The Geneva Papers on Risk and Insurance - Issues and Practice (2020) 45:657–689
https://doi.org/10.1057/s41288-020-00183-6

Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market

Dirk Wrede[1] · Tino Stegen[1] · Johann-Matthias Graf von der Schulenburg[1]

Received: 7 September 2019 / Accepted: 20 July 2020 / Published online: 7 September 2020

Abstract

This paper examines the design of affirmative and silent coverage in view of the cyber risks in traditional insurance policies for select product lines on the German market. Given the novelty and complexity of the topic and the insufficient coverage in the literature, we use two different sources. We analysed the general insurance terms and conditions of different traditional insurance lines using Mayring's qualitative content analysis. Also, we conducted interviews with experts from the German insurance industry to evaluate how insurers understand their silent cyber exposures, and what measures they take to deal with this new exposure. The study shows a considerable cyber liability risk potential for insurers in the considered insurance lines. This arises from the affirmative as well as silent cover inclusions and exclusions for cyber risks, which result from imprecise wordings of insurance clauses and insufficient descriptions of the contractually specified scope of the insurance coverage.

Keywords Cyber insurance · Traditional insurance policies · Cyber risk · Silent cyber coverage · Affirmative cyber coverage · Silent cyber

Open access funding provided by Projekt DEAL.

Electronic supplementary material The online version of this article (https://doi.org/10.1057/s41288-020-00183-6) contains supplementary material, which is available to authorized users.

✉ Dirk Wrede
dw@ivbl.uni-hannover.de

Tino Stegen
tino.stegen@hotmail.de

Johann-Matthias Graf von der Schulenburg
jms@ivbl.uni-hannover.de

[1] Gottfried Wilhelm Leibniz Universität Hannover, Institute for Risk and Insurance, Otto-Brenner-Straße 7, 30159 Hanover, Germany

Introduction

Cyber risks (e.g. cybercrime, IT failure/outage, data breaches, fines and penalties) are among the most critical business risks for companies worldwide in the 21st century (Allianz Global Corporate & Specialty (AGCS) 2020; World Economic Forum 2020). As a peril, cyber risk can be defined as 'any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure breakdown, and physical damage to humans and property' (Eling and Schnell 2016a, b). Generally, data protection-related breaches of obligations and confidentiality, business interruptions and data theft can result in financial damage and reputation losses (Cavusoglu et al. 2004; Smith 2004; Salmela 2008; Bulgurcu et al. 2010; Järveläinen 2013). Over the past two years, for example, cyberattacks caused total losses for companies in Germany of around EUR 205.7 billion (Bitkom 2020). [1]

In this context, insurance solutions are particularly useful for transferring risks from cyber threats to companies (Innerhofer-Oberperfler and Breu 2010; Tosh et al. 2017; Tonn et al. 2019). Three different general categories of cyber coverage are available on the insurance market: (1) stand-alone policies, (2) coverage in an insurance bundle and (3) silent cyber coverage (Coburn et al. 2016; OECD 2017b; EIOPA 2018a). The emergence of possibly overlapping coverage makes it complicated for insurers to design new products. On the one hand, integrating cyber coverage into traditional products creates complexity and opacity (Haas and Hofmann 2014; Siegel et al. 2018); on the other hand, current cyber coverage often contains imprecise insurance terms and conditions and insufficient descriptions of the contractually agreed scope (Baer 2003; Meland et al. 2015, 2017; Marotta et al. 2015, 2017). The terms and conditions of some policies also entirely lack any relevant information for cyber damages (Ruffle et al. 2015). Yet, the wording of the insurance terms and conditions, and descriptions of the contractually agreed scope, largely determine the structure of cyber coverage (Woods and Simpson 2017).

While new insurance products specifically include or exclude cyber risks, it is often unclear whether and to what extent existing policies cover them (Kirkpatrick 2015; Eling 2018; Siegel et al. 2018; Woods and Moore 2020). This unintended, implicit coinsurance leads to so-called 'silent cyber risks' of traditional insurance policies (Woods and Simpson 2017; EIOPA 2019). Silent cyber risks are defined as cyber risks that arise 'from implicit cyber exposure within 'all risks' and other liability insurance policies that do not explicitly exclude cyber risks' (Bank of England Prudential Regulation Authority (PRA) 2016).

Therefore, insurers face the challenge of identifying silent cyber risks in the various traditional insurance policies, in which cyber risks are regularly not mentioned or are not explicitly included or excluded. Similarly, in traditional insurance products, cyber risks are often defined, but their subsequent handling is not clear. This

[1] For the causes and costs of cyberattacks, see, for example, Romanosky (2016). On the problem of estimating the economic costs of cybercrime, see Anderson et al. (2013, 2019) and Hyman (2013).

makes it necessary to systematically identify, analyse and comprehensively quantify the existing but hitherto unknown cyber exposure. The aim is to take the individual components of existing silent cyber risks into account in the underwriting process. A detailed assessment of the existing silent cyber risks may entail uncalculated and difficult-to-quantify claim burdens for insurers (Willis Re 2017, 2018, 2019). At the same time, a holistic risk assessment should be carried out to reduce uncertainties by considering the existing accumulation aspects and developing adequate pricing approaches. As a result, insurers could include affirmative and comprehensive cyber coverage in their traditional insurance products. The topic of silent cyber exposure is also gaining the attention of insurance supervisory authorities (Pain and Anchen 2017; Eling 2018; Siegel et al. 2018). [2]

Even though the significance of affirmative and silent cyber coverage in traditional insurance products as well as the resulting exposures have been acknowledged in practice and research, only a few studies examine the design of cyber coverage components in traditional insurance products. The present study contributes to closing this research gap. It aims to systematically analyse the general terms and conditions of policies in selected insurance lines on the German market with regard to affirmative and silent coverage, thereby identify existing silent cyber risks. Expert interviews are also evaluated to deduct how the insurance industry is currently dealing with the topic.

The remainder of the article is structured as follows: at first a literature overview presents the general development of the cyber insurance market. In the process special attention will be paid to the supply and demand side. Subsequently, the state of research on the design of cyber coverage in insurance products and the legal background for the German jurisdiction from a theoretical perspective are presented. The third section focuses on the methods used and describes research design, data collection and evaluation procedures. The consecutive part presents the results of the content analysis of the insurance terms and conditions as well as the conducted interviews. The second-to-last section discusses and reflects on the results. To conclude, summarising remarks are made.

[2] International financial supervisory authorities are increasingly warning of considerable silent cyber risks in the portfolios of insurance companies. In the U.K., for example, the Bank of England Prudential Regulation Authority (PRA) called on the insurance industry in 2017 to address the problem of cyber risks in traditional insurance products and imposed specific requirements for managing silent cyber risks (see Bank of England Prudential Regulation Authority (PRA) 2017) and asked reinsurers and primary insurers to develop a silent cyber action plan by the middle of 2019. In Germany, the Federal Financial Supervisory Authority (BaFin) has also been increasingly concerned with this issue since 2019 and is now questioning insurers on their silent cyber risks. This includes collecting information from insurers on the number of insurance contracts containing silent cyber risks and how to address this issue in the context of a company's own risk and solvency assessment (ORSA). Similarly, the European Insurance and Occupational Pensions Authority (EIOPA) has taken silent cyber risks into account when developing its strategy on cyber underwriting. It has also started a number of initiatives and is emphasising its supervisory concerns, specifically in the area of silent/non-affirmative risks (see EIOPA 2020).

Literature review and theoretical background

Relationship between cyber insurance markets and the supply and demand of cyber risk insurance coverage

Nowadays, companies are facing a variety of internal and external cyber threats—cyber crime, hacktivism, cyber espionage and cyber war—and are affected by different forms of cyberattacks, such as denial of service, web-based attacks, malicious codes, viruses, worms and trojans, malware, malicious insiders, stolen devices as well as phishing and social engineering (Bendovschi 2015). The possible consequences of cyberattacks include theft, loss and destruction of data and information (Andrijcic and Horowitz 2006; McLaughlin 2011; Jouini et al. 2014; Amin 2019); failure and destruction of IT systems and software (Furnell and Warren 1999; McLaughlin 2011; Lagazio et al. 2014; Jouini et al. 2014; Romanosky 2016); business interruption (Andrijcic and Horowitz 2006; Bendovschi 2015; Amin 2019); disruption and destruction of production facilities (Lathrop and Stanisz 2016; Wu and Moon 2017; Elhabashy et al. 2019); disruption of production and business processes and procedures (Hiller and Russell 2013; Lathrop and Stanisz 2016; Pereira et al. 2017; Kiss et al. 2019); and personal injury and property damage (Zelle and Whitehead 2014). Accordingly, cyberattacks cannot only result in considerable financial losses (Gandhi et al. 2011; Jouini et al. 2014) but also physical damage (Lathrop and Stanisz 2016; Amin 2019). However, the insurance coverage of existing cyber policies is primarily limited to financial losses resulting from cyberattacks (Böhme and Schwartz 2010; Haas and Hofmann 2014). Since cyber policies generally do not provide insurance coverage for physical damages and personal injuries resulting from cyberattacks (Lathrop and Stanisz 2016; Franke 2017), the different consequences of cyber incidents may also affect the insurance coverage from various traditional insurance policies, thus resulting in silent cyber coverage, unless the policies include coverage exclusions.

Cyber insurance coverage has been available since the late 1970s. The market evolved from the technical risks/technical errors and omissions (E&O) sector. The 1980s saw the introduction of the first tech E&O insurance policies, which included cybersecurity insurance and were developed primarily for financial institutions as well as blue chip companies. The development and launch of cyber insurance as a stand-alone product was a response to the Y2K problem and was intended to close existing gaps in the insurance coverage of traditional property and casualty policies (Majuca et al. 2006; Camillo 2017).

Accordingly, cyber insurance is a comparatively new product (KPMG AG Wirtschaftsprüfungsgesellschaft 2017a; DiGrazia 2018) offering considerable growth potential in the German market (KPMG AG Wirtschaftsprüfungsgesellschaft 2017b; Wrede et al. 2018). With a total of 528 insurance companies and a premium volume of approximately EUR 202.4 billion in 2018, Germany is Europe's third-largest and the world's sixth-largest insurance market. In Europe, Germany, together with the U.K., is the leader in the area of non-life insurance,

among other things due to the comparatively great importance of industry and medium-sized commercial enterprises and the correspondingly high demand. In 2018, for example, the premium volume of the 120 German insurers in the industry/commercial/agricultural property insurance segment amounted to approximately EUR 6.9 billion. The 99 providers of engineering insurance had a premium volume of about EUR 2 billion, while the 42 companies in the credit, surety and fidelity insurance segment reached approximately EUR 1.7 billion (German Insurance Association (GDV) 2019).

In Germany, about 40 insurers and reinsurers offer cyber policies for business customers (Flagmeier and Heidemann 2018). In 2017, the premium volume amounted to approximately EUR 100 million (KPMG AG Wirtschaftsprüfungsgesellschaft 2017b). In 2018, about 33% of all companies in Germany had cyber coverage (Hiscox Ltd. 2018). Currently, the range of coverage for cyber risks in the cyber insurance market is highly segmented and primarily consists of a combination of traditional insurance products and independent cyber policies (Knutsen and Stempel 2018). Nonetheless, the cyber insurance market is still underdeveloped and underutilised (Anderson and Moore 2006; Zhao et al. 2013; Talesh 2018). However, the cyber insurance business is still relatively unattractive for providers, as highly IT-dependent companies mainly drive the demand for the corresponding insurance products and the market segment is still relatively limited (Bandyopadhyay et al. 2009).

As a result of the significant increase in provider-specific insurance coverage for cyber risks, the cyber insurance business is experiencing more substantial market growth and higher competition among companies (Kesan and Hayes 2017). The relevant literature includes several studies dealing with the investigation of cyber insurance markets in different countries (ENISA 2012; Choudhry 2014; Baban et al. 2017a, b; Franke 2017; Strupczewski 2017; Eling and Zhu 2018; Flagmeier and Heidemann 2018; Bahşi et al. 2019; Cole and Fier 2020). For example, Eling and Zhu (2018) investigate the supply of cyber insurance by property and casualty insurers in the U.S. market. The market for cyber insurance products in Sweden is analysed by Franke (2017). By contrast, Baban et al. (2017a) focus on the analysis of globally important cyber insurance markets in Germany, Switzerland, the U.S. and the U.K., while Koezuka (2016) examines the design of cyber insurance products in the Japanese market. Additional studies on the supply of insurance coverage for cyber risks in the Polish (Strupczewski 2017), Norwegian (Bahşi et al. 2019) and German (Choudhry 2014; Baban et al. 2017b; Flagmeier and Heidemann 2018) markets are available.

For individual cyber insurance markets, major market barriers for the supply and demand of cyber policies are discussed (ENISA 2012; Baban et al. 2017a, b). Information asymmetries and the global, interdependent and highly correlated damage potential of cyber risks are frequently cited as important market barriers for the provision of cyber insurance (Baer and Parkinson 2007; Moore 2010; ENISA 2012; Young et al. 2016; Baban et al. 2017a, b; OECD 2017a; Bodin et al. 2018). Furthermore, insufficient reinsurance capacity for the cyber insurance business is identified in the literature as an obstacle on the supply side. This is caused by difficulties in quantifying the possible accumulation of cyber risks

(ENISA 2012; OECD 2017a). Lack of experience in claims settlement and a lack of historical data on the frequency and severity of cyber incidents also constitute significant challenges to the provision of cyber insurance products (Baban et al. 2017a, b; Strupczewski 2017; EIOPA 2018b; Siegel et al. 2018). As a result, insurers are fundamentally uncertain as to whether, in the long term, the provision of cyber coverage is considered advantageous for individual companies or too risky (Baban et al. 2017a, b). Actuarially unclear data on the frequency and amount of cyber losses pose additional problems in calculating adequate premiums for cyber coverage. Furthermore, the high adaptability and dynamics of cyber threats are important growth-inhibiting factors for the cyber insurance market (Zhao et al. 2013). Shetty et al. (2018) emphasise that, in the long term, insurers will be able to satisfy the corporate demand for cyber coverage only if the difficulties mentioned above are overcome.

According to Tøndel et al. (2015), the factors influencing cyber insurance demand have hardly been investigated to date. Further, when analysing corporate demand for cyber coverage, Bandyopadhyay et al. (2009) emphasise the limited importance of insurance solutions for companies in IT risk management. In principle, the complexity and lack of transparency of the cyber insurance market has a restraining effect on the demand for cyber policies (Baban et al. 2017a, b). From the customer's perspective, the relatively high insurance premiums for cyber coverage (EIOPA 2018b) and the lack of consideration of individual company needs in the design of insurance coverage (OECD 2017a; EIOPA 2018b) also represent notable barriers to the demand for cyber policies. In this context, Franke and Meland (2019) examine the discrepancies between the cyber coverages offered by insurers and customer expectations.

Furthermore, the literature describes the information deficit associated with the offered cyber insurance products and their scope of coverage (ENISA 2012, 2016; Baban et al. 2017a, b; Meland et al. 2017; EIOPA 2018b; Siegel et al. 2018) as well as the inadequate perception of cyber risks as the most important obstacles on the demand side (Moore 2010; Baban et al. 2017a, b; De Smidt and Botzen 2018; Eling 2018). De Smidt and Botzen (2018) designate it a "not in my organisation effect". Additionally, companies do not recognise the need to purchase cyber insurance, as decision makers often assume that existing traditional insurance policies already provide comprehensive coverage against cyber risks (Beh 2001; Willis 2010; ENISA 2012; U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) 2012; Her Majesty's (HM) Government (UK) and Marsh Ltd. 2015; Marotta et al. 2015, 2017; OECD 2017a; Strupczewski 2017; Bodin et al. 2018; Knutsen and Stempel 2018; Schanz 2018). This cannot only be attributed to the lack of transparency and comprehensibility of insurance terms and conditions and the contractually agreed service content of cyber policies (Baer 2003; Meland et al. 2015; Marotta et al. 2015, 2017) but also to the high degree of complexity of insurance products (Eling and Wirfs 2016; Strupczewski 2017). Therefore, it is difficult for insured companies to assess existing insurance coverage (Middleton and Kazamia 2016). Also, insurance products often do not provide sufficient coverage for companies in the event of a claim (Siegel et al. 2002; Gordon et al. 2003; Toregas and Zahn 2014).

The lack of demand for cyber coverage also results from companies' lack of knowledge about the availability of cyber policies (Pain et al. 2016), since most companies that have already been affected by a cyber incident generally decide to purchase cyber insurance (Shackelford 2012). In this context, Meland et al. (2017) analyse the uncertainty on the company side in dealing with novel cyber insurance. Accordingly, many companies often prefer to enhance existing insurance products with cyber coverage components rather than purchase independent cyber policies (Middleton and Kazamia 2016). Therefore, several authors point out the lack of understanding on both the supply and demand side as one of the most significant market barriers (Biener et al. 2015; EIOPA 2018b). In summary, according to Eling and Schnell (2016a, b) and Tøndel et al. (2015), more empirical research seems necessary to examine the supply and demand sides.

Potential insurance coverage for cyber risks in traditional policies

There are only a few studies on systematic content analysis of the coverage and contractual conditions of insurance solutions for cyber risks. In this context, the immaturity of the products currently on the market is increasingly criticised (Bandyopadhyay and Shidore 2011; Meland et al. 2015, 2017; Tøndel et al. 2016; DiGrazia 2018). For example, Kesan et al. (2005) analyse the scope of coverage for cyber policies in general, whereas Majuca et al. (2006) examine the changes and adjustments in insurance coverage as the hacker insurance from the early 1990s evolved into the first independent cyber policies in the mid-2000s. Further, Baer and Parkinson (2007) show that the stand-alone cyber insurance policies of all leading insurance companies covered losses due to business interruption at that time. Marotta et al. (2015, 2017) analyse the insurance coverage of 14 cyber policies of internationally active insurers, showing that first-party coverage generally includes loss or damage to digital assets, business interruption losses, cyber extortion and theft of money and digital assets. However, third-party coverage generally includes the assumption of costs for information security and privacy breaches, IT forensics, as well as customer notifications and reporting obligations for privacy incidents, multimedia liability, loss of third-party data and third-party contractual indemnification.

Coburn et al. (2016) examine the coverage and product components of 26 cyber insurances from the U.K. insurance market. Talesh (2018) analyses the range of risk management services offered by over 30 cyber insurance products. Meanwhile, Woods et al. (2017) focus on the evaluation of content and structural design of application documents for cyber insurance, which serve for the collection and documentation of information on existing IT security measures in the companies. Franke (2018) examines the coverage of five cyber insurances and the business conditions of three electronic payment service providers regarding the coverage of defaults in electronic payment services. Romanosky et al. (2019) evaluate the content of the coverage of over 100 cyber policies in the U.S. insurance market to gain insight into the underwriting process and an insurance-specific understanding of cyber risks and their pricing. A first systematic analysis of cyber coverage in traditional insurance products was conducted by Haas (2016). However, this study is limited to the

examination of standard terms and conditions from the German Insurance Association (GDV) for business liability, electronics, property, business interruption, data and software insurance.

In the legal literature, a few publications deal with the design of cyber coverage components in traditional insurance products. Hunt (2019), for example, discusses the incorporation of cyber coverage components in all-risk property, commercial general liability, commercial crime, terrorism and directors' & officers' (D&O) insurance for the commercial real estate sector from a theoretical perspective and with respect to the U.S. insurance market. Jerry II and Mekel (2001) describe coverage for cyber risks in selected traditional insurances (commercial general liability coverage, D&O coverage, E&O coverage, media coverage, as well as intellectual property infringement, prosecution and defence coverage).

Theoretical perspective on the jurisdiction regarding the coverage of silent cyber damages in Germany

The problem of the lack of transparency when it comes to interpreting the insurance terms and conditions of traditional policies with regard to the effectiveness and interpretation of the risk inclusions or exclusions of silent cyber damages appears to be relevant for the German jurisprudence. International jurisdiction already deals with this question, as is shown, for example, by the court proceedings pending in the U.S. to clarify the effectiveness of the war exclusion clause in the Mondelez v. Zurich case. The corresponding statement of claim for USD 100 million was filed in October 2018 with the Circuit Court of Cook County, Illinois. The company Mondelez International Inc. (Mondelez) had taken out an all-risk property insurance policy from Zurich American Insurance Company (Zurich) that included coverage for physical loss or damage to electronic data, programmes or software and also physical loss or damage caused by the malicious introduction of a machine code or instruction. In June 2017, Mondelez fell victim to an attack by the malware program 'NotPetya'. As a result, 1700 servers and 24,000 laptops at Mondelez were permanently damaged and had to be replaced. According to Mondelez, this caused damages of well over USD 100 million for the company. This loss was reported to Zurich by the company. In June 2018, Zurich refused to cover Mondelez, citing the insurance policy's war exclusion clause. To date, it appears that no final decision has been made in this lawsuit (Ferland 2019).

German insurers have so far only reported isolated cases of silent cyber damage.[3] For this reason, to the best of our knowledge, there have not yet been any legal proceedings in Germany to clarify silent cyber claims. From a theoretical perspective, in the case of legal proceedings in Germany, the courts would generally take into account different interpretative principles when trying to interpret risk inclusion and exclusion clauses with ambiguous wording.

[3] For example, in 2019, in a survey of 27 insurers by the German Federal Financial Supervisory Authority (BaFin) to examine non-affirmative cyber risks in insurance policies, only two insurance companies reported known silent cyber losses in Germany (see Grund 2020).

Thus, the requirement of comprehensibility developed by the German jurisdiction, which prescribes taking into account the policyholder's interests when interpreting clauses, should apply. This should lead to assuming a broad interpretation of the regulations by the policyholders. They would interpret the inclusions rather generously since their interest is in the most widespread coverage possible. Theoretically, in case of doubt, this means that insurance coverage exists for all risks unless they are explicitly excluded.

Furthermore, the general terms and conditions used by insurance companies are subject to the law on general terms and conditions of business. According to this, clauses contradict the transparency requirement developed by the German jurisdiction and are therefore invalid if they are not clearly formulated and understandable. If there is any ambiguity in general insurance terms and conditions and, as a result, different alternatives for the application of the clause remain despite their interpretation, this ambiguity is usually at the expense of the insurer and the most favourable interpretation of the clause for the policyholder is then applicable. Ambiguity is typically assumed, e.g. in the own-damage clause common in D&O insurance policies or for the term damage event in general liability insurance (Pilz 2006).

Conversely, the principle of a narrow interpretation of risk exclusions in general insurance terms and conditions generally applies in order to protect the policyholder, so that insurance coverage is not reduced further than the apparent purpose of the clause requires. Theoretically, this results in the fact that, for silent cyber risks, the existing uncertainties regarding the scope of insurance coverage in traditional policies mean that the interpretation of risk inclusion and exclusion, as well as the definition of loss events from a legal perspective, increasingly need to be clarified in court proceedings. This serves the purpose of creating legal certainty for insurers and policyholders.

In summary, the lack of transparency in and the complexity of insurance terms and conditions and the content of cyber insurance policies, combined with the resulting insecurity of companies towards cyber coverage, are among the main reasons for the lack of corporate demand for cyber insurance. Moreover, there is hitherto no systematic analysis in the literature on affirmative and silent cyber coverage and the resulting silent cyber risks associated with traditional insurance products. To the best of our knowledge, this is the first empirical study that examines traditional corporate insurance products in the German insurance market for affirmative and silent cyber coverage.

Research design and data

Research context and methods

Due to the lack of context-specific research on the design of coverage for cyber risks in traditional insurance policies, as well as the explorative nature of our research objective, a qualitative research approach is used. Data are collected using two methods: (1) qualitative content analysis to examine general insurance terms and

conditions of different traditional product lines in the German market and (2) qualitative interviews with experts from the German insurance industry.

Data collection and analysis

Qualitative content analysis of general insurance terms and conditions

Methodologically, this study is based on a systematic evaluation of text documents (Miller and Alvarado 2005; Bowen 2009). The development of a scheme of categories based on the research objectives (Cavanagh 1997; Harwood and Garry 2003; Graneheim and Lundman 2004) and the coding of the text material using this differentiated scheme of categories (Weber 1990; Elo and Kyngäs 2008; Vaismoradi et al. 2013) is characteristic for qualitative content analysis. A content analysis of general insurance terms and conditions of select traditional product lines is carried out to examine insurance coverage for cyber risks. The general terms and conditions of insurance products represent a suitable data basis for the investigation because, on the one hand, they serve to describe the scope of the service and determine the insurance coverage. Thus, they provide the customer with the actual contractual contents of the policy. On the other hand, the comprehensibility of the contractual conditions and the contents are of central importance for customers' purchasing decisions regarding insurance contracts (Mainelli 2012). Here, currently effective versions of general insurance terms and conditions of the selected insurance products are considered so that the research results are up-to-date.

The evaluation is carried out following Mayring's model of qualitative content analysis, which enables a rule-based and systematic evaluation of the data (Mayring 2015). Qualitative data analysis software MAXQDA is used to facilitate and systematically structure the coding process. Due to the nature of the available text material, a pragmatic and appropriate combination of the two analysis techniques *inductive category formation* and *classifying structuring* was carried out (Mayring 2015).

Since the categories are derived directly from the text material to be analysed (Hsieh and Shannon 2005), the method is particularly suitable for investigating practical phenomena as well as problems for which theories and literature are only available to a limited extent. Accordingly, the qualitative content analysis follows an inductive procedure for the formation of categories, meaning that individual categories are derived directly from the material without reference to existing theoretical concepts (Kondracki et al. 2002; Thomas 2006; Finfgeld-Connett 2014). This approach aims directly at drawing conclusions to answer the research objective and is employed on a small sample of texts. The complexity of the qualitative data material will be stepwise and manually reduced by coding the documents (Potter and Levine-Donnerstein 1999). The data to be analysed are checked for relevant text segments, which are marked and given 'text-related' codes that describe the segment as precisely as possible (Gioia et al. 2013). The resulting scheme of primarily descriptive codes is structured and transferred into categories. This is done by checking the existing descriptive codes for their analytical content and combining those with similar meanings to create analytical categories. To those, further codes are assigned as

subcategories (Morse 2008; Graneheim et al. 2017). This content analytical scheme of categories forms the basis for the subsequent qualitative analysis.

Additionally, coding rules are formulated to ensure the text material is clearly assigned to categories. The rules are tested, adjusted and, if necessary, clarified and adapted. This would be based on parallel data analyses and frequent comparisons of the codings (Downe-Wamboldt 1992; Burla et al. 2008).

The entire text material was at first read several times to code it in successive steps, each increasing the level of abstraction, with a focus on the relevant text segments (Gioia et al. 2013). Based on the inductive category formation, a preliminary coding scheme is developed from the material through several iterations. It defines the aspects relevant to the analysis. As relevant coding units, individual cover components—hazard, damage and costs—and claims exclusions are defined. The context unit is a business insurance line and the evaluation unit consists of all general insurance terms and conditions of a single insurance line. A double-blind procedure, with two researchers developing the codes independently, is applied to guarantee coding quality (Guest et al. 2006). A complete test coding of parts of the text was carried out by the two researchers using the developed coding scheme to ensure a common understanding of the codes and their application. The researchers subsequently met to review the material as well as clarify and finalise the codes and categories.

Further, a description including a brief explanation of the code's meaning and its intended use was developed. The research team, including the two coders, discussed this preliminary coding scheme. In the process, the authors agreed on its further development based on a comparison of the created codings. Particular attention was paid to the stability of the developed codes and the structural design of the coding scheme (Hennink et al. 2017).

The analysed text material was evaluated with regard to information security violations. If a text segment met this selection criterion, a new category was created for it, or it was assigned to an existing one. The definition of the different characteristics of the categories by typification took place only after a complete passage of the material and the completion of the scheme. This was necessary to determine the maximum possible scope for each category and insurance line, as well as to create subcategories on this basis to ensure that the different characteristics of the individual categories are well defined. The final category scheme contains a total of 38 categories; 20 of them are main categories (see Fig. 1).

Subsequently, the coding of the remaining material was carried out independently by two researchers based on the final scheme, whereby uniform coding was ensured by regular coordination meetings and further checks of the scheme.

Sample and data

The database used comprises a total of 48 general terms and conditions from various traditional insurance lines. This study focuses on insurers operating in the German market with insurance lines serving corporate customers and falling under the jurisdiction of the respective primary Financial Supervisory Authority of a DACH region country (Germany, Austria or Switzerland). These are the Federal Financial Supervisory Authority (BaFin), the Austrian Financial

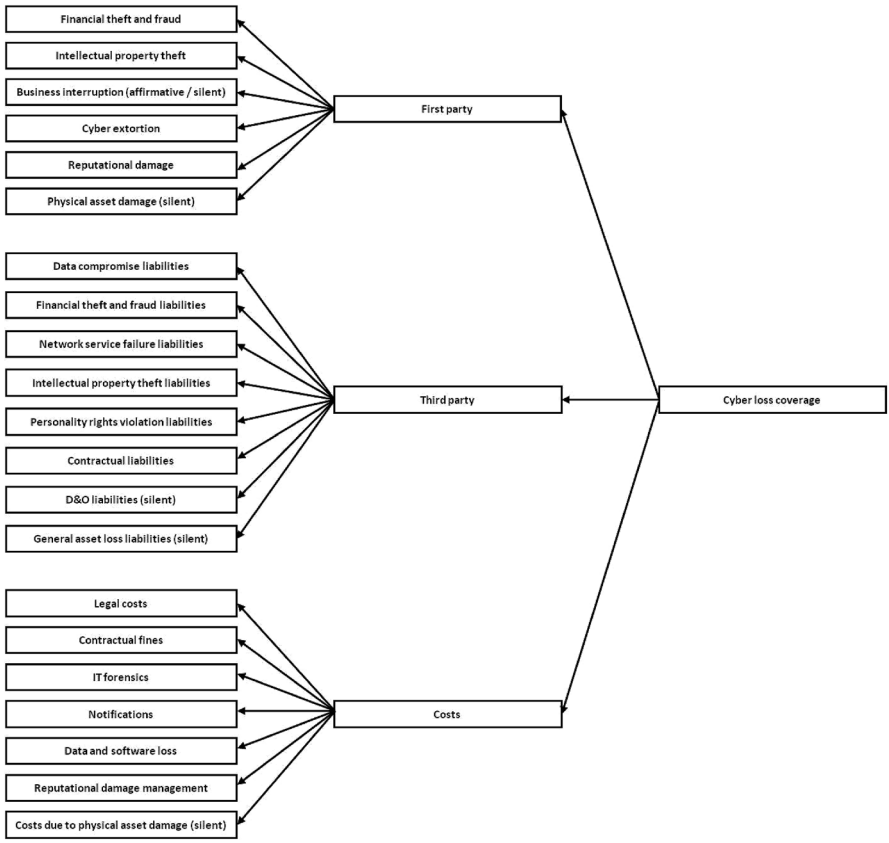

Fig. 1 Scheme of categories

Market Authority (FMA) and the Swiss Financial Market Supervisory Authority (FINMA). The examined product lines are business content and income, business and professional liability, pecuniary loss liability, fidelity insurance and D&O insurance. These lines are typically associated with extensive cyber coverage in the literature (Cohen and Anderson 2000; Jerry II and Mekel 2001; ENISA 2012; Flagmeier and Heidemann 2018; Armbrüster 2020; Gebert and Klapper 2020) and they contain, according to practitioners' opinion, significant silent cyber risks (Willis Towers Watson 2019). [4] The sample is the result of the multi-stage selection process described in Fig. 2. It is based on the flow chart according to the

[4] To the best of our knowledge, the German insurance market has so far only seen isolated cases of silent cyber damages, and until now there are no known cases of legal disputes to clarify possible insurance coverage of silent cyber damages in traditional insurance lines. In contrast, in the U.S., particularly in the case of commercial general liability insurance and general property insurance, disputes frequently arise before U.S. courts between policyholders and insurers regarding the coverage of damages caused by data breaches, privacy violations and loss of network or computer functionality due to a cyberattack.

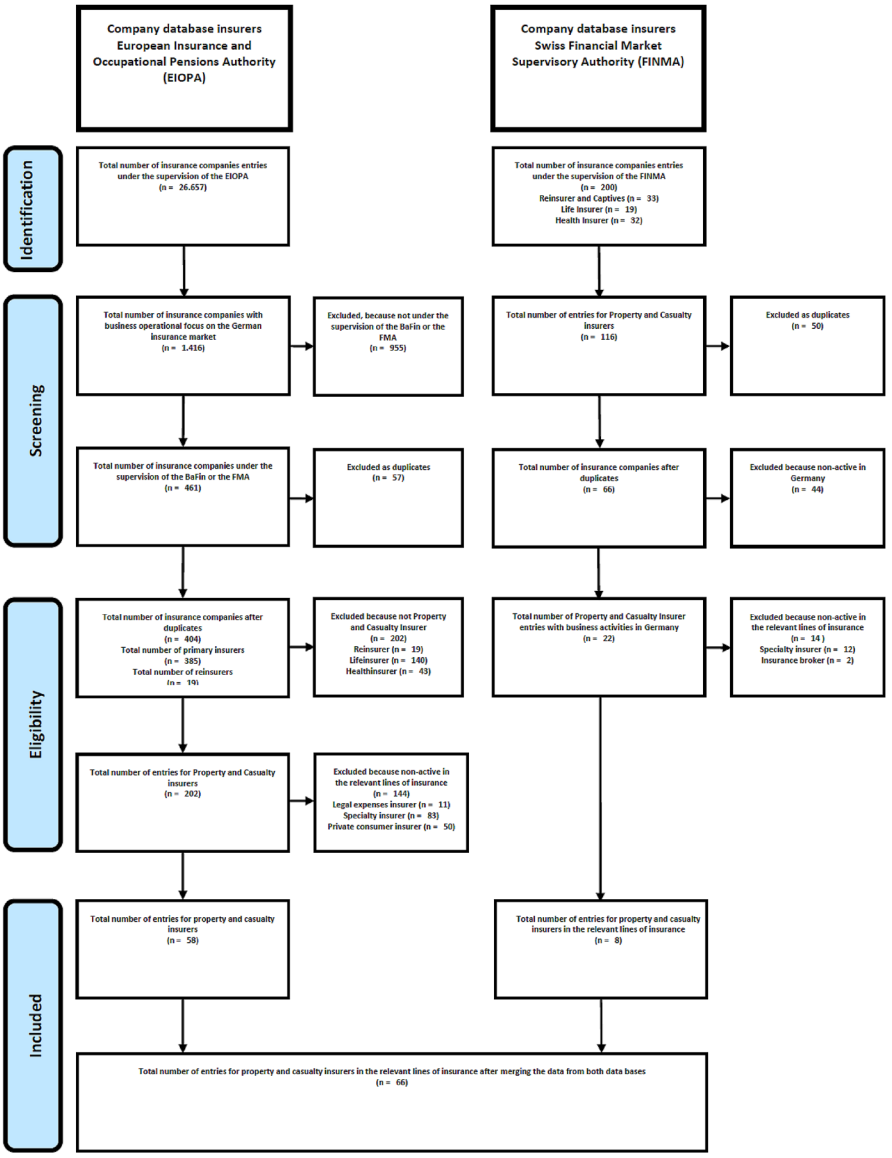

Fig. 2 Flow diagram of the selection process

PRISMA statement for the systematic selection of research objects (Moher et al. 2009).

The information on the selected insurance companies stems from EIOPA and FINMA, which provide databases of the insurers they supervise. The two databases contain data of all insurers operating in the German insurance market,

falling within the responsibilities of the most relevant Financial Supervisory Authorities of the DACH region (BaFin, FMA and FINMA).

First, entries from EIOPA's and FINMA's company databases were transferred to separate Excel files. The file generated from EIOPA's company database initially contained a total of 26,657 data sets and the one generated from FINMA's database 200. The individual data sets contained information on the names of the insurance companies, competent insurance supervisory authorities and business areas. It was possible to search the data records according to predefined selection criteria. Selection characteristics were chosen from the available information. While the first criterion was the German insurance market as a business area, the second selection criterion looked at the responsible insurance supervisory authority. After the first selection step, the number of relevant data sets from EIOPA's company database was reduced to 1416. The second criterion of the supervision by BaFin or FMA reduced the selection to 461 data sets. After the removal of duplicates, 404 data records remained. Since a further predefined selection by insurance type or business line was not possible, the remaining 404 data sets were screened manually using the information on the respective companies' websites. As a result, 202 property and casualty insurers were selected. Finally, we manually re-examined which of the 202 companies offered the insurance types relevant to the study. Based on the information in EIOPA's company database, the selection process identified 58 relevant insurers. In the same way, the data records in the Excel file containing the information from FINMA's company database were selected using the described process and the criteria. After removing duplicates and selecting property and casualty insurers, 66 data records remained. This number was further reduced based on the results of the manual information search by the researchers. A total of eight data sets of relevant insurers could finally be identified in FINMA's company database.

Merging the two Excel files yielded a database consisting of 66 data sets of insurance companies active in the relevant product segments of the German insurance market that fall under the responsibility of BaFin, FMA or FINMA. Before merging the two Excel files, it was documented in which of the relevant insurance lines the selected companies were offering policies to identify the appropriate insurance terms and conditions. For this purpose, the websites of the relevant insurers were examined. A database consisting of a total of 178 insurance terms and conditions resulted.

Collection of the relevant general insurance terms and conditions of the policies began in August 2018. For this purpose, all 66 insurance companies were contacted via e-mail. Additionally, the researchers conducted a systematic internet-based search to obtain the documents for the relevant insurance lines from the insurers' websites. As presented in Table 1, this resulted in the procurement of 48 of the 178 (approximately 27%) contract terms classified as relevant.

Qualitative interviews with experts from the German insurance industry

Additionally, qualitative interviews with representatives from the German insurance industry were performed in February and March 2020. A total of 33 companies from the primary insurance, reinsurance and industrial insurance brokerage

Table 1 Overview of insurance terms and conditions

Insurance line	Total number of relevant insurance terms and conditions	Number of insurance terms and conditions included in the analysis
Business content and income insurance	61	17
Business and professional liability insurance	58	15
Pecuniary loss liability insurance	23	4
Fidelity insurance	12	5
D&O insurance	24	7
Total	178	48

businesses were contacted as potential interview partners. Ultimately, 10 experts participated in the survey, resulting in a response rate of 30.3%. All interviews were conducted via telephone in a semi-structured form (Harvey 1988; Sturges and Hanrahan 2004; Cachia and Millward 2011) with a mixture of open questions allowing the interviewee to comment and expand on the subject more freely, and more specific questions requiring more precise answers. In preparation for the meetings, a questionnaire was developed and used for all the interviews. This questionnaire was sent to the experts beforehand in order for them to prepare and determine if it was recommendable to get further information or refer to additional experts. This survey includes various experts from different company areas. Table 2 displays the number of participants in the individual interviews and information regarding the experts' profession.

The interviews were recorded and transcribed for the analysis (McLellan et al. 2003), which is based on Mayring's qualitative content analysis (Mayring 2015). Two researchers independently analysed all transcriptions to identify different opinions on the management of silent cyber exposure among the informants.

Results

Results of the qualitative content analysis of general insurance terms and conditions

Business content and business income insurance

Business content and business income insurance as property insurance offers coverage for damages resulting from insured risks, such as vehicle impact, burglary, robbery, fire, water leakage or storm damage. Consequently, cyber risks are not explicitly addressed in this line of insurance. Therefore, the product-specific coverage design and individual product components may contain silent cyber coverage. This applies particularly to the insured risks of fire, water leakage and vehicle impact, as

Table 2 Interviewed experts and relevant data

Interview	Expert	Business segment/position	Business field	Place of business
1	1A	Head of Underwriting	Primary insurance	Germany
2	2A	Business Segment: International Steering/Head of Foreign Management	Primary insurance	Germany
3	3A	Business Segment: Financial Lines	Primary insurance	Germany
4	4A	Principal Department of Engineering Insurance	Primary insurance	Germany
5	5A	Senior Corporate Underwriter	Reinsurance	Germany
	5B	Senior Underwriter Casualty		
6	6A	Underwriter Non-life Reinsurance	Reinsurance	Germany
7	7A	Business Segment: Facultative Property & Engineering/General Manager	Reinsurance	Germany
8	8A	Business Segment: Global Line Engineering/Senior Underwriter	Reinsurance	Switzerland
9	9A	Head of Liability and Credit Insurance	Interest group	Germany
10	10A	Specialist Cyber Insurance	Industry insurance broker	Germany

cyberattacks can trigger them. The insurance coverage of all 17 examined policies in this line of business includes fire—triggered by blaze, explosion and impact or crash of an aircraft—and vehicle impact as named perils. Similarly, mains water damage due to incorrect operation or malfunctions of sprinkler systems is covered. In this respect, only two insurance policies contain explicit exclusions and three additional policies offer to include it as an optional extension. In total, silent cyber insurance coverage for losses caused by the above-mentioned insured perils as a result of cyberattacks exists in 15 analysed policies.

Furthermore, the insurance coverage of 15 of the 17 insurance products examined includes the reimbursement of costs resulting from the destruction of physical property caused by cyberattacks in the form of silent cyber coverage. In addition, 15 policies also provide coverage in the form of silent cyber coverage for financial losses due to business interruptions as a result of cyberattacks. If cyberattacks trigger the insured risks in this insurance line and no explicit exclusions are defined, these policies provide insurance coverage for the resulting damages and costs. This insurance line thus contains a considerable amount of silent cyber risks.

Two insurance policies define specific risk and coverage exclusions for losses caused by either malicious software or unauthorised actions and data misuse as a result of an unauthorised intrusion into computer systems. Standard exclusions for claims in connection with wars, civil unrest or nuclear energy are part of all examined contracts. One policy contains an explicit exclusion of cover for damages caused by employees. It is therefore highly probable that this policy does not provide insurance coverage for cybersecurity incidents caused by employees.

Business interruption coverage is a component in this line of insurance, which needs to be purchased additionally. If it is not added to a possible risk (e.g. fire), only the actual damages of the basis risk and not the loss of earnings are covered. Assuming that the policy includes a business interruption add-on, a cybersecurity incident triggering an insured risk will also result in payments based on this component. Therefore this add-on contains silent cyber risk as well. However, some limitations are generally included in the contracts.

Business and professional liability insurance

Business and professional liability insurance generally covers personal injury and property damage, as well as any resulting financial losses. Here, only the liability claims under private law of the affected parties are covered. Insofar as the 15 policies examined offer protection in the event of information security breaches, the scope of insurance coverage is very homogeneous and the insured benefits are almost identical across products. Accordingly, the insurance coverage of all analysed insurance policies for information security breaches includes, on the one hand, the classic benefits of liability insurance, such as defence against unjustified claims for damages, reimbursement of legal costs for the enforcement of claims for damages and release of the policyholder from justified claims for damages. On the other hand, in these cases, the insurance coverage of three policies additionally includes coverage for damages due to data alterations, disruptions of access to an electronic data exchange at third parties, violation of personal rights and rights to a name

and assumption of the costs for the recovery or recording of data not or incorrectly recorded. Insurance coverage for claims for damages arising from contractual liability is not included in any of the policies examined. However, if the policies exclude coverage for losses caused by information security violations, an optional extension for these risks is sometimes offered. For example, the available coverage extensions refer to the coinsurance of financial losses caused by data deletion, data protection violations or losses caused by electronic data transfer and internet use.

Pecuniary loss liability insurance

Pecuniary loss liability insurance covers pure financial losses. Therefore, all four examined policies from this line have identical coverage. For example, all policies include coverage for the financial losses of third parties in the event of violations committed during the exercise of professional activities. The insurance coverage includes legal liability regulations under private law, the assessment of liability issues, defence against unjustified claims for damages and indemnification of the policyholder against justified claims for damages. In all policies examined, there is no evidence of explicit coverage inclusions or exclusions addressing information security breaches. Thus, these products contain significant silent cyber coverage.

Fidelity insurance

Fidelity insurance offers companies protection against financial losses generated by white-collar crime. Generally, insurance coverage is provided for losses caused by deliberate unauthorised actions by company employees or other trusted persons of the company. These policies thus close the gaps in the insurance coverage of business and professional liability insurance, as well as financial loss liability insurance, that exist due to the exclusion of the risks associated with criminal offences. Further, this insurance also covers certain IT risks; for instance, there is coverage for financial losses caused by the tortious actions of outside third parties. Generally, the insurance provides coverage for losses resulting from the betrayal of secrets, as well as computer and data misuse. Additionally, the scope of coverage may also include the reimbursement of specific costs (i.e. IT, loss investigation and prosecution or public relations costs) (Seitz 2011).

In the event of an information security breach, all five policies examined include coverage for damages caused by unauthorised interference by third parties in the company's own IT systems, with or without the intention of personal enrichment, as well as the assessment of liability issues. Additionally, they cover damages caused by internal offenders as well as the assumption of costs incurred for IT forensics, legal prosecution and damage assessment. In contrast, the assumption of costs for the reacquisition and recovery of data or software products is only included in four policies. The reimbursement of notification costs in the event of data protection breaches is incorporated in the insurance coverage of two of the policies examined. Similarly, all policies examined cover losses resulting from spying on business secrets by third parties, including financial compensation for lost corporate profits. Additionally, the policies examined offer continued insurance coverage for

specific risks beyond the end of the contract for a period of up to three years. For losses caused by virus waves, extortion or ransom demands, the policies analysed either contain explicit coverage exclusions or no implicit or explicit risk inclusions or exclusions could be identified. While insurance coverage for reputational damage is generally excluded in all policies, four insurance companies cover at least the costs for their reduction. For business interruptions caused by information security breaches, four of the policies examined include temporary insurance coverage. Furthermore, three insurance policies also cover the assumption of contractual fines and defence costs in the event of cyber damage.

Directors' and officers' insurance

D&O insurance protects executive employees against a possible claim for financial losses resulting from a breach of duty committed in the course of their professional activities. Furthermore, all seven policies examined include insurance coverage for individually contractually-agreed-upon claims for damages, insofar as these arise from legal liability provisions. In addition, defence against unjustified claims for damages and reimbursement of external legal costs for the enforcement of claims for damages on behalf of the policyholder are included in the scope of benefits of all insurance products. Moreover, the insurance coverage of six of the seven policies examined incorporates the assumption of costs by the insurer for measures to reduce the client's reputational damage. Overall, the terms and conditions of all seven analysed insurance contracts show a different design and significant differences in the used formulations. No policy contains any unambiguous formulations that point to comprehensive affirmative insurance coverage for cyber damage. Hitherto, the terms and conditions of all seven analysed D&O insurance policies do not explicitly exclude coverage for cyber risks so that such claims are covered. Consequently, based on the content of the insurance terms and conditions and their formulations, it can be concluded that silent cyber coverage exists in this insurance line.

A summary of the results of the analysis of the above-mentioned insurance lines is given in Table 3.

Results of the qualitative expert interviews

The perception of silent cyber exposures and the implementation status of measures to deal with silent cyber risks show significant differences among the insurers surveyed. This is an exemplary expression for the German insurance industry still being in the early stages of dealing with silent cyber exposures compared to other international insurance markets.

Although all insurers take non-affirmative cyber risks into account in their risk management, the risk potential of silent cyber exposures for their own business is assessed very differently. Reinsurers generally place greater importance on silent cyber exposures, as these companies have been dealing with the issue for some time. One primary insurer surveyed rated the significance of silent cyber exposures as low due to its limited product portfolio. Thus, the company generally refrains from excluding silent

Table 3 Overview of the results of the qualitative content analysis of insurance terms and conditions

Insurance line					
Cyber loss coverage	Business content and income insurance	Business and professional liability insurance	Pecuniary loss liability insurance	Fidelity insurance	D&O insurance
Financial theft and fraud				5/5	
Intellectual property theft				5/5	
Business interruption (affirmative)				4/5	
Business interruption (silent)	15/17				
Cyber extortion				0/5	
Reputational damage				0/5	
Physical asset damage (silent)	15/17				
Data compromise liabilities		3/15			
Financial theft and fraud liabilities				5/5	
Network service failure liabilities		3/15			
Intellectual property theft liabilities				3/5	
Personality rights violation liabilities		3/15			
Contractual liabilities		0/15			
D&O liabilities (silent)					7/7
General asset loss liabilities (silent)			4/4		
Legal costs		15/15	4/4	5/5	7/7
Contractual fines				3/5	
IT forensics				5/5	
Notifications				2/5	
Data and software loss				4/5	
Reputational damage management				4/5	6/7
Costs due to physical asset damage (silent)	15/17				

cyber coverage and instead offers a complementary product component to cover cyber losses in traditional policies. Another primary insurer has already analysed all the terms and conditions for silent cyber exposures since 2017 and adjusted them accordingly. Consequently, the company currently has only explicit risk inclusions or exclusions for cyber risks in all policies. Another company only started an active exchange with other insurers on the subject of silent cyber in 2019 and is now preparing an analysis of its terms and conditions without yet having specified concrete business policy measures for dealing with silent cyber risks.

The total number of identified cases of silent cyber damage at the interviewed companies is very low so far. Due to the scarcity of experience and data on silent cyber claims, the risk models used in the risk management of the surveyed companies are primarily based on expert knowledge. However, they do not possess sufficient expertise on cyber risks, so building up expert knowledge to assess and quantify silent cyber exposures is of high priority. Additionally, reinsurers are essential partners from the perspective of all primary insurers surveyed, as they have better databases on cyber losses and more IT know-how. By making these resources available to primary insurers, they can act as service providers.

For accumulation control, seven of the insurers surveyed used scenario-based catastrophe models, which are predominantly based on approaches for the modelling of natural catastrophe risks. One of the primary insurers also plans to use a scenario-based catastrophe model to analyse silent cyber exposures and is currently preparing a project to introduce a corresponding modelling approach. However, from the perspective of all the reinsurers in the sample, the catastrophe models currently used to model silent cyber exposures are still not sophisticated enough, since the bases for the proposed catastrophic cyber risk scenarios are mostly dependent on qualitative assumptions and expert assessments. Due to the lack of data on silent cyber claims, one reinsurer uses cyber insurance claims data to analyse potential silent cyber exposures in traditional lines of business. Three of the companies surveyed are also conducting advanced risk assessments and stress tests to better assess the impact of cyber loss scenarios on insurance portfolios in traditional lines of business.

For the pricing of affirmative cyber coverage in traditional lines of business, reinsurers make use of existing pricing tools for cyber insurance contracts. In contrast, so far only one of the primary insurers surveyed takes affirmative cyber coverage into account in the pricing without, however, disclosing a separate premium for this in the risk calculation for the client.

In the case of the reinsurers, existing silent cyber coverage in the contracts of the traditional lines of business have in many cases been eliminated by general exclusions and subsequent standard re-inclusions of specific cyber-related risks combined with additional sublimits. In the meantime, German primary insurance companies have also begun to implement similar measures.

Discussion

The results demonstrate that the examined traditional policies offer limited coverage for cyber damages. From the insurers' perspective, the definition of the insured risk in the traditional insurance lines is particularly complicated, given the constant development and high complexity of cyber threats. Existing risk definitions in the terms and conditions should be reformulated and expanded so that inclusions or exclusions become more evident for policyholders (ENISA 2017). Furthermore, silent coverage offers considerable cyber liability potential in the examined traditional insurance lines, which could potentially even amount to systemic risk.

Moreover, terms and conditions often contain imprecise wording of contract contents and insufficient descriptions of the scope of coverage of the insurance policies. However, through the language and formulations used in the terms and conditions, the insurance companies decisively determine the design of the offered insurance coverage and support the development and subsequent establishment of uniform definitions in the contracts (ENISA 2017; Woods and Simpson 2017). Consequently, the examined policies show significant differences in their content due to the respective formulations. For example, the majority of the insurance terms and conditions do not contain standardised definitions of the term 'information security violation' as a triggering factor for determining the insured event. Some contractual terms and conditions exhibit apparent differences in the definition and classification of the term 'information security violation'. Additionally, the terms and conditions sometimes contain different wordings in the descriptions of the contractually defined benefits, although the individual components of the insurance coverage are similar in design.

Thus, the wording used in the terms and conditions of the insurance policies causes uncertainty for insurers and customers concerning existing insurance coverage as well as inclusions and exclusions for cyber risks. This makes it considerably more difficult for insurers to identify silent coverage and to estimate the existing cyber liability potential. Further, the insured companies can only make inadequate assessments of their current insurance coverage for cyber damages (Carter and Enoizi 2020).

The results of the expert interviews show that the German insurance industry is still in the early stages of dealing with silent cyber exposures compared to other international insurance markets. Although insurers are aware of the existing cyber liability potentials in their property and liability portfolios and have begun to analyse the terms and conditions, no uniform implementation status of measures for managing silent cyber risks is discernible in the market. Primary insurers, in particular, should develop a holistic strategy for managing silent cyber risks and the resulting inherent accumulation exposure in order to convert existing silent cyber coverage into affirmative insurance solutions. This would also be advantageous in relation to the supervisory authorities and rating agencies, in order to demonstrate effective risk management with regard to the underwriting of cyber risks.

Depending on the individual implementation level of measures to manage silent cyber risks, reinsurers can support primary insurers by providing a comprehensive range of services. Examples include knowledge exchange, training, provision of wording manuals, accumulation risk assessments, claims data collections and the development of interactive scenario-based analysis tools for risk assessment and visualisation (e.g. through heat maps) in underwriting. In addition, there are a few products from InsurTechs that help insurers examine the extent of silent cyber exposures in their traditional lines of business through automated analyses.

By using scenario-based risk analyses, it is possible to model the development and potentially damaging effects of different cyberattack scenarios. This permits the transparent assessment and forecasting of potential loss developments, including possible accumulative losses on the level of the insurance contract portfolio for cyber insurance and silent cyber exposures in traditional insurance lines. Based on historical cyber damage data, the use of cyber risk heat maps in the context of a risk assessment allows the visualisation of the probability of occurrence and extent of damages due to cyber risks. This provides underwriters with a holistic picture, providing information on company-specific cyber exposure. It also provides the opportunity to identify potential cyber risk hot spots for a variety of industry sectors.

Assuming that most contracts with silent cyber exposure have no effective limitation, it should be in regulators' interest to support and even enforce the establishment of effective risk management by the insurers. This is even more apparent since one large or multiple small-but-connected cyber events might have a substantial or even systemic impact. The financial consequences can translate into limited capacities for other insurance lines and into a fire sale of some assets. The former would have effects exclusively on the insurance market, while the latter could cause chain reactions in the whole capital market. Even the failure of just one insurer could have substantial effects on the insurance market through possible reputational damage. This should justify some reactions by regulators, which could affect individual companies (e.g. higher capital requirements) or the whole market (e.g. legal upper limits, mandatory reinsurance, a risk pool or even state-guaranteed reinsurance).

Another option for the regulator, or a public–private partnership, in Germany could be the development and provision of uniform tools for detecting and reporting cyber damages in traditional lines of business. This could be a shared data pool on cyber claims, which also allows for a differentiation between silent and affirmative cyber damages. With the help of this database, insurers would be able to analyse their silent cyber risks, including accumulation exposures. This would also help the calculation of appropriate insurance premiums.

To set up such a data pool, however, an appropriate legal framework must be established by the government or a legally secure construct needs to be created for the organisation to be founded. This applies in particular with regard to competition law, as the combination of data could violate current legislation (Eling and Schnell 2016a, b). Moreover, legal clarification is also required as to which cyber damage data may be legally collected, stored and exchanged across companies (Falco et al. 2019). However, when setting up such a data pool, implementing the right incentives for large insurers to provide the necessary data might prove

difficult (U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) 2012; Tøndel et al. 2016; Woods and Simpson 2017), as they see too little benefit in such cooperation for themselves (U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) 2012; Tøndel et al. 2016; Siegel et al. 2018). This would mean that only insurers with limited databases would make their data available by actively participating in the information exchange (U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) 2012; Woods and Simpson 2017).

In order for customers to ensure adequate insurance coverage against cyber risks, they should actively involve insurers, experienced brokers or other respective experts to conduct a risk analysis, discuss the results intensively and arrange for the corresponding coverage. This makes it possible to identify unknown overlapping coverage from different lines of business and to eliminate gaps in the coverage. However, this often does not take place because all parties involved have little interest in such time-consuming and information-intensive exchanges. In general, all parties involved are interested in an efficient assessment process, while clients in particular tend to provide as little data as possible (U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) 2012; Tøndel et al. 2016) and intermediaries are subject to conflicts of interest (Yusuf 2011).

In the event of a conflict, the German jurisdiction would be the final authority on the interpretation of the insurance terms and conditions and would thus contribute to improving transparency. In case of doubt, the predominant interpretation, according to the principle of an average policyholder, already suggests a customer-friendly interpretation. The future influence of the jurisdiction is currently unclear as there are still no legal proceedings to clarify silent cyber in Germany and, therefore, no court or supreme court decisions exist to date.

Although this article provides initial insights into the existence of affirmative and silent insurance protection from cyber risks and the resulting silent cyber coverage for selected traditional lines of business, the approach chosen here is not without limitations. Because of the chosen sample size, the results of the qualitative study are limited in their generalisability and representativeness (Firestone 1993; Miles and Huberman 1994). For example, biases may exist due to the selection process of the investigated objects and the choice of interviewees. The former is a selection of insurance lines based exclusively on the literature, while the whole evaluation targets only one single national insurance market.

Furthermore, the limitations of the sample selection should be considered when interpreting the results. This study focuses on the analysis of specific traditional insurance lines in the German insurance market. Since the design of the insurance coverage and product components of the various policies in diverse product lines can differ significantly, the results can only be transferred to other lines of insurance to a limited extent. Also, this study focuses on the German insurance market, limiting the transferability of the results to other countries since country-specific features and particularities are reflected in both the design of coverage and the framework that each national insurance market provides.

Similarly, qualitative interviews were conducted within the scope of the study exclusively with experts from German companies. For example, a subsequent investigation could provide a survey of experts from other international insurance markets to gain additional valuable insights into the way insurers deal with silent cyber risks.

As described, only general insurance terms and conditions were used for the content analysis, being either provided by the contacted insurers or accessible on the insurers' websites. As a result, the insurance terms and conditions of the insurance lines not addressed in this study may contain further affirmative and silent cyber coverage that is not apparent due to the limited amount of data available for content analysis. However, most insurance policies offered on the German market within the considered product lines have a similar range of coverage and comparable product components. Further research, e.g. in the form of quantitative studies, is needed to validate our results with a more comprehensive data set and to generalise the findings. Additional insurance lines in the German market could be included and existing silent cyber exposures compared. Accordingly, additional quantitative and qualitative studies could generate valuable knowledge on the existence, design and management of affirmative and silent cyber coverage in different traditional insurance products on the one hand and other countries on the other hand.

Conclusion

Traditional insurance lines are increasingly affected by claims resulting from cyber risks. As a result, insurance companies also face the challenge of identifying and quantifying silent cyber exposures in traditional insurance lines. However, this is made more difficult by the design of the terms and conditions of individual insurance lines. These largely determine the definition and scope of insurance coverage. Further, general insurance terms and conditions almost always contain imprecise wordings and insufficient descriptions of the contractually specified insurance coverage.

We used Mayring's qualitative content analysis to examine general insurance terms and conditions of different traditional product lines in the German market with regard to the design of affirmative and silent cyber coverages. Additionally, interviews with German insurance experts were conducted to evaluate how insurers understand and manage their silent cyber exposures. Overall, the findings show a partial exposure in different insurance lines due to the current design of the terms and conditions. This causes a considerable amount of silent cyber coverage, which can even lead to systemic effects. Since the German insurance market is still in an early stage of tackling silent cyber risks, insurers have not yet developed holistic strategies for managing silent cyber exposures. Silent cyber exposures require systematic identification and quantification since the involved claims burdens are hard to estimate for insurers. Also, national and European insurance supervisory authorities increasingly pay attention to the problem of silent cyber exposures.

References

Allianz Global Corporate & Specialty SE (AGCS). 2020. *Allianz risk barometer 2020: Identifying the major business risks for 2020*. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf. Accessed 31 March 2020.

Amin, Z. 2019. A practical road map for assessing cyber risk. *Journal of Risk Research* 22 (1): 32–43.

Anderson, R.J., C. Barton, R. Böhme, R. Clayton, C.H. Gañán, T. Grasso, M. Levi, M. Vasek, and T. Moore. 2019. Measuring the changing cost of cybercrime. Paper presented at the 18th Workshop on the Economics of Information Security (WEIS), Boston, MA, USA, June 3–4.

Anderson, R.J., C. Barton, R. Böhme, R. Clayton, M.J.G. Van Eeten, M. Levi, T. Moore, and S. Savage. 2013. Measuring the cost of cybercrime. In *The economics of information security and privacy*, ed. R. Böhme, 265–300. Heidelberg, New York, NY, Dordrecht, London: Springer.

Anderson, R.J., and T. Moore. 2006. The economics of information security. *Science* 314 (5799): 610–613.

Andrijcic, E., and B. Horowitz. 2006. A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk Analysis: An International Journal* 26 (4): 907–923.

Armbrüster, C. 2020. New technologies. Political, legal, economic and factual impact in Germany. German National Report. World Congress of the International Insurance Law Association (AIDA) 2018. Zeitschrift für die gesamte Versicherungswissenschaft. https://doi.org/10.1007/s12297-020-00460-2.

Baban, C.P., T. Barker, Y. Gruchmann, C. Paun, A.C. Peters, and T.H. Stuchtey. 2017a. *Cyberversicherungen als Beitrag zum IT-Risikomanagement—Eine Analyse der Märkte für Cyberversicherungen in Deutschland, der Schweiz, den USA und Großbritannien*. Standpunkt zivile Sicherheit Nr. 8. Potsdam: Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (BIGS). https://www.bigs-potsdam.org/app/uploads/2020/02/Standpunkt_8_2017-Online_120218.pdf. Accessed 15 September 2019.

Baban, C.P., Y. Gruchmann, C. Paun, A.C. Peters, and T.H. Stuchtey. 2017b. *Cyber insurance as a contribution to IT risk management—An analysis of the market for cyber insurance in Germany*. Policy Paper No. 7. Potsdam: Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (BIGS). https://www.bigs-potsdam.org/app/uploads/2020/06/PP_No7_Cyber-Insurance.pdf. Accessed 15 September 2019.

Baer, W.S. 2003. Rewarding IT security in the marketplace. *Contemporary Security Policy* 24 (1): 190–208.

Baer, W.S., and A. Parkinson. 2007. Cyberinsurance in IT security management. *IEEE Security and Privacy* 5 (3): 50–56.

Bahşi, H., U. Franke, and E. Langfeldt Friberg. 2019. The cyber-insurance market in Norway. *Information and Computer Security* 28 (1): 54–67.

Bandyopadhyay, T., V.S. Mookerjee, and R.C. Rao. 2009. Why IT managers don't go for cyber-insurance products. *Communications of the ACM* 52 (11): 68–73.

Bandyopadhyay, T., and S. Shidore. 2011. Towards a managerial decision framework for utilization of cyber insurance instruments in IT security. Paper presented at the 7th Americas Conference on Information Systems (AMCIS), Detroit, MI, USA, August 4–7.

Bank of England Prudential Regulation Authority (PRA). 2016. *Consultation Paper | CP39/16: Cyber insurance underwriting risk*. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2016/cp3916. Accessed 15 September 2019.

Bank of England Prudential Regulation Authority (PRA). 2017. *Supervisory Statement | SS4/17: Cyber insurance underwriting risk*. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417. Accessed 15 September 2019.

Beh, H.G. 2001. Physicial losses in cyberspace. *Connecticut Insurance Law Journal* 8 (1): 55–86.

Bendovschi, A. 2015. Cyber-attacks—Trends, patterns and security countermeasures. *Procedia Economics and Finance* 28: 24–31.

Biener, C., M. Eling, and J.H. Wirfs. 2015. Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance—Issues and Practice* 40 (1): 131–158.

Bodin, L.D., L.A. Gordon, M.P. Loeb, and A. Wang. 2018. Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy* 37 (6): 527–544.

Böhme, R., and G. Schwartz. 2010. Modeling cyber-insurance: Towards a unifying framework. Paper presented at the 9th Workshop on the Economics of Information Security (WEIS), Cambridge, MA, USA, June 7–8.

Bowen, G.A. 2009. Document analysis as a qualitative research method. *Qualitative Research Journal* 9 (2): 27–40.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly* 34 (3): 523–548.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom). 2020. *Spionage, Sabotage und Datendiebstahl—Wirtschaftsschutz in der vernetzten Welt: Studienbericht 2020*. https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf. Accessed 31 March 2020.

Burla, L., B. Knierim, J. Barth, K. Liewald, M. Duetz, and T. Abel. 2008. From text to codings: Intercoder reliability assessment in qualitative content analysis. *Nursing Research* 57 (2): 113–117.

Cachia, M., and L. Millward. 2011. The telephone medium and semi-structured interviews: A complementary fit. *Qualitative Research in Organizations and Management: An International Journal* 6 (3): 265–277.

Camillo, M. 2017. Cyber risk and the changing role of insurance. *Journal of Cyber Policy* 2 (1): 53–63.

Carter, R.A., and J. Enoizi. 2020. *Cyber war and terrorism: Towards a common language to promote insurability.* Zurich: The Geneva Association. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_war_terrorism_commonlanguage_final.pdf. Accessed 23 July 2020.

Cavanagh, S. 1997. Content analysis: Concepts, methods and applications. *Nurse Researcher* 4 (3): 5–16.

Cavusoglu, H., H. Cavusoglu, and S. Raghunathan. 2004. Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems* 14: 65–75.

Choudhry, U. 2014. *Der Cyber-Versicherungsmarkt in Deutschland: Eine Einführung*. Wiesbaden: Springer Gabler.

Coburn, A., P. Ulrich, R. Savage, T. Harvey, G. Woo, P. Sarabandi, S. Arnold, E. Glennie, C. Vos, S. Ruffle, É. Leverett, A. Skelton, J. Copic, S. Sweeney, A. Rais-Shaghagi, V. Kasaite, S. Kelly, D. Ralph, M. Tuveson, L. Pryor, and T. Evan. 2016. *Managing cyber insurance accumulation risk*. Cambridge, UK: Risk Management Solutions, Inc. and University of Cambridge Centre for Risk Studies. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf. Accessed 15 September 2019.

Cohen, D.R., and R.D. Anderson. 2000. Insurance coverage for cyber-losses. *Tort & Insurance Law Journal* 35 (4): 891–928.

Cole, C.R., and S.G. Fier. 2020. An empirical analysis of insurer participation in the U.S. cyber insurance market. *North American Actuarial Journal*. https://doi.org/10.1080/10920277.2020.1733615.

De Smidt, G.A., and W.J.W. Botzen. 2018. Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance—Issues and Practice* 43 (2): 239–274.

DiGrazia, K. 2018. Cyber insurance, data security, and blockchain in the wake of the Equifax breach. *Journal of Business & Technology Law* 13 (2): 255–277.

Downe-Wamboldt, B. 1992. Content analysis: Method, applications, and issues. *Health Care for Women International* 13 (3): 313–321.

Elhabashy, A.E., L.J. Wells, and J.A. Camelio. 2019. Cyber-physical security research efforts in manufacturing—A literature review. *Procedia Manufacturing* 34: 921–931.

Eling, M. 2018. Cyber risk and cyber risk insurance: Status quo and future research. *The Geneva Papers on Risk and Insurance—Issues and Practice* 43 (2): 175–179.

Eling, M., and W. Schnell. 2016a. *Ten key questions on cyber risk and cyber risk insurance*. Zurich: The Geneva Association. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public//cyber-risk-10_key_questions.pdf. Accessed 15 September 2019.

Eling, M., and W. Schnell. 2016b. What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance* 17 (5): 474–491.

Eling, M., and J.H. Wirfs. 2016. *Cyber risk: Too big to insure?—Risk transfer options for a mercurial risk class*. I●VW HSG Schriftenreihe, Bd. 59. St. Gallen: Institut für Versicherungswirtschaft, Universität St. Gallen. http://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/studien/cyberrisk2016.pdf. Accessed 15 September 2019.

Eling, M., and J. Zhu. 2018. Which insurers write cyber insurance? Evidence from the U.S. property and casualty insurance industry. *Journal of Insurance Issues* 41 (1): 22–56.

Elo, S., and H. Kyngäs. 2008. The qualitative content analysis process. *Journal of Advanced Nursing* 62 (1): 107–115.

European Insurance and Occupational Pensions Authority (EIOPA). 2018a. *EU-U.S. insurance dialogue project: The cyber insurance market*. https://www.eiopa.europa.eu/sites/default/files/publications/other_documents/181031_eu-us_project_cyber_insurance_white_paper_publication.pdf. Accessed 15 September 2019.

European Insurance and Occupational Pensions Authority (EIOPA). 2018b. *Understanding cyber insurance—A structured dialogue with insurance companies*. https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf. Accessed 15 September 2019.

European Insurance and Occupational Pensions Authority (EIOPA). 2019. *Cyber risk for insurers—Challenges and opportunities*. https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf. Accessed 31 March 2020.

European Insurance and Occupational Pensions Authority (EIOPA). 2020. *EIOPA strategy on cyber underwriting*. https://www.eiopa.europa.eu/sites/default/files/publications/cyber-underwriting-strategy-february-2020_0.pdf. Accessed 31 March 2020.

European Network and Information Security Agency (ENISA). 2012. *Incentives and barriers of the cyber insurance market in Europe*. https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport. Accessed 15 September 2019.

European Union Agency for Network and Information Security (ENISA). 2016. *Cyber insurance: Recent advances, good practices and challenges*. https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges/at_download/fullReport. Accessed 15 September 2019.

European Union Agency for Network and Information Security (ENISA). 2017. *Commonality of risk assessment language in cyber insurance: Recommendations on cyber insurance*. https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance/at_download/fullReport. Accessed 15 September 2019.

Falco, G., M. Eling, D. Jablanski, M. Weber, V. Miller, L.A. Gordon, S.S. Wang, J. Schmit, R. Thomas, M. Elvedi, T. Maillart, E. Donavan, S. Dejung, E. Durand, F. Nutter, U. Scheffer, G. Arazi, G. Ohana, and H. Lin. 2019. Cyber risk research impeded by disciplinary barriers. *Science* 366 (6469): 1066–1069.

Ferland, J. 2019. Cyber insurance—What coverage in case of an alleged act of war? Questions raised by the *Mondelez v. Zurich* case. *Computer Law & Security Review* 35 (4): 369–376.

Finfgeld-Connett, D. 2014. Use of content analysis to conduct knowledge-building and theory-generating qualitative systematic reviews. *Qualitative Research* 14 (3): 341–352.

Firestone, W.A. 1993. Alternative arguments for generalizing from data as applied to qualitative research. *Educational Researcher* 22 (4): 16–23.

Flagmeier, W., and J. Heidemann. 2018. *Sonderheft: Cyber-Versicherungen*, 4th ed. Köln: Wolters Kluwer.

Franke, U. 2017. The cyber insurance market in Sweden. *Computers & Security* 68: 130–144.

Franke, U. 2018. Cyber insurance against electronic payment service outages: A document study of terms and conditions from electronic payment service providers and insurance companies. In *Security and Trust Management: 14th International Workshop, STM 2018, Barcelona, Spain, September 6–7, 2018, Proceedings*, ed. S.K. Katsikas, and C. Alcaraz, 73–84. Cham: Springer.

Franke, U., and P.H. Meland. 2019. Demand side expectations of cyber insurance. Paper presented at the International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Oxford, United Kingdom, June 3–4.

Furnell, S.M., and M.J. Warren. 1999. Computer hacking and cyber terrorism: The real threats in the new millennium? *Computers & Security* 18 (1): 28–34.

Gandhi, R., A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante. 2011. Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine* 30 (1): 28–38.

Gebert, Y., and S. Klapper. 2020. § 24 Cyberversicherung. In *Der Versicherungsprozess: Ansprüche und Verfahren—Praxishandbuch*, 4th ed., ed. J. Veith, J. Gräfe, and Y. Gebert, 1360–1383. Baden-Baden: Nomos.

German Insurance Association (GDV). 2019. *Statistical yearbook of German insurance 2019*. https://www.en.gdv.de/resource/blob/52084/8586ea0d4ff8aba4982b18792111967a/statistical-yearbook-2019—broschuere-data.pdf. Accessed 31 March 2020.

Gioia, D.A., K.G. Corley, and A.L. Hamilton. 2013. Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational Research Methods* 16 (1): 15–31.

Gordon, L.A., M.P. Loeb, and T. Sohail. 2003. A framework for using insurance for cyber-risk management. *Communications of the ACM* 46 (3): 81–85.

Graneheim, U.H., B.-M. Lindgren, and B. Lundman. 2017. Methodological challenges in qualitative content analysis: A discussion paper. *Nurse Education Today* 56: 29–34.

Graneheim, U.H., and B. Lundman. 2004. Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today* 24 (2): 105–112.

Grund, F. 2020. Cyber-Risiken: Die Sicht der Aufsicht. Keynote presented at the 22. EUROFORUM-Jahrestagung Haftpflicht 2020, Hamburg, Germany, January 21–22. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Reden/re_200121_Haftpflicht-Jahrestagung_EDVA.html. Accessed 31 March 2020.

Guest, G., A. Bunce, and L. Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field Methods* 18 (1): 59–82.

Haas, A. 2016. Management von Cyber-Risiken und Möglichkeiten des Risikotransfers: eine ökonomische und versicherungstechnische Analyse. PhD diss., Universität Hohenheim. http://opus.uni-hohenheim.de/volltexte/2016/1192/pdf/Diss_Haas_Buchdruck_Final.pdf. Accessed 15 September 2019.

Haas, A., and A. Hofmann. 2014. Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. *Zeitschrift für die gesamte Versicherungswissenschaft* 103 (4): 377–407.

Harvey, C.D.H. 1988. Telephone survey techniques. *Canadian Home Economics Journal* 38 (1): 30–35.

Harwood, T.G., and T. Garry. 2003. An overview of content analysis. *The Marketing Review* 3 (4): 479–498.

Hennink, M.M., B.N. Kaiser, and V.C. Marconi. 2017. Code saturation versus meaning saturation: How many interviews are enough?. *Qualitative Health Research* 27 (4): 591–608.

Her Majesty's (HM) Government (UK) and Marsh Ltd. 2015. *UK cyber security: The role of insurance in managing and mitigating the risk*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf. Accessed 15 September 2019.

Hiller, J.S., and R.S. Russell. 2013. The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review* 29 (3): 236–245.

Hiscox Ltd. 2018. *Hiscox cyber readiness report 2018*. https://www.hiscox.de/wp-content/uploads/2018/02/Hiscox-Cyber-Readiness-Report-2018-FINAL.pdf. Accessed 31 March 2020.

Hsieh, H.-F., and S.E. Shannon. 2005. Three approaches to qualitative content analysis. *Qualitative Health Research* 15 (9): 1277–1288.

Hunt, T.D. 2019. "The internet of buildings": Insurance of cyber risks for commercial real estate. *Oklahoma Law Review* 71 (2): 397–452.

Hyman, P. 2013. Cybercrime: It's serious, but exactly how serious?. *Communications of the ACM* 56 (3): 18–20.

Innerhofer-Oberperfler, F., and R. Breu. 2010. Potential rating indicators for cyberinsurance: An exploratory qualitative study. In *Economics of information security and privacy*, ed. T. Moore, D. Pym, and C. Ioannidis, 249–278. Boston, MA: Springer.

Järveläinen, J. 2013. IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management* 33 (3): 583–590.

Jerry II, R.H., and M.L. Mekel. 2001. Cybercoverage for cyber-risks: An overview of insurers' responses to the perils of e-commerce. *Connecticut Insurance Law Journal* 8 (1): 7–36.

Jouini, M., L.B.A. Rabai, and A.B. Aissa. 2014. Classification of security threats in information systems. *Procedia Computer Science* 32: 489–496.

Kesan, J.P., and C.M. Hayes. 2017. Strengthening cybersecurity with cyberinsurance markets and better risk assessment. *Minnesota Law Review* 102 (1): 191–276.

Kesan, J.P., R.P. Majuca, and W.J. Yurcik. 2005. Cyberinsurance as a market-based solution to the problem of cybersecurity—A case study. Paper presented at the 4th Workshop on the Economics of Information Security (WEIS), Cambridge, MA, USA, June 2–3.

Kirkpatrick, K. 2015. Cyber policies on the rise. *Communications of the ACM* 58 (10): 21–23.

Kiss, M., G. Breda, and L. Muha. 2019. Information security aspects of Industry 4.0. *Procedia Manufacturing* 32: 848–855.

Knutsen, E.S., and J.W. Stempel. 2018. The techno-neutrality solution to navigating insurance coverage for cyber losses. *Penn State Law Review* 122 (3): 645–682.

Koezuka, T. 2016. The cyber insurance in Japan. In *The "Dematerialized" insurance: Distance selling and cyber risks from an international perspective*, ed. P. Marano, I. Rokas, and P. Kochenburger, 201–223. Cham: Springer.

Kondracki, N.L., N.S. Wellman, and D.R. Amundson. 2002. Content analysis: Review of methods and their applications in nutrition education. *Journal of Nutrition Education and Behavior* 34 (4): 224–230.

KPMG AG Wirtschaftsprüfungsgesellschaft. 2017a. *e-Crime in der deutschen Wirtschaft 2017—Computerkriminalität im Visier*. http://hub.kpmg.de/hubfs/LandingPages-PDF/e-crime-studie-2017-KPMG.pdf. Accessed 15 September 2019.

KPMG AG Wirtschaftsprüfungsgesellschaft. 2017b. *Neues Denken, Neues Handeln—Versicherungen im Zeitalter von Digitalisierung und Cyber Studienteil B: Cyber*. https://assets.kpmg.com/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-cyber-de.pdf. Accessed 15 September 2019.

Lagazio, M., N. Sherif, and M. Cushman. 2014. A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security* 45: 58–74.

Lathrop, A.J., and J.M. Stanisz. 2016. Hackers are after more than just data: Will your company's property policies respond when cyber attacks cause physical damage and shut down operations? *Environmental Claims Journal* 28 (4): 286–303.

Mainelli, M. 2012. Learn from insurance: Cyber bore. *The Journal of Risk Finance* 14 (1): 100–102.

Majuca, R.P., W.J. Yurcik, and J.P. Kesan. 2006. *The evolution of cyberinsurance*. Working Paper. Urbana-Champaign, IL: University of Illinois at Urbana-Champaign. https://arxiv.org/ftp/cs/papers/0601/0601020.pdf. Accessed 15 September 2019.

Marotta, A., F. Martinelli, S. Nanni, A. Orlando, and A. Yautsiukhin. 2017. Cyber-insurance survey. *Computer Science Review* 24: 35–61.

Marotta, A., F. Martinelli, S. Nanni, and A. Yautsiukhin. 2015. *A survey on cyber-insurance*. Technical Report IIT TR-17/2015. Pisa: Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche. http://www.iit.cnr.it/sites/default/files/TR-17-2015.pdf. Accessed 15 September 2019.

Mayring, P. 2015. *Qualitative Inhaltsanalyse: Grundlagen und Techniken*, 12th ed. Weinheim, Basel: Beltz.

McLaughlin, K.L. 2011. Cyber attack! Is a counter attack warranted?. *Information Security Journal: A Global Perspective* 20 (1): 58–64.

McLellan, E., K.M. MacQueen, and J.L. Neidig. 2003. Beyond the qualitative interview: Data preparation and transcription. *Field Methods* 15 (1): 63–84.

Meland, P.H., I.A. Tøndel, M.E.G. Moe, and F. Seehusen. 2017. Facing uncertainty in cyber insurance policies. In *Security and Trust Management: 13th International Workshop, STM 2017, Oslo, Norway, September 14–15, 2017, Proceedings*, ed. G. Livraga, and C. Mitchell, 89–100. Cham: Springer.

Meland, P.H., I.A. Tøndel, and B. Solhaug. 2015. Mitigating risk with cyberinsurance. *IEEE Security and Privacy* 13 (6): 38–43.

Middleton, K., and M. Kazamia. 2016. Cyber insurance: underwriting, scope of cover, benefits and concerns. In *The "Dematerialized" insurance: Distance selling and cyber risks from an international perspective*, ed. P. Marano, I. Rokas, and P. Kochenburger, 185–200. Cham: Springer.

Miles, M.B., and A.M. Huberman. 1994. *Qualitative data analysis: An expanded sourcebook*, 2nd ed. Thousand Oaks, CA, London, New Delhi: SAGE Publications.

Miller, F.A., and K. Alvarado. 2005. Incorporating documents into qualitative nursing research. *Journal of Nursing Scholarship* 37 (4): 348–353.

Moher, D., A. Liberati, J. Tetzlaff, D.G. Altman, and The PRISMA Group. 2009. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Annals of Internal Medicine* 151 (4): 264–269.

Moore, T. 2010. The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection* 3 (3–4): 103–117.

Morse, J.M. 2008. Confusing categories and themes. *Qualitative Health Research* 18 (6): 727–728.

Organization for Economic Co-operation and Development (OECD). 2017a. *Enhancing the role of insurance in cyber risk management*. Paris: OECD Publishing. https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf. Accessed 15 September 2019.

Organization for Economic Co-operation and Development (OECD). 2017b. *Supporting an effective cyber insurance market: OECD report for the G7 Presidency*. https://www.oecd.org/daf/fin/insurance/Supporting-an-effective-cyber-insurance-market.pdf. Accessed 15 September 2019.

Pain, D.L., and J. Anchen. 2017. *Cyber: Getting to grips with a complex risk*. sigma No 1/2017. Zurich: Swiss Re Institute Economic Research & Consulting. http://media.swissre.com/documents/sigma1_2017_en.pdf. Accessed 15 September 2019.

Pain, D.L., J. Anchen, M. Bundt, E. Durand, M. Schmitt, and C. Bieck. 2016. *Cyber: In search of resilience in an interconnected world*. Zurich: Swiss Re Ltd. Economic Research & Consulting and IBM Institute for Business Value. https://www.swissre.com/dam/jcr:30b64544-9514-4389-aaf1-13fb74f51eab/ZRH-16-09789-P1_Cyber+Publication_web.pdf. Accessed 15 September 2019.

Pereira, T., L. Barreto, and A. Amaral. 2017. Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing* 13: 1253–1260.

Pilz, K. 2006. Das Spannungsverhältnis von Unklarheitenregel und Transparenzgebot—insbesondere bei Allgemeinen Versicherungsbedingungen. *Zeitschrift für die gesamte Versicherungswissenschaft* 95 (Supplement 1): 231–247.

Potter, W.J., and D. Levine-Donnerstein. 1999. Rethinking validity and reliability in content analysis. *Journal of Applied Communication Research* 27 (3): 258–284.

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

Romanosky, S., L. Ablon, A. Kuehn, and T. Jones. 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk?. *Journal of Cybersecurity* 5 (1). https://doi.org/10.1093/cybsec/tyz002.

Ruffle, S., É. Leverett, A. Coburn, J. Copic, S. Kelly, T. Evan, D. Ralph, M. Tuveson, O. Bochmann, L. Pryor, and J.Z. Yeo. 2015. *Business blackout: The insurance implications of a cyber attack on the US power grid*. Cambridge, UK: Lloyd's of London and University of Cambridge Centre for Risk Studies. https://www.lloyds.com/~/media/files/news-and-insight/risk-insight/2015/business-blackout/business-blackout20150708.pdf. Accessed 15 September 2019.

Salmela, H. 2008. Analyzing business losses caused by information systems risk: A business process analysis approach. *Journal of Information Technology* 23 (3): 185–202.

Schanz, K.-U. 2018. *Understanding and addressing global insurance protection gaps*. Zurich: The Geneva Association. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/understanding_and_addressing_global_insurance_protection_gaps.pdf. Accessed 30 June 2020.

Seitz, S. 2011. Die aktuelle Bedeutung und Gestaltung der Vertrauensschadenversicherung—zugleich eine rechtsvergleichende Betrachtung der Fidelity Insurance in den USA. *Zeitschrift für die gesamte Versicherungswissenschaft* 100 (5): 779–793.

Shackelford, S.J. 2012. Should your firm invest in cyber risk insurance?. *Business Horizons* 55 (4): 349–356.

Shetty, S., M. McShane, L. Zhang, J.P. Kesan, C.A. Kamhoua, K. Kwiat, and L.L. Njilla. 2018. Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance—Issues and Practice* 43 (2): 224–238.

Siegel, C.A., T.R. Sagalow, and P. Serritella. 2002. Cyber-risk management: Technical and insurance controls for enterprise-level security. *Information Systems Security* 11 (4): 33–49.

Siegel, M., N. Bartol, J.J. Carrascosa Pulido, S.E. Madnick, M. Coden, M.S. Jalali, and M.J. Bernaski. 2018. *Cyber insurance as a risk mitigation Strategy*. Zurich: The Geneva Association. https://

www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_insurance_as_a_risk_mitigation_strategy.pdf. Accessed 15 September 2019.

Smith, G.S. 2004. Recognizing and preparing loss estimates from cyber-attacks. *Information Systems Security* 12 (6): 46–57.

Strupczewski, G. 2017. The cyber insurance market in Poland and determinants of its development from the insurance broker's perspective. *Economics and Business Review* 3 (2): 33–50.

Sturges, J.E., and K.J. Hanrahan. 2004. Comparing telephone and face-to-face qualitative interviewing: A research note. *Qualitative Research* 4 (1): 107–118.

Talesh, S.A. 2018. Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. *Law & Social Inquiry* 43 (2): 417–440.

Thomas, D.R. 2006. A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation* 27 (2): 237–246.

Tøndel, I.A., P.H. Meland, A. Omerovic, E.A. Gjære, and B. Solhaug. 2015. *Using cyber-insurance as a risk management strategy: Knowledge gaps and recommendations for further research*. Technical Report SINTEF A27298. Oslo: SINTEF ICT. https://sintef.brage.unit.no/sintef-xmlui/bitstream/handle/11250/2379189/SINTEF%2bA27298.pdf?sequence=3&isAllowed=y. Accessed 15 September 2019.

Tøndel, I.A., F. Seehusen, E.A. Gjære, and M.E.G. Moe. 2016. Differentiating cyber risk of insurance customers: The insurance company perspective. In *Availability, Reliability, and Security in Information Systems: IFIP WG 8.4, 8.9, TC 5 International Cross-Domain Conference, CD-ARES 2016, and Workshop on Privacy Aware Machine Learning for Health Data Science, PAML 2016, Salzburg, Austria, August 31 – September 2, 2016, Proceedings*, ed. F. Buccafurri, A. Holzinger, P. Kieseberg, A.M. Tjoa, and E. Weippl, 175–190. Cham: Springer.

Tonn, G., J.P. Kesan, L. Zhang, and J. Czajkowski. 2019. Cyber risk and insurance for transportation infrastructure. *Transport Policy* 79: 103–114.

Toregas, C., and N. Zahn. 2014. *Insurance for cyber attacks: The issue of setting premiums in context*. Technical Report GW-CSPRI-2014-1. Washington, DC: Cyber Security Policy and Research Institute, The George Washington University. https://cspri.seas.gwu.edu/sites/cspri.seas.gwu.edu/files/downloads/cyberinsurance_paper_pdf_0.pdf. Accessed 15 September 2019.

Tosh, D.K., S. Shetty, S. Sengupta, J.P. Kesan, and C.A. Kamhoua. 2017. Risk management using cyber-threat information sharing and cyber-insurance. In *Game Theory for Networks: 7th International EAI Conference, GameNets 2017, Knoxville, TN, USA, May 9, 2017, Proceedings*, ed. L. Duan, A. Sanjab, H. Li, X. Chen, D. Materassi, and R. Elazouzi, 154–164. Cham: Springer.

U.S. Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD). 2012. *Cybersecurity insurance workshop readout report*. https://www.cisa.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf. Accessed 15 September 2019.

Vaismoradi, M., H. Turunen, and T. Bondas. 2013. Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences* 15 (3): 398–405.

Weber, R.P. 1990. *Basic content analysis*, 2nd ed. Newbury Park, CA, London, New Delhi: SAGE Publications.

Willis, A.R. 2010. Business insurance: First-party commercial property insurance and the physical damage requirement in a computer-dominated world. *Florida State University Law Review* 37 (4): 1003–1022.

Willis Re. 2017. *2017 silent cyber risk outlook: Is silent cyber risk creeping up on insurers?*. https://www.willistowerswatson.com/-/media/WTW/Insights/2017/09/Silent-Cyber-Survey.pdf. Accessed 15 September 2019.

Willis Re. 2018. *2018 silent cyber risk outlook: Silent cyber risk concerns growing across the board*. https://www.willistowerswatson.com/-/media/WTW/Insights/2018/09/silent-cyber-risk-concerns-growing-across-the-board-2018.pdf?modified=20180914214751. Accessed 15 September 2019.

Willis Re. 2019. *2019 silent cyber risk outlook: Silent cyber risk concerns decline after 2018 spike*. https://www.willistowerswatson.com/-/media/WTW/Insights/2019/08/silent-cyber-risk-outlook-2019.pdf?modified=20190827083929. Accessed 31 March 2020.

Willis Towers Watson. 2019. *Industrieversicherungen MARKTspot 2019—Rückblick | Ausblick*. https://www.willistowerswatson.com/-/media/WTW/Insights/2019/06/MARKTspot-2019_FINAL.pdf?modified=20190620013848. Accessed 31 March 2020.

Woods, D.W., and T. Moore. 2020. Does insurance have a future in governing cybersecurity? *IEEE Security and Privacy* 18 (1): 21–27.
Woods, D.W., and A.C. Simpson. 2017. Policy measures and cyber insurance: A framework. *Journal of Cyber Policy* 2 (2): 209–226.
Woods, D.W., I. Agrafiotis, J.R.C. Nurse, and S. Creese. 2017. Mapping the coverage of security controls in cyber insurance proposal forms. *Journal of Internet Services and Applications* 8 (1): 8. https://doi.org/10.1186/s13174-017-0059-y.
World Economic Forum. 2020. *The global risks report 2020*. 15th ed. Geneva: World Economic Forum. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. Accessed 31 March 2020.
Wrede, D., T. Freers, and J.-M. Graf von der Schulenburg. 2018. Herausforderungen und Implikationen für das Cyber-Risikomanagement sowie die Versicherung von Cyberrisiken—Eine empirische Analyse. *Zeitschrift für die gesamte Versicherungswissenschaft* 107 (4): 405–434.
Wu, M., and Y.B. Moon. 2017. Taxonomy of cross-domain attacks on cybermanufacturing system. *Procedia Computer Science* 114: 367–374.
Young, D., J. Lopez Jr., M. Rice, B. Ramsey, and R. McTasney. 2016. A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection* 14: 43–57.
Yusuf, T.O. 2011. Brokers' incentives and conflicts of interest in the control of opportunism. *The Journal of Risk Finance* 12 (3): 168–181.
Zelle, A.R., and S.M. Whitehead. 2014. Cyber liability: It's just a click away. *Journal of Insurance Regulation* 33 (6): 145–168.
Zhao, X., L. Xue, and A.B. Whinston. 2013. Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. *Journal of Management Information Systems* 30 (1): 123–152.

About the authors

Dirk Wrede Dipl.-Oec., born in 1980, has been a doctoral student and research associate since 2014 at the Institute for Risk and Insurance, Leibniz University Hannover. Prior to that, he studied economics at the University of Kassel. His research interests include risk management and the insurability of critical infrastructures, insurance coverage for cyber risk and managerial accounting in insurance companies.

Tino Stegen M. Sc., born in 1983, studied economics from 2011 to 2018 at the Leibniz University Hannover. In his professional activities, he works in the field of regulation and risk management in the insurance industry, in particular on the topics of business and risk strategy, as well as the analysis and rating of insurance conditions.

Johann-Matthias Graf von der Schulenburg , born in 1950, teaches risk and insurance and health economics at the Leibniz University Hannover. He is the director of the Institute for Risk and Insurance and member of the board of the House of Insurance (HoI). He also leads the Center for Health Economics Research Hannover (CHERH). He was the founding president of the German Society for Health Economics and the Vice President of the German Risk and Insurance Association.