastic products (WZ08-22)	76.5	82.4	100.0	100.0	100.0	90.4	100.0
Manufacture of other non-metallic mineral products (WZ08-23)	83.3	**58.2**	100.0	85.0	100.0	85.0	100.0
Manufacture of basic metal (WZ08-24)	56.3	84.8	100.0	84.4	100.0	**71.9**	100.0
Manufacture of fabricated metal products, except machinery and equipment (WZ08-25)	80.2	84.5	99.5	96.9	97.5	91.9	97.4
Manufacture of computer, electronic and optical products (WZ08-26)	94.4	100.0	100.0	98.1	100.0	100.0	100.0
Manufacture of electrical equipment (WZ08-27)	82.1	82.3	100.0	100.0	100.0	98.7	100.0
Manufacture of machinery and equipment N.E.C. (WZ08-28)	84.6	91.9	100.0	95.1	100.0	100.0	95.9
Manufacture of furniture (WZ08-31)	69.4	63.3	**89.8**	100.0	**89.8**	100.0	100.0
Other manufacturing (WZ08-32)	87.5	91.1	100.0	98.2	100.0	100.0	100.0
Waste collection, treatment and disposal activities; materials recovery (WZ08-38)	76.5	87.9	97.0	93.5	100.0	93.8	100.0
Construction of buildings (WZ08-41)	80.6	76.7	96.1	99.2	100.0	95.2	100.0
Civil engineering (WZ08-42)	83.3	69.2	100.0	90.9	100.0	91.8	91.8
Specialised construction activities (WZ08-43)	89.0	69.2	96.6	93.0	100.0	94.3	96.8
Wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45)	89.9	85.2	97.5	92.2	100.0	95.1	97.5
Wholesale trade, except of motor vehicles and motorcycles (WZ08-46)	87.5	95.1	100.0	94.6	98.8	98.5	98.8
Retail trade, except of motor vehicles and motorcycles (WZ08-47)	85.0	80.2	100.0	91.2	98.2	94.5	98.2
Land transport and transport via pipeline (WZ08-49)	72.6	59.7	95.2	92.7	99.3	86.3	92.1
Warehousing and support activities for transportation (WZ08-52)	86.0	82.5	98.2	85.7	93.0	91.2	94.8
Accommodation (WZ08-55)	83.9	75.2	97.8	91.4	97.8	94.2	95.5
Food and beverage service activities (WZ08-56)	83.1	71.8	91.5	100.0	91.5	86.4	87.3
Publishing activities (WZ08-58)	87.1	100.0	100.0	90.3	100.0	100.0	100.0
Computer programming, consultancy and related activities (WZ08-62)	96.6	98.9	100.0	100.0	100.0	96.6	100.0

Financial service activities, except insurance and pension funding (WZ08-64)	98.8	97.6	100.0	96.1	100.0	100.0	100.0
Real Estate Activities (WZ08-68)	89.0	92.7	100.0	97.5	100.0	97.6	100.0
Legal and accounting activities (WZ08-69)	87.6	95.0	100.0	96.0	100.0	100.0	96.2
Activities of head offices; management consultancy activities (WZ08-70)	98.8	84.7	100.0	95.2	95.3	94.1	100.0
Architectural and engineering activities; technical testing and analysis (WZ08-71)	87.2	97.3	100.0	100.0	100.0	100.0	100.0
Advertising and market research (WZ08-73)	100.0	100.0	100.0	100.0	97.0	100.0	87.5
Travel agency, tour operator and other reservation service and related activities (WZ08-79)	98.0	91.8	100.0	100.0	100.0	100.0	100.0
Services to buildings and landscape activities (WZ08-81)	87.9	83.3	100.0	91.9	100.0	100.0	100.0
Office administrative, office support and other business support activities (WZ08-82)	86.7	82.2	100.0	100.0	100.0	100.0	100.0
Education (WZ08-85)	90.3	92.1	98.4	94.2	97.4	98.1	100.0
Human health activities (WZ08-86)	83.3	84.4	99.0	100.0	100.0	93.8	100.0
Residential care activities (WZ08-87)	95.9	98.6	100.0	92.3	100.0	87.7	93.3
Social work activities without accommodation (WZ08-88)	85.7	90.8	100.0	95.4	95.8	91.6	100.0
Sports activities and amusement and recreation activities (WZ08-93)	92.9	100.0	100.0	92.9	100.0	92.9	100.0
Activities of membership organisations (WZ08-94)	98.1	100.0	100.0	98.1	100.0	100.0	100.0
Other personal service activities (WZ08-96)	98.5	73.9	100.0	92.8	100.0	98.5	**87.0**

IT security measure: 8: Minimum requirements for passwords., 9: individual assignment of access and user rights 10: regular backups, 11: physically separate storage of backups, 12: up-to-date anti-virus software, 13: regular and prompt installation available security up-dates and patches, 14: protection of the data IT systems with firewall

Highlighting: bold: smallest share per IT security measure; grey background: the five smallest shares per IT security measure.

Table 49 **Companies with cyber insurance by WZ08 second-tier classes**

in percent; weighted data

	Does your company have insurance against information security breaches?			
WZ08 classes (level 2; short name; only if N≥30)	Yes	No	Don't know	N
Crop and animal production, hunting and related service activities (WZ08-01)	**0.0**	87.5	12.5	40
Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials (WZ08-16)	**0.0**	97.0	3.0	33
Manufacture of fabricated metal products, except machinery and equipment (WZ08-25)	21.7	57.6	20.7	92
Manufacture of electrical equipment (WZ08-27)	32.4	38.2	29.4	34
Manufacture of machinery and equipment N.E.C. (WZ08-28)	24.6	54.4	21.1	57
Construction of buildings (WZ08-41)	14.3	65.3	20.4	49
Civil engineering (WZ08-42)	5.3	92.1	2.6	38
Specialised construction activities (WZ08-43)	14.5	72.9	12.6	214
Wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45)	12.8	65.1	22.1	86
Wholesale trade, except of motor vehicles and motorcycles (WZ08-46)	16.8	56.7	26.4	208
Retail trade, except of motor vehicles and motorcycles (WZ08-47)	17.7	56.7	25.5	141
Land transport and transport via pipeline (WZ08-49)	17.9	74.4	7.7	78
Warehousing and support activities for transportation (WZ08-52)	9.1	75.8	15.2	33
Accommodation (WZ08-55)	24.6	63.2	12.3	57
Food and beverage service activities (WZ08-56)	19.4	77.4	3.2	31
Computer programming, consultancy and related activities (WZ08-62)	8.1	62.2	29.7	37
Financial service activities, except insurance and pension funding (WZ08-64)	69.0	19.0	11.9	42
Real Estate Activities (WZ08-68)	20.5	61.4	18.2	44
Legal and accounting activities (WZ08-69)	10.7	51.8	37.5	56
Activities of head offices; management consultancy activities (WZ08-70)	17.1	43.9	39.0	41
Architectural and engineering activities; technical testing and analysis (WZ08-71)	15.0	54.0	31.0	100
Services to buildings and landscape activities (WZ08-81)	15.4	71.8	12.8	39
Education (WZ08-85)	15.3	63.8	20.9	177
Human health activities (WZ08-86)	46.9	28.6	24.5	49
Residential care activities (WZ08-87)	26.5	61.8	11.8	34
Social work activities without accommodation (WZ08-88)	25.0	39.1	35.9	64
Activities of membership organisations (WZ08-94)	29.4	67.6	2.9	34
Other personal service activities (WZ08-96)	22.7	65.9	11.4	44

Highlighting: bold: smallest share; grey background: the five smallest shares

Table 50 **Prevalence rates for cyber-attacks in total according to WZ08 classes of the second level**

in percent; weighted data

	Total cyber-attacks[323]	
WZ08 classes (level 2; short name; only if N≥30)	Annual prevalence	Lifetime prevalence[324]
Crop and animal production, hunting and related service activities (WZ08-01)	23.6 (n=72)	48.5 (n=68)
Manufacture of food products (WZ08-10)	35.6 (n=73)	58.8 (n=68)
Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials (WZ08-16)	28.3 (n=60)	36.4 (n=55)
Printing and reproduction of recorded media (WZ08-18)	46.9 (n=49)	87.8 (n=49)
Manufacture of chemicals and chemical products (WZ08-20)	46.2 (n=39)	71.1 (n=38)
Manufacture of rubber and plastic products (WZ08-22)	46.2 (n=52)	68.6 (n=51)
Manufacture of other non-metallic mineral products (WZ08-23)	60.0 (n=60)	**94.5** (n=55)
Manufacture of basic metal (WZ08-24)	43.8 (n=32)	
Manufacture of fabricated metal products, except machinery and equipment (WZ08-25)	41.4 (n=198)	64.6 (n=192)
Manufacture of computer, electronic and optical products (WZ08-26)	40.7 (n=54)	74.1 (n=54)
Manufacture of electrical equipment (WZ08-27)	49.4 (n=79)	71.8 (n=78)
Manufacture of machinery and equipment N.E.C. (WZ08-28)	56.1 (n=123)	80.3 (n=117)
Manufacture of furniture (WZ08-31)	46.9 (n=49)	70.8 (n=48)
Other manufacturing (WZ08-32)	46.4 (n=56)	85.7 (n=56)
Waste collection, treatment and disposal activities; materials recovery (WZ08-38)	25.0 (n=32)	61.3 (n=31)
Construction of buildings (WZ08-41)	26.6 (n=128)	58.8 (n=119)
Civil engineering (WZ08-42)	22.7 (n=66)	37.7 (n=61)
Specialised construction activities (WZ08-43)	39.1 (n=442)	52.7 (n=431)
Wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45)	46.3 (n=203)	72.4 (n=203)
Wholesale trade, except of motor vehicles and motorcycles (WZ08-46)	53.1 (n=416)	73.7 (n=410)
Retail trade, except of motor vehicles and motorcycles (WZ08-47)	38.6 (n=277)	63.8 (n=271)
Land transport and transport via pipeline (WZ08-49)	26.7 (n=146)	47.6 (n=143)
Warehousing and support activities for transportation (WZ08-52)	32.8 (n=58)	52.6 (n=57)
Accommodation (WZ08-55)	33.6 (n=137)	57.8 (n=135)
Food and beverage service activities (WZ08-56)	33.8 (n=71)	64.2 (n=67)
Publishing activities (WZ08-58)	**71.0** (n=31)	86.7 (n=30)
Computer programming, consultancy and related activities (WZ08-62)	40.9 (n=88)	62.5 (n=88)
Financial service activities, except insurance and pension funding (WZ08-64)	29.4 (n=85)	54.4 (n=79)
Real Estate Activities (WZ08-68)	35.8 (n=81)	55.0 (n=80)
Legal and accounting activities (WZ08-69)	34.3 (n=105)	58.1 (n=105)
Activities of head offices; management consultancy activities (WZ08-70)	48.8 (n=86)	79.0 (n=81)
Architectural and engineering activities; technical testing and analysis (WZ08-71)	53.4 (n=193)	73.8 (n=187)
Advertising and market research (WZ08-73)	24.2 (n=33)	45.5 (n=33)
Travel agency, tour operator and other reservation service and related activities (WZ08-79)	56.3 (n=48)	75.0 (n=48)
Services to buildings and landscape activities (WZ08-81)	62.1 (n=66)	79.0 (n=62)

[323] For a description of the types of attacks included, see chapter 6.

[324] See footnote 268.

Office administrative, office support and other business support activities (WZ08-82)	34.8 (n=46)	76.1 (n=46)
Education (WZ08-85)	46.7 (n=317)	77.2 (n=312)
Human health activities (WZ08-86)	30.2 (n=96)	61.1 (n=90)
Residential care activities (WZ08-87)	25.3 (n=75)	40.5 (n=74)
Social work activities without accommodation (WZ08-88)	45.4 (n=119)	62.2 (n=119)
Sports activities and amusement and recreation activities (WZ08-93)	24.4 (n=41)	52.4 (n=42)
Activities of membership organisations (WZ08-94)	62.3 (n=53)	94.2 (n=52)
Other personal service activities (WZ08-96)	20.3 (n=69)	47.1 (n=68)

Highlighting: bold: largest share; grey background: the five largest shares

Table 51 **Annual prevalence rates by cyber-attack type and second level WZ08 classes**

in percent; weighted data

	Cyber-attack type							
WZ08 classes (level 2; short name; only if N≥30)	1	2	3	4	5	6	7	8
Crop and animal production, hunting and related service activities (WZ08-01)	13.7	6.8	8,3	0,0	7,4	0,0	1,4	8,3
Manufacture of food products (WZ08-10)	4.1	3.2	9,9	0,0	6,9	0,0	2,7	19,4
Manufacture of wood and of products of wood and cork, except furniture; manufacture of articles of straw and plaiting materials (WZ08-16)	23.3	23.3	18,3	0,0	16,1	0,0	11,7	25,0
Printing and reproduction of recorded media (WZ08-18)	4.1	0.0	24,5	10,4	10,4	2,0	2,3	33,3
Manufacture of chemicals and chemical products (WZ08-20)	15.8	13.2	28,9	0,0	0,0	**13,2**	2,6	28,9
Manufacture of rubber and plastic products (WZ08-22)	15.7	13.7	9,8	0,0	3,9	1,9	5,9	19,6
Manufacture of other non-metallic mineral products (WZ08-23)	21.4	**26.8**	37,5	8,9	**30,0**	0,0	10,0	36,7
Manufacture of basic metal (WZ08-24)	3.1	3.1	9,4	0,0	0,0	3,1	21,9	37,5
Manufacture of fabricated metal products, except machinery and equipment (WZ08-25)	11.2	3.1	16,9	1,0	1,6	1,1	6,6	25,6
Manufacture of computer, electronic and optical products (WZ08-26)	13.0	3.7	14,8	0,0	3,7	1,9	5,6	24,5
Manufacture of electrical equipment (WZ08-27)	20.3	8.1	32,1	6,4	1,3	6,8	9,0	23,1
Manufacture of machinery and equipment N.E.C. (WZ08-28)	22.2	32.2	39,2	1,6	2,7	6,0	16,9	38,3
Manufacture of furniture (WZ08-31)	12.2	12.2	14,3	0,0	18,8	10,4	10,4	32,7
Other manufacturing (WZ08-32)	**26.8**	23.2	28,6	1,8	8,9	11,5	3,6	38,2
Waste collection, treatment and disposal activities; materials recovery (WZ08-38)	9.4	6.5	12,5	0,0	6,5	0,0	9,4	9,4
Construction of buildings (WZ08-41)	16.3	8.5	12,5	3,9	3,9	0,0	9,3	2,3
Civil engineering (WZ08-42)	9.1	9.1	18,2	1,5	0,0	0,0	9,1	11,5
Specialised construction activities (WZ08-43)	8.1	10.3	23,7	1,1	3,7	1,1	3,0	23,6
Wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45)	19.1	20.7	27,2	4,9	5,4	3,0	12,8	23,2
Wholesale trade, except of motor vehicles and motorcycles (WZ08-46)	10.1	12.0	26,1	5,2	5,4	1,5	11,4	26,7
Retail trade, except of motor vehicles and motorcycles (WZ08-47)	17.6	9.3	19,0	5,5	4,1	5,4	4,3	17,0
Land transport and transport via pipeline (WZ08-49)	6.3	9.1	12,8	2,1	4,8	4,1	7,6	11,8
Warehousing and support activities for transportation (WZ08-52)	12.5	3.5	15,8	0,0	1,8	1,8	8,8	17,9
Accommodation (WZ08-55)	16.1	6.6	21,3	2,2	6,0	2,9	2,2	18,7
Food and beverage service activities (WZ08-56)	1.4	23.9	18,8	4,2	8,8	4,4	8,7	20,6
Publishing activities (WZ08-58)	6.3	3.2	**58,1**	0,0	15,6	12,9	3,2	**53,3**
Computer programming, consultancy and related activities (WZ08-62)	8.0	4.5	17,2	1,1	21,6	1,1	6,8	17,0
Financial service activities, except insurance and pension funding (WZ08-64)	3.5	10.8	15,7	0,0	2,4	0,0	3,5	22,2
Real Estate Activities (WZ08-68)	12.5	8.8	15,2	1,2	8,8	3,7	12,2	25,0
Legal and accounting activities (WZ08-69)	14.3	6.7	11,4	0,0	1,0	0,0	1,9	24,0
Activities of head offices; management consultancy activities (WZ08-70)	12.9	10.1	44,7	**10,6**	8,3	5,9	9,4	17,9
Architectural and engineering activities; technical testing and analysis (WZ08-71)	18.1	12.8	24,9	6,8	11,5	7,3	10,9	27,7
Advertising and market research (WZ08-73)	3.0	3.1	3,1	0,0	15,2	0,0	3,0	21,2
Travel agency, tour operator and other reservation service and related activities (WZ08-79)	2.1	8.9	24,5	0,0	2,1	8,3	**31,3**	39,6
Services to buildings and landscape activities (WZ08-81)	16.1	12.7	25,8	7,6	11,9	1,6	15,2	28,8
Office administrative, office support and other business support activities (WZ08-82)	4.4	7.1	8,7	2,3	4,8	0,0	17,4	24,4
Education (WZ08-85)	16.4	14.8	21,7	2,6	8,3	5,0	7,4	16,8

Human health activities (WZ08-86)	9.5	15.8	12,4	0,0	10,4	5,6	14,6	14,6
Residential care activities (WZ08-87)	11.4	10.7	13,5	0,0	1,3	0,0	1,4	20,3
Social work activities without accommodation (WZ08-88)	14.0	9.5	32,2	4,2	1,7	9,2	17,6	31,1
Sports activities and amusement and recreation activities (WZ08-93)	16.7	2.4	9,5	0,0	2,4	2,4	2,4	4,8
Activities of membership organisations (WZ08-94)	5.8	12.2	27,1	2,1	20,8	0,0	25,0	30,8
Other personal service activities (WZ08-96)	1.4	1.6	10,3	0,0	0,0	0,0	2,9	10,3

Cyber-attack type: 1: ransomware, 2: spyware, 3: other malware, 4: manual hacking, 5: (D)DoS, 6: defacing, 7: CEO fraud, 8: phishing

Highlighting: bold: largest share per type of attack; grey background: the five largest shares per type of attack

Table 52 **Share of companies with affected data by data type and second level WZ08 classes**

in percent; weighted data

	Data type					
WZ08 class (level 2; short name; only if N≥30)	1	2	3	4	5	N
Manufacture of fabricated metal products, except machinery and equipment (WZ08-25)	21.3	9.8	16.4	4.9	1.6	61
Manufacture of electrical equipment (WZ08-27)	15.8	0.0	0.0	13.5	2.9	37
Manufacture of machinery and equipment N.E.C. (WZ08-28)	43.9	19.3	3.6	22.8	**30.4**	57
Construction of buildings (WZ08-41)	0.0	0.0	0.0	0.0	0.0	33
Specialised construction activities (WZ08-43)	25.6	6.9	12.5	9.4	6.3	160
Wholesale and retail trade and repair of motor vehicles and motorcycles (WZ08-45)	**57.5**	**28.7**	**27.6**	23.0	23.0	87
Wholesale trade, except of motor vehicles and motorcycles (WZ08-46)	21.3	10.6	10.6	13.8	7.4	188
Retail trade, except of motor vehicles and motorcycles (WZ08-47)	30.7	10.0	11.3	**29.7**	9.9	100
Land transport and transport via pipeline (WZ08-49)	17.1	16.7	2.9	5.6	5.6	36
Accommodation (WZ08-55)	23.3	21.4	16.3	0.0	2.3	43
Computer programming, consultancy and related activities (WZ08-62)	2.9	2.8	0.0	2.8	0.0	35
Legal and accounting activities (WZ08-69)	31.4	20.0	5.7	14.3	28.6	34
Activities of head offices; management consultancy activities (WZ08-70)	30.6	13.9	13.9	27.0	16.2	36
Architectural and engineering activities; technical testing and analysis (WZ08-71)	22.7	6.7	11.9	12.4	10.2	88
Services to buildings and landscape activities (WZ08-81)	30.0	11.1	9.8	0.0	9.8	40
Education (WZ08-85)	22.3	10.7	3.3	11.6	9.1	121
Social work activities without accommodation (WZ08-88)	38.6	20.5	4.5	6.8	27.3	44

Data type: 1: Data in total, 2: non-public customer data, 3: non-public data of business partners, 4: Product data, 6: Strategy, sales and financial information.

Highlighting: bold: largest share per data type; grey background: the three largest shares per data type

Table 53 **Overview of the state of research in Chapter 2**

		Studies/reports				
Characteristics		1	2	3	4	5
formally	**Author*in/institution**	Bitkom e.V.	Bitkom e.V.	Federal Criminal Police Office (BKA)	BSI, Alliance for Cyber Security	BSI, Alliance for Cyber Security
	Year of publication	2017	2018	2018	2018	2019
	Title	Economic protection in the digital world	Espionage, sabotage and data theft - economic protection in industry	Cybercrime - Federal Situation 2017	Cyber Security Survey 2017	Cyber Security Survey 2018 (version 18.04.2019)
methodological	**Method**	CATI	CATI	Secondary analysis (Police statistic)	Online survey	Online survey
	Region	GER	GER	GER	GER	GER
	Survey period	01.-03.2017	05.2018	2017	10.-11.2017	02.-03.2019
	Basic population	all companies >10 Employees	Industrial companies >10 Employees	n.r.	n.a.	n.a.
	Selection population (contact details)	n.a.	n.a.	n.r.	n.a.	n.a.
	Sample type	stratified random sample	stratified random sample	n.r.	random sample	random sample
	Net sample	1,069	503	n.r.	879	1,039
	Sector differentiation	No sectors mentioned	5 sectors Chemical/Pharmaceutical, Automotive, Mechanical and Plant Engineering, H.v. Communication/Electronics, Other	n.r.	4 sectors User companies (49 %), IT-DL/manufacturers/providers (20 %), others (17 %), public service (14 %)	4 **sectors** Other (54 %), Information & Communication (18 %), Energy Supply (17 %), Public Administration (11 %)
	Size differentiation	10-99 100-499 >500	10-99 100-499 >500	n.r.	1-499 (66 %) >500 (33 %)	1-249 (57 %) >250 (43 %)
content-related	**Risk assessment**				✓	✓
	Prevalence	✓	✓		✓	✓
	IT security structures	✓	✓		✓	✓
	Investments/budget					
	Non-financial damage/ consequences	✓	✓	✓	✓	✓
	Costs incurred in EUR	✓	✓	✓		
	Reporting behaviour	✓	✓	✓		
	Cyber insurance		✓			
	Recommendations for action		✓			

		Studies				
	Characteristics	6	7	8	9	10
formally	**Author*in/institution**	BSI, Alliance for Cyber Security	Federal Printing Office	CISCO Inc.	DsiN e.V.	Eco e.V.
	Year of publication	2016	2017	2017	2016	2017
	Title	Survey on ransomware-related affectedness	Digitization and IT security in German companies	2017 Annual Cybersecurity Report/ Security Capabilities Benchmark Study	Security Monitor Medium-sized Businesses 2016	eco Study IT Security 2017
methodological	**Method**	Online survey	CATI	n.a.	Online survey	Expert interviews
	Region	GER	GER	International (13 countries)	GER	GER
	Survey period	04.2016	02.-03.2017	n.a.	06.15-03.2016	n.a.
	Basic population	n.a.	all companies >20 Employees	n.a.	n.a.	n.a.
	Selection population (contact details)	n.a.	n.a.	n.a.	n.a.	n.a.
	Sample type	n.a.	stratified random sample	n.a.	n.a.	n.a.
	Net sample	592	500	2,912	1,320	590
	Sector differentiation	no sectors mentioned	9 sectors **Top three:** Machinery/plant engineering (13 %), banks/insurance companies (13 %), IT/telecommunications (13 %)	11 sectors **Top three:** Financial Services (18 %), Non-Key Industry (16 %), Manufacturing (12 %)	No sectors mentioned	7 sectors **Top three:** IT/telecommunications (49 %), services (21 %), public institutions (9 %)
	Size differentiation	1-49 (30 %) 50-249 (20 %) 250-999 (20 %) 1,000-10,000 (20 %) >10,000 (7 %)	20-99 (35 %) 100-499 (35 %) 500-1,999 (20 %) >2,000 (10 %)	250-999 (50 %) 1,000-9,999 (38 %) >10,000 (12 %)	1-9 (34 %) 10-50 (26 %) 51-200 (18 %) 201-500 (10 %) <500 (12 %)	1-10 (24 %) 11-50 (24 %) 51-250 (18 %) 251-1,000 (15 %) <1,000 (18 %)
content-related	**Risk assessment**	✓		✓		✓
	Prevalence	✓				
	IT security structures	✓	✓	✓	✓	✓
	Investments/budget		✓	✓		✓
	Non-financial damage/ consequences	✓		✓		
	Costs incurred in EUR	✓				
	Reporting behaviour	✓				
	Cyber insurance					
	Recommendations for action				✓	

		Studies				
Characteristics		11	12	13	14	15
formally	**Author*in/institution**	GDV e.V.	Gehem et al. (The Hague Centre for Strategic Studies)	Hillebrand et al (wik GmbH)	Hiscox Ltd	IBM Cooperation
	Year of publication	2018	2015	2017	2018	2018
	Title	Cyber risks in medium-sized companies	Assessing Cyber Security	Current situation of IT security in SMEs	Hiscox Cyber Readiness Report	IBM X-Force Threat Intelligence Index 2018
methodological	**Method**	Interviews	Qualitative meta-analysis of reports	CATI	Online survey	Secondary Analysis of Customer Data
	Region	GER	International (15 countries)	GER	International (5 countries)	International
	Survey period	03.-04.2018	n.a.	03.-05.2017	10.-11.2017	2017
	Basic population	n.a.	n.r.	all relevant companies. Industries m. 1-499 Employees	n.a.	n.a.
	Selection population (contact details)	n.a.	n.r.	commercial company database	n.a.	n.a.
	Sample type	n.a.	n.r.	stratified random sample	n.a.	n.a.
	Net sample	300	65 reports	1,508	4,103	> 1 million
	Sector differentiation	n.a.	n.r.	12 sectors according to WZ classes	16 sectors **Top three:** Technology/ Media/ Communication (14 %), Retail & Wholesale (8 %), Healthcare & Pharmaceutical (8 %)	5 sectors Financial Services, Information & Communication, Manufacturing, Retail, Professional Services
	Size differentiation	n.a.	n.r.	1-49 (33 %) 50-99 (33 %) 100-499 (33 %)	2-249 (70 %) >250 (30 %)	n.a.
content-related	**Risk assessment**	✓		✓	✓	
	Prevalence		✓		✓	✓
	IT security structures	✓		✓	✓	✓
	Investments/budget	✓		✓	✓	
	Non-financial damage/ consequences	✓	✓	✓	✓	
	Costs incurred in EUR		✓		✓	
	Reporting behaviour					
	Cyber insurance	✓			✓	
	Recommendations for action	✓		✓		

		Studies				
Characteristics		16	17	18	19	20
formally	**Author*in/institution**	North Chamber of Industry and Commerce (IHK)	Allensbach Institute for Public Opinion Research (i.A. Deutsche Telekom)	Maria Kjaerland	Klahr et al (UK Department for Culture, Media & Sport)	Bollhöfer & Jäger (MPI)
	Year of publication	2013	2015	2006	2017	2018
	Title	Company survey on how the North German economy is affected by cybercrime	Cyber Security Report 2015	A taxonomy and comparison of computer security incidents from the commercial and government sectors	Cyber Security Breaches Survey 2017	Industrial espionage and competitive intelligence
methodological	**Method**	Online survey	CATI	Secondary Analysis Event Data (CERT CC)	CATI + face-to-face interviews	Paper-Pencil- + Online Survey
	Region	GER	GER	USA	UK	GER
	Survey period	01.-02.2013	08.-10.2015	2001/02	10.2016-01.2017	06.-09.2017
	Basic population	Member companies of various associations in North GER	n.a.	n.r.	n.a.	Industry-related Unt. <251 Employees
	Selection population (contact details)	6,000 companies written to	n.a.	n.r.	n.a.	23,462 companies, based on Hoppenstedt company database, 6,284 written to
	Sample type	n.a.	n.a.	n.r.	Random sample	Random sample
	Net sample	713	645	1,397	1,523	583
	Sector differentiation	4 Sectors Services (47 %), Industry (24 %), Trade (17 %), Other (12 %)	no sectors mentioned	commercial and public sector	All sectors excluding individual companies, public sector, forestry and agriculture, fishing and mining	15 sectors of the manufacturing industry or industry-related DL **Top three:** mechanical engineering (23 %), metal industry (15 %), electrical engineering (11 %)
	Size differentiation	1-10 (21 %) 11-50 (26 %) 51-100 (11 %) 101-250 (16 %) >250 (26 %)	50-99 100-249 250-999 >1,000	n.a.	2-9 (33 %) 10-49 (31 %) 50-249 (24 %) >250 (11 %)	1-9 (5 %) 10-49 (41 %) 50-249 (44 %) >250 (10 %)
content-related	**Risk assessment**	✓	✓		✓	✓
	Prevalence	✓			✓	✓
	IT security structures	✓			✓	✓
	Investments/budget	✓	✓		✓	
	Non-financial damage/ consequences	✓			✓	✓
	Costs incurred in EUR				✓	
	Reporting behaviour	✓			✓	✓
	Cyber insurance				✓	
	Recommendations for action	✓			✓	

		Studies				
	Characteristics	21	22	23	24	25
formally	Author*in/institution	Paoli et al.	Ponemon Institute (i.A. Accenture)	Ponemon Institute (i.A. IBM)	Ponemon Institute (i.A. IBM)	PwC Network
	Year of publication	2018	2017	2016	2017	2018
	Title	The impact of cybercrime on businesses	COST OF CYBER CRIME STUDY	The Cyber Resilient Organization in Germany	2017 Cost of Data Breach Study	1. Strengthening digital society against cyber shocks und 2. Revitalizing privacy and trust in a data-driven world
methodological	Method	Online survey	Qualitative interviews	Questionnaire	Qualitative interviews	Online survey
	Region	BEL	International (7 countries)	GER, US, UK	International	International (122 countries)
	Survey period	07.-08.2016	n.a.	05.2015	n.a.	04.-05.2017
	Basic population	Belgium companies with particular relevance for cyber-attacks	n.a.	n.a.	n.a.	n.a.
	Selection population (contact details)	9,249 companies with particular relevance to cyber-attacks (trade, DL, finance) based on FEB data were contacted	n.a.	n.a.	n.a.	n.a.
	Sample type	Conscious selection	n.a.	n.a.	n.a.	n.a.
	Net sample	310	254	445	419	9,500
	Sector differentiation	4 sectors Other (57 %), Technology (23 %), Chemical & Life Science (10 %), Commerce & Services (10 %)	15 sectors with < 2,000 to >25,000 **Top three:** Financial (16 %), Industrial (12 %), Services (11 %)	14 sectors **Top three:** Financial Services (15 %), Public Sector (11 %), Health & Pharmaceuticals (10 %)	17 sectors **Top three:** Financial (15 %), Industrial (15 %), Services (14 %)	n.a.
	Size differentiation	1-49 (52 %) 50-249 (22 %) >250 (27 %)	<2.000 (11 %) 2,000-5,000 (17 %) 5,001-10,000 (22 %) >10,001 (50 %)	1-499 (11 %) 500-1,000 (19 %) 1,001-5,000 (27 %) 5,001-10,000 (24 %) >10,000 (19 %)	1-499 (12 %) 500-1,000 (20 %) 1,001-5,000 (26 %) 5,001-10,000 (21 %) >10,000 (21 %)	n.a.
content-related	Risk assessment			✓		✓
	Prevalence	✓				
	IT security structures		✓	✓		✓
	Investments/budget		✓	✓		
	Non-financial damage/ consequences	✓	✓			
	Costs incurred in EUR	✓	✓		✓	
	Reporting behaviour					
	Cyber insurance					
	Recommendations for action					

		Studies				
Characteristics		26	27	28	29	30
formally	Author*in/institution	PwC AG	PwC Strategy& (i.A. BMI)	Sasha Romanosky	Ramona Rantala (U.S. Department of Justice)	Osborne et al (UK Home Office)
	Year of publication	2017	2016	2016	2008	2018
	Title	In the sights of the cyber gangsters	Cyber security strategy	Examining the costs and causes of cyber incidents	Cybercrime against Businesses, 2005	Crime against businesses: Findings from the 2017 Commercial Victimisation Survey
methodological	Method	CATI	Online survey	Secondary analysis economic loss data	Paper Pencil Survey	CATI
	Region	GER	GER	USA	USA	England, Wales
	Survey period	09.-10.2016	04.-05.2016	n.a.	n.a.	09.-12.2017
	Basic population	n.a.	n.a.	n.a.	n.a.	All companies in England and Wales with a turnover in excess of GBP 79 000
	Selection population (contact details)	n.a.	Associated companies of BDI, BITKOM, DIHK, UP KRITIS	Commercial company database	Commercial company database Dunn & Bradstreet	Interdepartmental Business Register (IDBR))
	Sample type	n.a.	n.a.		stratified random sample	stratified random sample
	Net sample	400	309	>12,000 observations	8,079	1,865 (split half: 4,027)
	Sector differentiation	9 sectors **Top three:** Other (22 %), Industry (20 %), Trade/Consumption (20 %)	19 sectors **Top three:** Manufacturing industry (17 %), IT service providers (16 %), energy supply (13 %)	10 sectors according to NAICS	36 sectors according to NAICS **Top three:** Manufacturing, Healthcare, Utilities	4 sectors by UK SIC Producing industry (26 %), Entertainment & Arts (25 %), Wholesale & Retail (24 %), Forestry & Agriculture (24 %)
	Size differentiation	200-499 (50 %) 500-1,000 (50 %)	1-9 (9 %) 10-49 (14 %) 50-249 (23 %) 250-499 (9 %) 500-999 (10 %) 1,000-9,999 (20 %) >10,000 (15 %)	n.a.	2-24 (18 %) 25-99 (22 %) 100-999 (25 %) >1,000 (27 %)	1-9 (57 %) 10-49 (24 %) >50 (19 %)
content-related	Risk assessment	✓	✓			
	Prevalence	✓	✓	✓	✓	✓
	IT security structures	✓	✓		✓	✓
	Investments/budget	✓	✓			
	Non-financial damage/ consequences	✓		✓	✓	
	Costs incurred in EUR	✓		✓	✓	
	Reporting behaviour		✓			
	Cyber insurance					
	Recommendations for action	✓				

Characteristics		Studies	
		31	32
formally	**Author*in/institution**	Vanson Bourne (i.A. Dell Inc.)	Verizon LLC
	Year of publication	2014	2018
	Title	Protecting the organization against the unknown	2018 Data Breach Investigations Report
methodological	**Method**	Online survey + CATI	Secondary analysisCustomer system data
	Region	International	International
	Survey period	10.-11.2013	n.a.
	Basic population	n.a.	n.a.
	Selection team (contact details)	n.a.	n.a.
	Sample type	n.a.	n.a.
	Net sample	1,440	> 1 million Observations
	Sector differentiation	no sectors mentioned	21 sectors
	Size differentiation	501-1,000 (23 %) 1,001-3,000 (23 %) 3,001-5,000 (23 %) 5,001-10,000 (23 %) >10,000 (8 %)	n.a.
content-related	**Risk assessment**	✓	
	Prevalence		✓
	IT security structures	✓	✓
	Investments/budget	✓	
	Non-financial damage/ consequences		
	Costs incurred in EUR	✓	
	Reporting behaviour		
	Cyber insurance		
	Recommendations for action		

ANNEX 2: QUESTIONNAIRE

Brief description of the questionnaire used (Interview/questionnaire was originally conducted in German language; filtering sequences are not shown)

A Introduction

A01 In which area are you active in your company?
(Management/ Board of Directors; IT & Information Security; Data Protection; Plant Safety; Revision/Audit; External Service Provider; Other [with free text]; I don't know; Not specified [multiple answers possible])

A02 Why do you think your company could become a target of a cyber-attack? Do you have...?
(Special products, manufacturing processes or services [e.g. due to special technology, design, materials, innovation]; special reputation/customer base [e.g. high level of awareness, high security standards, special discretion]), response options: (Yes; No; Do not know; Not specified)

A03 How high do you estimate the risk for your company to be damaged by a cyber-attack in the next 12 months, ...
(... which also affects many other companies at the same time? [e.g. malware sent out en masse]; ... which only affects your company? [e.g. targeted espionage attack]), possible answers: (Very low; Rather low; Rather high; Very high; Don't know; Not specified)

B Experienced attacks

B01 Always related to the last 12 months: How often was your company affected by the following types of attack and had to react?
(Ransomware, which had the goal of encrypting company data; Spyware, which had the goal of spying out user activities or other data; Other malicious software - e.g. viruses, worms or Trojans; Manual hacking, i.e. Manipulation of hardware and software without the use of specific malware; Denial of Service ((D)DoS) attacks, which aimed to overload web or email servers; Defacing attacks, which aimed to modify the company's web content without authorization; CEO fraud, in which a company executive was faked in order to cause certain actions by employees; Phishing, in which employees were fooled with real-looking emails or web pages in order to e.g. prevent the use of the company's web site e.g. to obtain sensitive company data [multiple answers possible]), reply options: (Number [numeric]; Don't know; Not specified)

B02 Has your company been threatened with any of the cyber-attacks described above in the last 12 months by an attacker?
(Yes; No; Don't know; Not specified)

B03 How likely do you think it is that a cyber-attack on your company has occurred in the last 12 months but has not been noticed?
(Very unlikely; Rather unlikely; Rather likely; Very likely; Don't know; Not specified)

B04 What cyber-attack has your company ever been affected by?
(Ransomware attack; Spyware attack; Other malware attack; Manual hacking; (D)DoS attack; Defacing attack; CEO fraud; Phishing; Other attack [multiple answers possible]), response options: (Yes; No; Don't know; Not specified)

B05 Which cyber-attack of the last 12 months was the most severe?
(Ransomware attack; Spyware attack; Other attack with malware; Manual hacking; (D)DoS attack; Defacing attack; CEO fraud; Phishing; Other attack [multiple answers possible; only if B01 at least once number>0]), response options: (Yes; No; Don't know; Not specified)

B06 Was this most severe attack threatened in advance by an attacker?
(Yes; No; Don't know; Not specified [only on the most severe cyber-attack of the last 12 months])

B07 Are there any suspicions from which circle the perpetrator or perpetrators come?
(Former or active employees; Business partners (e.g. service providers, suppliers); Competitors; Other outsiders; No (no assumption); Don't know; Not specified [only on the most severe cyber-attack of the last 12 months])

B07a From which hierarchical level did the perpetrator or perpetrators come?
(Management or top management; Middle management; Staff; Don't know; Not specified [multiple answers possible; only if B07 = "employee" or "business partner"; only for the most severe cyber-attack of the last 12 months])

B08 Was there a ransom demand during this attack? How much was it?
(Yes [with numerical value in EUR]; No; Don't know; Not specified [only the most severe cyber-attack of the last 12 months])

B08a Has your company complied with the ransom demand?
(Yes; No; Don't know; Not specified [only on the most severe cyber-attack of the last 12 months])

B08b Did the attackers keep their promises (data decryption or stopping the attack)?
(Yes; No; Don't know; Not specified [only on the most severe cyber-attack of the last 12 months])

B09 You were the victim of a malware attack. What was the infection path? By...
(E-mail; Website (e.g. active content, downloads); storage media (e.g. USN, SD-Cars, CD); mobile devices (e.g. net/notebooks, tablets, smartphones etc.); other known infection path [multiple answers possible; only for the most severe cyber-attack of the last 12 months]) Answer options: (Yes; Probably; No; Don't know; Not specified)

B10 Were the following IT systems affected by the most severe attack?
(web presence (e.g. online marketplaces, shops, customer portals); e-mail and communication (e.g. partner portals, network storage); order and customer management (e.g. appointment and reservation systems, invoice management); production control (machine and plant control); warehousing and logistics; banking and trading; accounting and controlling (e.g. for annual financial statements, preparation of reports); other software to provide services (e.g. project planning, CAD, static calculations) [multiple answers possible; only for the most severe cyber-attack of the last 12 months]), response options: (Yes; No; Don't know; Not specified)

B10a If so, how important is this IT system for your company?
(Web presence; e-mail and communication; order and customer management; production control; locations and logistics; banking & trading; accounting and controlling;

provision of services [multiple answers possible; only for the most severe cyber-attack of the last 12 months]), possible answers: ((rather) important; (rather) unimportant)

B10b For how long could it not be used or only to a very limited extent?
(Web presence; e-mail and communication; order and customer management; production control; locations and logistics; banking & trading; accounting and controlling; provision of services [multiple answers possible; only for the most severe cyber-attack of the last 12 months]), response options: Outage in hours [numeric])

B11 Was the following data affected by the attack?
(Non-public customer data (e.g. access data, bank data, addresses, patient data, etc.); non-public data of business partners (e.g. access data, bank data, addresses, etc.); product data (e.g. construction plans, recipes, source codes, etc.); strategy, sales and financial information (e.g. price lists, reorganisation plans, acquisitions, financial and accounting data [multiple answers possible; only for the most severe cyber-attack of the last 12 months]), response options: (Yes; No; Don't know; Not specified)

B11a Has this data been deleted, manipulated, stolen or encrypted?
(Non-public customer data (e.g. access data, bank data, addresses, patient data, etc.); non-public data of business partners (e.g. access data, bank data, addresses, etc.); product data (e.g. construction plans, recipes, source codes, etc.); strategy, sales and financial information (e.g. price lists, reorganisation plans, acquisitions, financial and accounting data [multiple answers possible; only for the most severe cyber-attack of the last 12 months]), answer options: (Deleted; Manipulated; Stolen; Encrypted; none of these; don't know; Not specified)

B12 Did the company incur direct costs from the attack? If yes, what was the approximate amount?
(External consultation (e.g. legal advice, emergency management); Immediate measures for defence and clarification; Damages/penalties; Outflow of funds; Business interruption; Restoration/replacement [multiple answers possible; only for the most severe cyber-attack of the last 12 months], response options: (Yes [with numerical indication in EUR]; No; Not specified)

B13 Who has learned of this incident?
(Customers; business partners; insurers; owners of the company; public [multiple answers possible; only for the most severe cyber-attack of the last 12 months], possible answers: (Yes; No; Don't know; Not specified)

B14 To which government agencies/authorities have you contacted about this incident?
(Nearest police station; Police cybercrime unit; Office for the Protection of the Constitution; Federal Office for Information Security (BSI); State Data Protection Commissioner; Other; Not a governmental agency [multiple answers possible; only for the most severe cyber-attack of the last 12 months], possible answers: (Yes; No; Don't know; Not specified)

B15 Has the cyber-attack been reported to the police?
(Yes; No; Don't know; No information [only on the most severe cyber-attack of the last 12 months])

B16 How do you evaluate the work of the police or law enforcement agencies in your case?
(The investigation has disrupted our operations; I am generally satisfied with the work of the police; I would recommend other companies to report cyber-attacks [multiple

answers possible; only on the most severe cyber-attack in the last 12 months and if reported to the police], possible answers: (Fully agree; Rather Agree; Rather Disagree; Fully disagree; Don't know; Not specified)

B17 Were the perpetrators in your case identified?
(Yes; No; Don't know; Not specified [only on the most severe cyber-attack of the last 12 months and if reported to the police])

B18 Why was the cyber-attack not reported to the police?
(Because there was a risk of damage to the company's image; because there was a risk of disruption to work; because authorities might demand access to confidential data; low chance of success in the investigation; I didn't know who to turn to for this; other [multiple answers possible; only for the most severe cyber-attack of the last 12 months and in the case of no report to the police]): (Yes; No; Don't know; Not specified)

C IT security structures

C01 Which of the following measures are currently in place in your company? Please also indicate whether this was already in place before or after the most severe cyber-attack.
(Written guidelines for information and IT security; written guidelines for emergency management; regular risk and vulnerability analyses; compliance with the guidelines is regularly checked and violations are punished if necessary; certification of IT security (e.g. according to ISO 27001 or VdS 3473); IT security training for employees; exercises or simulations for the failure of important IT systems; minimum requirements for passwords; individual assignment of access and user rights depending on the task; regular backups [daily; weekly; less frequently]; physically separate storage of backups; up-to-date anti-virus software; regular and prompt installation of available security updates and patches; protection of IT systems with a firewall [multiple answers possible]), response options: (Yes; No; Only after the attack; don't know; Not specified)

C02 What type of firewall do you use?
(Simple firewall, i.e. packet filtering by source and destination address by software firewall or router at network level; Extended firewall, i.e. additional monitoring and filtering by packet content (Deep Packet Inspection DPI) at application level and logging of data traffic; Don't know; Not specified [only if protection of IT systems with a firewall = Yes])

C03 Does your company have an insurance against information security breaches (cyber insurance)?
(Yes; No; Don't know; Not specified [Split-Half method: Group B only])

C04 Would you recommend cyber insurance to others?
(Yes; No; Don't know; Not specified [Split-Half method: Group B only; only if cyber insurance is available])

C04a Have you ever tried to take out your cyber insurance?
(Yes; No; Don't know; Not specified [Split-Half method: Group B only; only if cyber insurance is available])

C04b Have you received compensation from the insurance company?
(Yes; No; Don't know; Not specified [Split-Half procedure: only group B; only if cyber insurance is available and services are used])

C04c Did this cover all the damage?

(Yes; No; Don't know; Not specified [Split-Half Procedure: Group B only; only if cyber insurance exists and benefits are claimed and received])

C05 Why does your company not have cyber insurance?
(We haven't dealt with this yet; The price-performance ratio is not right; Other reason; don't know; Not specified [Split-Half procedure: only group B; multiple answers possible; only if no cyber insurance is available])

C06 To what extent do the following statements apply to your company?
(The management is aware of IT risks and complies with the specifications; The staff is aware of IT risks and complies with the specifications; A lot is being done in the company for IT security ('more than classic protective measures') [multiple answers possible]), possible answers: (Does not apply at all; Rather does not apply; Rather applies; Applies completely; Don't know; Not specified)

C07 How big was the budget in the last 12 months for...
(... the IT as a whole (incl. personnel, consulting, hardware and software); ... IT security and information security, incl. personnel, consulting, hardware and software), possible answers: (numerical indication in EUR or classified: ≤ 50,000; < 100.00; < 500,000; < 1 million; < 5 million; < 10 million; 10 million and more; not applicable, don't know; not specified])

C08 Who do you contact to obtain information on IT and information security?
(State institutions (e.g. Office for the Protection of the Constitution, Police, BSI); IT security software manufacturers; consulting service providers; professional associations, chambers (e.g. IHK, BVMW); Internet research; technical literature/ journals; other; do not contact anyone [multiple answers possible]), answer possibilities: (Yes; No; Don't know; Not specified)

D Company characteristics

D01 When was your company founded?
(Foundation year or age classified: ≤ 2 years; < 10 years; < 25 years; < 100 years; from 100 years; don't know; not specified)

D02 Do you consider your company to be a critical infrastructure in terms of the IT security law?
(Yes; No; Don't know the law; Don't know; Not specified)

D03 How high was the total turnover of your company in the last financial year?
(numerical indication in EUR or classified: ≤ 500,000 EUR; < 1 million EUR; < 2 million EUR; < 10 million EUR; < 50 million EUR; < 500 million EUR; 500+ million EUR)

D04 Does your company export products or services?
(Yes; No; Don't know; Not specified [only the company, not the group])

D05 How many locations with their own IT infrastructure does your company have ...
(...in Germany; abroad [only the company, not the group]), possible answers: (numerical specification; Don't know; Not specified)

D06 How many employees in your company invest the majority of their working time in ...
(... the operation of IT in total; thereof especially the operation of IT- and information security?), possible answers: (numerical indication; Don't know; Not specified)

D07 Has your company outsourced IT functions?
(Email & communication; network administration & maintenance; web presence (e.g. online marketplaces, shops, customer portals); cloud software & cloud storage; IT security (e.g. incident detection, SIEM, threat intelligence); other; no IT functions outsourced [multiple answers possible]), response options: (Yes; No; Don't know; Not specified)

D08 Are detailed responsibilities, contacts and job descriptions of employees publicly available on the Internet?
(Yes; Partially; No; Don't know; Not specified)

FIGURES

TABLES

BIBLIOGRAPHY

Adams, Anne; Sasse, Martina Angela (1999): Users are not the enemy. Why users compromise security mechanisms and how to take remedial measures. In Communications of the ACM 42 (12), pp. 40–46.

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

Bayerl, Petra Saskia; Rüdiger, Thomas-Gabriel (2018): Braucht eine digitale Gesellschaft eine digitale Polizei? In Deutsche Polizei (7), pp. 4–14.

Berg, Achim; Niemeier, Michael (2019): Wirtschaftsschutz in der digitalen Welt. Bitkom e.V. Berlin, 11/6/2019. Available online at https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019.pdf, checked on 11/7/2019.

Bitkom e.V. (2017): Wirtschaftsschutz in der digitalen Welt. Available online at https://www.bitkom.org/Presse/Anhaenge-an-PIs/2017/07-Juli/Bitkom-Charts-Wirtschaftsschutz-in-der-digitalen-Welt-21-07-2017.pdf, checked on 8/28/2018.

Bitkom e.V. (2018): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie. Studienbericht 2018.

Blanke, Karen; Gauckler, Britta; Sattelberger, Sabine (2011): Fragebogen auf dem Prüfstand. Testmethoden und deren Einsatz in der amtlichen Statistik. In Wirtschaft und Statistik (8/2008), pp. 641–649. Available online at https://www.destatis.de/DE/Publikationen/WirtschaftStatistik/Monatsausgaben/WistaAugust08.pdf?__blob=publicationFile, checked on 5/7/2013.

Böhme, Rainer (Ed.) (2013): The Economics of Information Security and Privacy. Berlin, Heidelberg, s.l.: Springer Berlin Heidelberg. Available online at http://dx.doi.org/10.1007/978-3-642-39498-0.

Bollhöfer, Esther; Jäger, Angela (2018): Wirtschaftsspionage und Konkurrenzausspähung. Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Edited by Max-Planck-Institut für ausländisches und internationales Strafrecht. Freiburg i. Br. (Reihe A: Arbeitsberichte, 09/2018).

Brandl, Stefan; Zimmermann, Mara; Grau, Nadine; Wilms, Sascha; Engler, Nils (2016): SicherheitsMonitor 2016 Mittelstand. IT-Sicherheitslage in Deutschland. Edited by DsiN e.V. DsiN e.V.

Büchner, Stefanie (2018a): Digitale Infrastrukturen. Spezifik, Relationalität und die Paradoxien von Wandel und Kontrolle. In Arbeits- und Industriesoziologische Studien (AIS) 11 (2), pp. 279–293.

Büchner, Stefanie (2018b): Zum Verhältnis von Digitalisierung und Organisation. In Zeitschrift für Soziologie 47 (5), pp. 332–348.

Bundesamt für Sicherheit in der Informationstechnik: Cyber-Sicherheits-Umfrage 2017. Edited by Bundesamt für Sicherheit in der Informationstechnik. Bonn. Available online at https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=3.

Bundesamt für Sicherheit in der Informationstechnik (2015): Die Lage der IT-Sicherheit in Deutschland. Bonn. Available online at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob=publicationFile&v=3, checked on 3/2/2016.

Bundesamt für Sicherheit in der Informationstechnik (2016): Umfrage zur Betroffenheit durch Ransomware – 04/2016. Edited by Bundesamt für Sicherheit in der Informationstechnik. Bonn. Available online at https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ransomware-umfrage-2016-04.html#download=1.

Bundesamt für Sicherheit in der Informationstechnik (Ed.) (2017): Die Lage der IT-Sicherheit in Deutschland 2017. Bonn. Available online at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf, checked on 3/26/2019.

Bundesamt für Sicherheit in der Informationstechnik (Ed.) (2019a): Cyber-Sicherheits-Umfrage. Cyber-Risiken & Schutzmaßnahmen in Unternehmen. Betrachtungszeitraum 2018. Version 1.1 vom 18.04.2019. Bonn. Available online at https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2018.pdf?__blob=publicationFile&v=9, checked on 4/24/2019.

Bundesamt für Sicherheit in der Informationstechnik (Ed.) (2019b): Cyber-Sicherheits-Umfrage. Cyber-Risiken & Schutzmaßnahmen in Unternehmen. Betrachtungszeitraum 2018. Version 1.0 vom 10.04.2019. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (2019c): Ransomware. Bedrohungslage, Prävention & Reaktion. Bonn. Available online at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf, checked on 9/2/2019.

Bundesdruckerei GmbH (2017): Digitalisierung und IT-Sicherheit in deutschen Unternehmen. Eine repräsentative Untersuchung, erstellt von der Bundesdruckerei GmbH in Zusam-menarbeit mit KANTAR EMNID. Berlin.

Bundeskriminalamt (Ed.) (2018): Cybercrime. Bundeslagebild 2017. Wiesbaden. Available online at https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.pdf, checked on 3/28/2019.

Bundesministerium für Wirtschaft und Energie (2012): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie. Edited by Bundesministerium für Wirtschaft und Energie (BMWi). Berlin.

Burr, William E.; Dodson, Donna F.; Newton, Elaine M.; Perlner, Ray A.; Polk, W. Timothy; Gupta, Sarbari; Nabbus, Ebad A. (2003): Electronic Authentication Guideline. Edited by National Institute of Standards and Technology (NIST Special Publication, 800-63-2).

Chen, Liang; Ho, Shirley S.; Lwin, May O. (2016): A meta-analysis of factors predicting cyberbullying perpetration and victimization. From the social cognitive and media effects approach. In New Media & Society, pp. 1–20.

Cisco (2017): 2017 Annual Cybersecurity Report.

Cobb, Stephen (2015): Sizing Cybercrime. Incidents and Accidents, Hints and Allegations. Virus Bulletin Conference September 2015.

Computer Security Institute (2011): 2010/2011 Computer Crime and Security Survey. New York, NY. Available online at https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf, checked on 9/18/2019.

Connolly, Lena Y.; Wall, David S. (2019): The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. In Computers & Security 87.

Dreißigacker, Arne; Riesner, Lars (2018): Private Internetnutzung und Erfahrung mit computerbezogener Kriminalität. Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015 und 2017. Edited by Kriminologisches Forschungsinstitut Niedersachsen e. V. Hannover (KFN-Forschungsbericht, 139).

Dreißigacker, Arne; Skarczinski, Bennet von; Wollinger, Gina Rosa (2020): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer repräsentativen Unternehmensbefragung 2018/2019. Ed. by Kriminologisches Forschungsinstitut Niedersachsen e. V. Hannover (KFN-Forschungsbericht, 152).

eco - Verband der Internetwirtschaft e.V. (2017): eco Studie IT-Sicherheit 2017. Available online at https://www.eco.de/wp-content/blogs.dir/eco_report_it-sicherheit-2017.pdf, checked on 3/28/2019.

Fansher, Ashley K.; Randa, Ryan (2018): Risky Social Media Behaviors and the Potential for Victimization. A Descriptive Look at College Students Victimized by Someone Met Online. In Violence and Gender.

Florencio, Dinei; Herley, Cormac (2012): Sex, Lies and Cybercrime Surveys. Edited by Microsoft Research. Redmond, WA, USA.

Gehem, Maarten; Usanov, Artur; Frinking, Erik; Rademaker, Michel (2015): Assessing Cyber Security. A Meta-Analyses of threats, trends and responses to cyber attacks. The Hague.

Georgia Institute of Technology (2016): Emerging Cyber Threats Report 2016. Edited by Georgia Institute of Technology. Atlanta, GA, USA.

Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2018): Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung Frühjahr 2018. Edited by GDV. Berlin.

Grassi, Paul A.; Fenton, James L.; Newton, Elaine M.; Perlner, Ray A.; Regenscheid, Andrew R.; Burr, William E. et al. (2017): Digital Identity Guidelines. Authentication and Lifecycle Management. Edited by National Institute of Standards and Technology (NIST Special Publication, 800-63B).

Hartmann, Josef (2017): Stichprobenziehung und Feldzugang in Organisationsstudien. In Stefan Liebig, Wenzel Matiaske, Sophie Rosenbohm (Eds.): Handbuch Empirische Organisationsforschung, vol. 4. Wiesbaden: Springer Gabler, pp. 185–211.

Henson, Billy; Reyns, Bradford W.; Fisher, Bonnie S. (2016): Cybercrime Victimization. In Carlos A. Cuevas, Callie Marie Rennison (Eds.): The Wiley Handbook on the Psychology of Violence, vol. 38. Chichester, UK: John Wiley & Sons, Ltd, pp. 553–570.

Hillebrand, Annette; Niederprüm, Antonia; Schäfer, Saskja; Thiele, Sonja; Henseler-Ungar, Iris (2017): Aktuelle Lage der IT-Sicherheit in KMU. Edited by Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK). Bad Honnef.

Hiscox (2017): The Hiscox Cyber Readiness Report 2017. Hiscox Ltd. London, UK, checked on 1/12/2018.

Hiscox (2018): Hiscox Cyber Readiness Report 2018. Hamilton, Bermuda.

Huber, Edith; Pospisil, Bettina (2018): Täter und Opfer von Cybercrime. In Edith Huber, Bettina Pospisil (Eds.): Die Cyber-Kriminellen in Wien. Eine Analyse von 2006-2016. Krems: Edition Donau-Universität Krems, pp. 23–45.

Huber, Edith; Pospisil, Bettina; Seböck, Walter (2018): Cybercrime-Delikt in Österreich - Ein Rückblick 2006 bis 2016. In Klaus Boers, Marcus Schaerff (Eds.): Kriminologische Welt in Bewegung. Mönchengladbach: Forum Verlag (Neue Kriminologische Schriftenreihe der Kriminologischen Gesellschaft e.V., 117), pp. 265–275.

IBM Cooperation (2018): IBM X-Force Threat Intelligence Index 2018. Armonk, NY, USA.

Industrie- und Handelskammer Nord e.V. (2013): Unternehmensbefragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime. Hamburg. Available online at https://www.hannover.ihk.de/fileadmin/data/Dokumente/Themen/Sicherheit/Studie_Cybercrime_Umfrageauswertung_10062013.pdf, checked on 2/2/2018.

Kantar Emnid (2019): Cyberangriffe gegen Unternehmen. Methodenreport. Nicht veröffentlicht. Bielefeld.

Kersten, Heinrich; Klett, Gerhard; Reuter, Jürgen; Schröder, Klaus-Werner (2016): IT-Sicherheitsmanagement nach der neuen ISO 27001. ISMS, Risiken, Kennziffern, Controls.

Wiesbaden: Springer Vieweg (Edition). Available online at http://dx.doi.org/10.1007/978-3-658-14694-8.

Kigerl, A. (2012): Routine Activity Theory and the Determinants of High Cybercrime Countries. In Social Science Computer Review 30 (4), pp. 470–486.

Klahr, Rebecca; Shah, N. Jayesh; Sheriffs, Paul; Rossington, Tom; Pestell, Gemma; Button, Mark; Wang, Victoria (2017): Cyber Security Breaches Survey 2017. Main Report. Edited by UK Department for Culture, Media and Sport. London, UK.

McGuire, Mike; Dowling, Samantha (2013): Cyber crime: A review of the evidence: Chapter 2: Cyber-enabled crimes - fraud and theft. Edited by Home Office (Research Report, 75).

Meier, Bernd-Dieter (2012): Sicherheit im Internet. Neue Herausforderungen für Kriminologie und Kriminalpolitik. In MschrKrim 95 (3), p. 184. Available online at 204.

Meško, Gorazd (2018): On Some Aspects of Cybercrime and Cybervictimization. In European Journal of Crime, Criminal Law and Criminal Justice 26 (3), pp. 189–199.

Min, Byungho; Varadharajan, Vijay; Tupakula, Udaya; Hitchens, Michael (2014): Antivirus security: naked during updates. In Software: Practice and Experience 44 (10), pp. 1201–1222.

Näsi, Matti; Räsänen, Pekka; Kaakinen, Markus; Keipi, Teo; Oksanen, Atte (2017): Do routine activities help predict young adults' online harassment: A multi-nation study. In Crimi-nology & Criminal Justice 17 (4), pp. 418–432.

Ngo, Fawn; K. Jaishankar (2017): Commemorating A Decade In Existence Of The International Journal Of Cyber Criminology. A Research Agenda To Advance The Scholarship On Cyber Crime. In International Journal of Cyber Criminology 11 (1).

Nurse, Jason R. C.; Creese, Sadie; Goldsmith, Michael; Lamberts, Koen (2011): Guidelines for usable cybersecurity: Past and present. Third International Workshop on Cyberspace Safety and Security (CSS). Mailand, 9/8/2011.

Organisation for Economic Co-operation and Development (2015): Digital Security Risk Management for Economic and Social Prosperity. Paris: OECD Publishing.

Osborne, Sarah; Currenti, Rosanna; Calem, Maria; Husband, Hannah (2018): Crime against businesses: findings from the 2017 Commercial Victimisation Survey. Edited by UK Home Office. UK Home Office (Statistical Bulletin 07/18).

Paoli, Letizia; Visschers, Jonas; Verstraete, Cedric (2018): The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium. In Crime, Law and Social Change 70 (4), pp. 397–420.

Pascual, Al; Marchini, Kyle (2015): 2016 Data Breach Fraud Impact Report. Edited by Javelin LLC. Available online at https://www.javelinstrategy.com/press-release/16-billion-stolen-127-million-identity-fraud-victims-2014-according-javelin-strategy, checked on 9/9/2016.

Pfeiffer, Sabine (2015): Warum reden wir eigentlich über Industrie 4.0? Auf dem Weg zum digitalen Despotismus. In Mittelweg 36 (6), pp. 14–36.

Ponemon Institute (2016): The Cyber Resilient Organization in Germany: Learning to Thri-ve against Threats. Michigan, USA.

Ponemon Institute (2017a): 2017 Cost of Data Breach Study. Global Overview. Michigan, USA.

Ponemon Institute (2017b): Cost of Cyber Crime Study. Insights on the Security Investments that make a Difference. Edited by Accenture. Michigan, USA.

Prätor, Susann (2014): Ziele und Methoden der Dunkelfeldforschung. Ein Überblick mit Schwerpunkt auf Dunkelfeldbefragungen im Bereich der Jugenddelinquenz. In Stefanie Eif-ler, Daniela Pollich (Eds.): Empirische Forschung über Kriminalität. Methodologische und methodische Grundlagen. Wiesbaden: VS Verl. für Sozialwiss. (Kriminalität und Gesellschaft), pp. 31–65.

PricewaterhouseCoopers AG WPG (2017): Im Visier der Cyber-Gangster - So gefährdet ist die Informationssicherheit im deutschen Mittelstand. With assistance of Philipp Engemann, Derk Fischer, Björn Gosdzik, Tobias Koller, Nial Moore. Available online at https://www.pwc-wissen.de/pwc/de/shop/publikationen/Im+Visier+der+Cyber-Gangster/?card=21564, checked on 1/12/2018.

PricewaterhouseCoopers Network (2018): Revitalizing privacy and trust in a data-driven world. Key findings from The Global State of Information Security Survey 2018.

Prüfer, Peter; Rexroth, Margrit (2005): Kognitive Interviews. Mannheim (ZUMA How-to, 15).

PwC Strategy& GmbH (2016): Cybersicherheitsstrategie. Ergebnisse der Online-Erhebung. Edited by Bundesministerium des Innern. Available online at https://www.ihk-nuernberg.de/de/media/PDF/Innovation-Umwelt/informationssicherheit/newsletter/cybersicherheitsstrategie-ergebnisse-der-online-erhebung-05-2016.pdf, checked on 3/28/2019.

Rantala, Ramona (2008): Cybercrime against Businesses, 2005. Edited by U.S. Department of Justice. U.S. Department of Justice. Washington DC, USA (Bureau of Justice Statistics, Special Report).

Romanosky, Sasha (2016): Examining the costs and causes of cyber incidents. In Journal of Cybersecurity 2 (2), 121-135.

Ryan, Julie J.; Jefferson, Theresa I. (2003): The Use, Misuse, and Abuse of Statistics in Information Security Research. In Proceedings of the 23rd ASEM National Conference.

Sasse, Martina Angela; Brostoff, Sacha; Weirich, Dirk (2001): Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. In BT Technology Journal 19 (3), pp. 122–131.

Schäfer, Michael (2018): Daseinsvorsorge. In : Gabler Wirtschaftslexikon. Wiesbaden: Springer Gabler. Available online at https://wirtschaftslexikon.gabler.de/definition/daseinsvorsorge-28469/version-252099, checked on 4/1/2019.

Schnell, Rainer; Noack, Marcel (2015): Stichproben, Nonresponse und Gewichtung für Viktimisierungsstudien. In Nathalie Guzy, Christoph Birkel, Robert Mischkowitz (Eds.): Vikti-misierungsbefragungen in Deutschland. Methodik und Methodologie. Wiesbaden: Bundes-kriminalamt (Polizei + Forschung, 47.2), pp. 8–75.

Smith, Paul (2013): Sampling and Estimation for Business Surveys. In Ger Snijkers, Diane Willimack, Gustav Haraldsen, Jacqui Jones (Eds.): Designing and Conducting Business Surveys. s.l.: Wiley, pp. 165–218.

Snijkers, Ger; Meyermann, Alexia (2017): Betriebs- und Unternehmenssurveys. Der Surveyprozess und Surveyqualität. In Stefan Liebig, Wenzel Matiaske, Sophie Rosenbohm (Eds.): Handbuch Empirische Organisationsforschung. Wiesbaden: Springer Fachmedien Wiesbaden, pp. 241–272.

Statistisches Bundesamt (Destatis) (2008): Klassifikation der Wirtschaftszweige (WZ 2008). Mit Erläuderungen. Wiesbaden. Available online at https://www.klassifikationsserver.de/klassService/jsp/variant/downloadpdf?variant=wz2008&language=DE, checked on 4/24/2019.

Statistisches Bundesamt (Destatis) (2018): Unternehmensregister-System. Qualitätsbericht 2017. Wiesbaden. Available online at https://www.destatis.de/DE/Methoden/Qualitaet/Qualitaetsberichte/Unternehmen/unternehmensregister.pdf, checked on 7/30/2019.

Statistisches Bundesamt (Destatis) (2019a): Unternehmen und Arbeitsstätten. Gewerbean-zeigen. Mai 2019. Wiesbaden (Fachserie 2 Reihe 5).

Statistisches Bundesamt (Destatis) (2019b): Unternehmen und Arbeitsstätten. Insolvenzverfahren. Mai 2019. Wiesbaden (Fachserie 2 Reihe 4.1).

Stiller, Anja; Boll, Lukas; Kretschmer, Saskia; Wollinger, Gina Rosa; Dreißigacker, Arne (2020): Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer qualitativen

Interviewstudie mit Experten. Edited by Kriminologisches Forschungsinstitut Niedersachsen e. V. Hannover (KFN-Forschungsbericht Nr. 155). Available online at: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_155.pdf, checked on 7/24/2020.

Sukwong, Orathai; Kim, Hyong; Hoe, James (2011): Commercial Antivirus Software Effectiveness: An Empirical Study. In Computer 44 (3), pp. 63–70.

techconsult (2017): IT- und Informationssicherheit: Technische Maßnahmen und Lösungen in Mittelstand und öffentlichen Verwaltungen. Studienbericht zur Security Bilanz Deutschland 2017. Kassel, Haar.

Tsitsika, Artemis; Janikian, Mari; Wójcik, Szymon; Makaruk, Katarzyna; Tzavela, Eleni; Tzavara, Chara et al. (2015): Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries. In Computers in Human Behavior 51, pp. 1–7.

van de Weijer, Steve G.A.; Leukfeldt, Rutger; Bernasco, Wim (2019): Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. In European Journal of Criminology 16 (4), pp. 486–508.

Vanson Bourne (2014): Protecting the organization against the unknown. A new generation of threats. Edited by Vanson Bourne, Dell Inc.

Verband der TÜV e.V. (Ed.) (2019): Cybersecurity Studie. Berlin. Available online at https://www.vdtuev.de/dok_view?oid=769635.

Verizon (2018): 2018 Data Breach Investigations Report (11).

Wegge, Denis; Vandebosch, Heidi; Eggermont, Steven; van Rossem, Ronan; Walrave, Michel (2016): Divergent Perspectives. Exploring a Multiple Informant Approach to Cyber-bullying Victimization and Perpetration. In European Journal on Criminal Policy and Re-search 22 (2), pp. 235–251.

Willis, Gordon B. (2005): Cognitive interviewing. A tool for improving questionnaire design. Thousand Oaks: SAGE.

AUTHORS

Arne Dreißigacker studied at the Berlin University of Applied Sciences for Administration and Justice and worked for the Berlin police between 2001 and 2004. He then studied sociology at the Martin Luther University of Halle (Saale), and in 2013 he received a doctoral scholarship at the Criminological Research Institute of Lower Saxony (KFN) and has been a research assistant there since 2015. His research focuses on the officially non-registered crimes, domestic burglary, prejudice crime and cybercrime. Since October 2018, he has led the research project Cyber-attacks against companies at KFN.

Bennet von Skarczinski studied business administration at the Hanover University of Applied Sciences and Arts and has been working for PricewaterhouseCoopers (PwC) in the area of finance, cyber security & privacy since 2015. Since December 2017, he has also been an associate staff member at the Criminological Research Institute of Lower Saxony (KFN) in the project Cyber-attacks against Companies. Moreover, he is a PhD student at the Chair of Accounting and Information Systems at the University of Osnabrück. His main focus is on the management of information security in companies and cyber-economics.

Prof. Dr. Gina Rosa Wollinger studied sociology in Leipzig and received her doctorate in 2018 from the Faculty of Social Sciences and Philosophy there. Between 2012 and 2018 she worked at the Criminological Research Institute of Lower Saxony (KFN) and since December 2017 she has been in charge of the research project Cyber-attacks against companies, which she initiated, before she took up a professorship for sociology and criminology at the University of Police and Public Administration NRW in October 2018. Her research focuses on domestic burglary, cybercrime and victimology.

ISBN: 978-3-948647-06-3