Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 219 (2023) 521–528

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2022

Consumer Cyber Insurance as Risk Transfer: A Coverage Analysis

Florian Schütz *, Florian Rampold, Andre Kalisch, Kristin Masuch

University of Goettingen, Platz der Göttinger Sieben 5, Göttingen 37073, Germany

Abstract

The internet has become an integral part of most people's lives. Although this has many advantages, such as constant entertainment and easy access to resources, the internet also has its downsides. Studies indicate that people tend to be more concerned with the cyber risks that arise from their internet usage than before. While cyber insurance for businesses has been on the market for several years, the novel type of consumer cyber insurance (CCI) mitigates cyber risks to a residual level. However, we argue that both supply and demand sides do not have a shared understanding of CCIs due to the complexity and dynamics of cyber risks. Therefore, we conduct a content analysis regarding the coverage of CCI to (1) demonstrate the potential value of such insurance policies for private households and (2) increase consumer awareness of the dynamically changing cyber risk situation.

Keywords: Consumer Cyber Insurance; Cyber Loss; Cyber Risk; Cyber Coverage; Insurance Innovation.

1. Introduction

As the 21st century has moved on, the internet has increasingly evolved into an integral part of daily life [1,2]. Current studies indicate that internet users are increasing worldwide [3,4]. Moreover, time spent on the internet is growing, and lockdowns have exacerbated this development due to the COVID-19 pandemic [5]. The everyday

* Corresponding author. Tel.: +49-551-39-26072
E-mail address: florian.schuetz@uni.goettingen.de

10.1016/j.procs.2023.01.320

activities that individuals of different ages and backgrounds undertake on the internet are thereby manifold [6], e.g., online shopping, online banking, and email communication [7,8]. Despite the opportunities linked to internet use, there are also tremendous challenges. For instance, internet use is associated with many cyber risks [9], e.g., cybercrime, IT failure, and data breaches [10]. However, not only governmental institutions and companies but also citizens are increasingly affected by cyber risks due to increased digitalization [11]. It is becoming apparent that consumers are exposed to various cyber threats, such as identity or payment card theft [12].

A study of crime statistics from the UK indicates that during the COVID-19 pandemic, individuals were more acutely affected by cyber-crimes than organizations [7]. Monteith et al. [13] point out that individuals using unfamiliar technologies without appropriate security awareness training are vulnerable targets for cybercriminals. Measures such as antivirus software and firewalls are also proven technical methods to ensure security against cyber-attacks [14]. But even with the use of preventive and technical IT security measures, cyber risks can best be reduced to a level of residual risk rather than eliminated [9]. As European insurers have recognized that consumers are faced with cyber risks increasingly, they are thus trying to create an offer with cyber insurance policies [12]. However, the design of consumer cyber insurance policies is complicated from insurers' perspective due to a lack of commonality of cyber risk assessment language and thus lack of an appropriate pricing approach [12,15].

At the same time, for customers to understand consumer cyber insurance, explicit language and standardization are needed in the policies [16]. The difficulty of comparing the coverage of corporate cyber insurance policies for decision makers mentioned by Romanosky et al. [17] may also explain the low willingness to adopt consumer cyber insurance shown in earlier studies [18]. We conclude that consumers need a clear understanding of the highly diversified market for consumer cyber insurance policies and their cyber-specific characteristics. Therefore, this paper deals with the following research question: *Which currently available insurance products can cover consumer cyber losses?*

We address this research gap by conducting a content analysis of consumer cyber insurance policies. Our research approach contributes to existing cyber risk and insurance literature in at least three ways. First, we investigate the idea of cyber risk transfer through cyber insurance, not in a general or corporate context, but explicitly for consumers. Secondly, we argue that understanding the current coverage of consumer cyber insurance is necessary for consumers to make value-adding decisions according to their individual cyber risk profiles. Hence, the coverage of existing consumer cyber insurance policies identified in this study can be compared with the surveyed customer expectations. By bias-reduced benchmarking actual and consumer needs-based target coverage, we can thus provide recommendations for continuous cyber insurance product optimization given the dynamic cyber risks.

2. Research Background

2.1. Understanding cyber risks from the perspective of insurance economics

As a result of digitalization, society is increasingly exposed to cyber risks, which take familiar, tangible forms such as DoS attacks, reputational damage, or data theft [19]. However, the cyber risk does not yet seem to have an established definition due to its multidimensional characteristics [20]. The term cyber risk is composed of two distinctive constructs: cyber and risk. Whereas cyber refers to electronic communication networks and virtual reality, the risk is defined as an event with the possibility of adverse effects [21,22]. On the one hand, few researchers limit cyber risk to malicious events caused by digital interaction, which negatively impact corporate operations [21]. On the other hand, cyber risk can be understood in a much broader sense [21], e.g., as a failure of information systems [23] or information security risk [24]. Biener et al. [21] synthesize these considerations and elaborate cyber risk to be "operational risk emanating from information stored on data volumes and networks". This definition leaves out the interaction of electronic communication networks. Hence, following Cebula et al. [25], we define cyber risk as any risk emerging from the use of IT that compromises the confidentiality, availability, or integrity of data or services. Since cyber insurance is a risk transfer tool [20], this informs us about the range of cyber risks to consider (or exclude).

2.2. Understanding cyber insurances from the perspective of information systems

In the research and insurance industry, cyber insurance has received increased attention in recent years [26–30], with information technology, economic, statistical, and actuarial perspectives being adopted, among others [20]. Due

to the steady rise of interconnected devices and the global availability of the internet, cyber insurance represents an evolving business for the insurance industry [31]. By acquiring cyber insurance, policyholders aim to transfer cyber risks to a third party and thus protect themselves from financial losses from cyber-attacks [30,32]. This monetary compensation is realized (1) collectively and (2) over a period of time [21]. Zeller and Scherer [20] point out that cyber insurance can go beyond compensation for financial losses, contrary to conventional insurance products.

The business model behind cyber insurance offers a range of services that aim to minimize adverse impacts for organizations arising from cyber incidents [31]. In return for a premium payment due in advance, an insurer obligates itself to provide loss-dependent benefits in the case of one of the contractually agreed loss events [33]. Similar to other types of insurance products, cyber insurance policies insure "first-party" losses suffered by the policyholder and so-called third-party losses caused by the policyholder to a third party outside of the policy [17]. Although cyber insurance formally exists, its current coverage appears insufficient in the face of increasing cyber risks [34].

Along with the increasing number of observed cyber-attacks, the scientific community's interest in cyber insurance has also risen [35]. This is reflected in a large number of publications. Frequently cited literature reviews such as Eling and Schnell [22] limited their search queries to "cyber insurance" and "cyber risk (insurance)". According to our findings, different terms for cyber insurance policies vary significantly. Parallel to "cyber insurance" [17,36,37], the terms "cyber risk insurance" [22,38,39], "cyber liability insurance" [40–42], "data breach liability insurance" [41], "internet insurance" [9], or "cyber security insurance" [29,31,35,43] are mainly used equivalently according to our evaluation. In our work, we refer to cyber insurance as the most common one describing our object of interest.

In general, three different categories of cyber coverage can be distinguished in the insurance market: (1) stand-alone cyber policies, (2) cyber coverage as part of an existing traditional insurance product, and (3) silent cyber coverage in the form of policies without exclusions or gaps in explicit exclusions [44–46]. According to Wrede et al. [44], the problem of silent cyber coverage is also taken more and more into consideration by insurance supervisory authorities in Germany and within the EU. Against this background, Sigholm and Larsson [32] consider the underwriting data of insurers to be a suitable measure for assessing the overall economic costs resulting from cyber-attacks. Beyond those considerations, such as the insurability of cyber risks, the insurance market offers an increasing range of cyber insurance policies [20]. At the same time, industry experts also predict an increasing demand for cyber insurance policies due to both the increased frequency of cyber incidents and the resulting cyber risk awareness [12].

Considering the supply and demand side, Marotta et al. [36] assess the European market for cyber insurance as promising, given the growth and the limited presence of competing insurers. However, previous studies such as Biener et al. [21] and Romanosky et al. [17] explicitly focus on companies' customers. European Insurance and Occupational Pensions Authority [12] attributes the fact that companies and consumers could increasingly become the target market of cyber insurance coverage due to the growing importance of the Internet of Things (IoT) and the higher risk exposure in the use of digital resources. Although Labunets et al. [47] provide an initial blueprint of the cyber insurance ecosystem, it does not sufficiently consider consumers' perspectives as actors and instead focuses on companies as cyber insurance policyholders. Even some highly specialized insurance products focusing on the consumer, such as Identity Theft Insurance, exist [48,49], these products cover only a subset of potential consumer cyber losses. The investigation of cyber losses covered by personal identity insurance available in the US insurance market seems relevant, although not only, e.g., homeowner insurance, but the breadth of insurance lines available to consumers should be investigated [50]. Synoptically, in contrast to previous strategies of dealing with risks (i.e., avoidance, reduction, mitigation), consumer cyber insurance represents a specific risk transfer option for private households. That is why we explicitly focus on consumers as policyholders of available cyber insurance product lines.

3. Research Approach

In order to answer our research question about the current coverage of consumer cyber insurance, we opted for a qualitative research design. Therefore, we base our research approach on Wrede et al. [44], Romanosky et al. [17] and Woods [50], who have conducted coverage analyses of cyber insurance with different points of view. Further developing previous studies, we would like to focus on external validity in our study. More specifically, if a consumer wants to cover his cyber risks through insurance, it does not directly matter to him whether it is a stand-alone policy or a cyber insurance element embedded in a traditional insurance policy. As Woods [50] suggested, we, therefore, include other insurance lines in our analysis besides stand-alone policies. Also, detached from other influencing factors

such as premium level, or experience with the insurers, the customer interested in consumer cyber insurance would want to find out about all the products available in their language for decision-making. Following the approach of Wrede et al. [44], we, therefore, examine not only a country-specific market, in contrast to various previous studies in the field of cyber insurance coverage [17,50,51]. Wrede et al. [44] analyzed corporate cyber insurance in the DACH region (Germany, Austria, and Switzerland) by including silent cyber coverage of traditional insurance stand-alone policies. Adapted to consumer cyber insurances, besides stand-alone policies (SAI), we examine German-language liability insurance (LYI) policies, legal protection insurance (LPI) policies, and household insurance (HOI) available for private households. Therefore, we identified insurers from the databases of the German Federal Financial Supervisory Authority (BaFin), Swiss Financial Market Supervisory Authority (FINMA), and Financial Market Authority for Austria (FMA) by using the PRISMA method for the systematic selection of research objects [52]. All three databases were filtered according to various criteria. First, death funds, pension funds, life insurers, discontinuing companies, and insurers outside the DACH region were excluded since they do not offer private insurance that could cover cyber risks. Apart from excluding insurers by filtering and removing duplicates in the databases, eight further (non-)established "insurers" were added via search engines to avoid sampling bias. Thus, it was possible to identify 133 insurers and their 281 consumer cyber insurance policies (Figure 1). Similar to Wrede et al. [44], those insurance policies (and in our study also product information sheets) were analyzed using the MAXQDA analysis software. However, contrary to Wrede et al. [44], a content analysis according to Kuckartz [53] was used methodically for the inductive formation of the code system, which offers the advantage of a more iterative approach with several cycles.

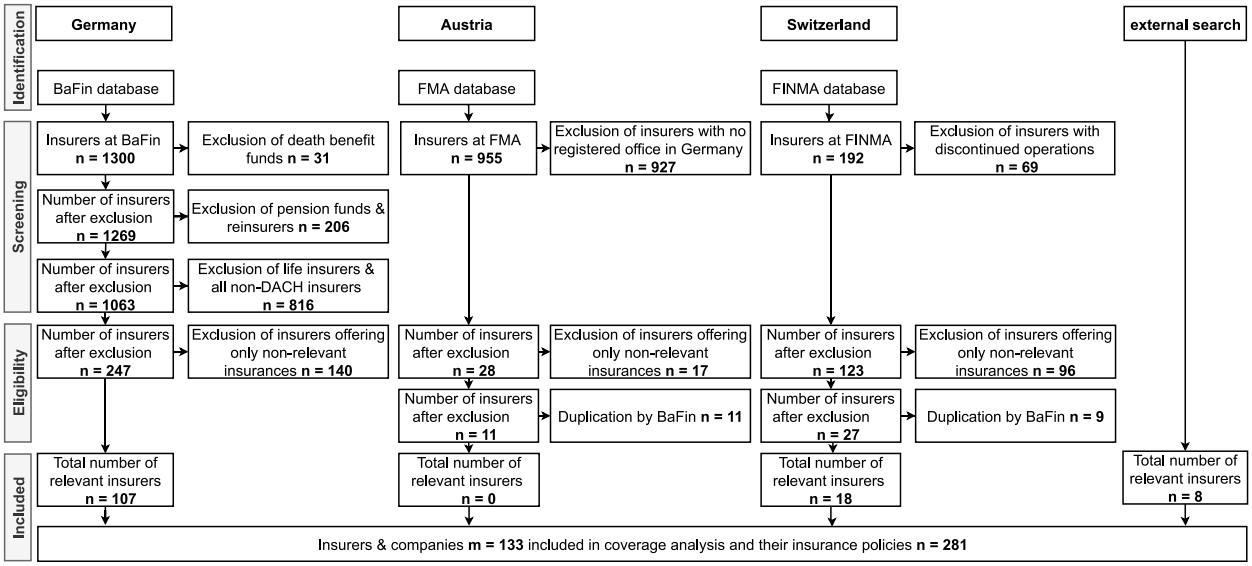

Figure 1. Flow diagram of the selection process based on Moher et al. (2009)

4. Results

Resulting from the analysis, Table 1 shows the scope of coverage for the consumer segment and provides an overall view of insurance options for cyber risks ranging from stand-alone insurances (SAI) to traditional insurances (LYI, LPI, HOI). For each of the four insurance products, we have indicated how the distribution occurs in absolute and relative terms compared with the total amount of the particular coverage. In addition to the distinction between (1) first-party and (2) third-party coverage described initially, we divide the identified coverage into two different categories: (3) legal services and (4) IT assistance services. Many financially severe losses (e.g., online shopping fraud, identity theft, reputational damage) caused by cyber risks are covered mainly in the SAIs – except for the unintentional transmission of malware in the case of LYI. Moreover, despite their coverage focus, LPIs are not truly superior to SAIs in all legal services (especially in the case of legal protection in the event of identity theft). SAIs are

distinguished from traditional insurance products such as LYI, LPI, and HOI, especially by IT assistance services, which primarily comprise preventive security measures such as the provision of antivirus software or data safes. Our results show that by excluding or not mentioning the scope of coverage in the insurance terms and conditions makes many traditional insurance policies only partially suitable for consumers in terms of cybercrime.

Table 1. Overview of the cyber coverage and their frequencies in consumer cyber insurance policies in the DACH region

ID	Coverage	SAI	LYI	LPI	HOI	n
1	First party					
1.1	Compensation for losses on internet purchases/sales	26 *(63.41%)*	1 *(2.44%)*	3 *(7.32%)*	11 *(26.83%)*	41
1.2	Identity abuse	28 *(47.46%)*	1 *(1.69%)*	9 *(15.25%)*	21 *(35.59%)*	59
1.3	Replacement costs of payment cards and ID documents	15 *(53.57%)*	8 *(28.57%)*	0	5 *(17.86%)*	28
1.4	Bank account/card blocking service	11 *(68.75%)*	0	1 *(6.25%)*	4 *(25%)*	16
1.5	Data recovery	20 *(39.22%)*	2 *(3.92%)*	1 *(1.96%)*	28 *(54.90%)*	51
1.6	Initial psychological counseling	27 *(65.85%)*	3 *(7.32%)*	8 *(19.51%)*	3 *(7.32%)*	41
1.7	Delete personal & misused data	23 *(56.1%)*	10 *(24.39%)*	5 *(12.2%)*	3 *(7.32%)*	41
2	Third party					
2.1	Unintentional transmission of malware	4 *(7.55%)*	49 *(92.45%)*	0	0	53
2.2	Violation of data protection regulations	4 *(100%)*	0	0	0	4
2.3	Violation of copyright regulations	4 *(40%)*	1 *(10%)*	4 *(40%)*	1 *(10%)*	10
2.4	Violation of confidentiality regulations	2 *(100%)*	0	0	0	2
2.5	Compensation in the event of cyberbullying by co-insureds	3 *(33.33%)*	1 *(11.11%)*	5 *(55.56%)*	0	9
3	Legal services					
3.1	Initial legal advice	17 *(56.67%)*	1 *(3.33%)*	12 *(40%)*	0	30
3.2	Legal protection in case of copyright infringement claims	9 *(64.29%)*	0	4 *(28.57%)*	1 *(7.14%)*	14
3.3	Legal protection in case of damage claims	5 *(31.25%)*	0	10 *(62.5%)*	1 *(6.25%)*	16
3.4	Legal protection in case of prosecutions	5 *(41.67%)*	0	7 *(58.33%)*	0	12
3.5	Active legal protection in case of identity theft or damage to reputation	6 *(85.71%)*	0	0	1 *(14.29%)*	7
3.6	Digital inheritance	2 *(18.18%)*	1 *(9.09%)*	7 *(63.64%)*	1 *(9.09%)*	11
4	IT assistance services					
4.1	IT-specific consultation	9 *(81.82%)*	0	1 *(9.09%)*	1 *(9.09%)*	11
4.2	Monitoring platform	16 *(84.21%)*	0	1 *(5.26%)*	2 *(10.53%)*	19
4.3	Data safe	5 *(55.56%)*	1 *(11.11%)*	0	3 *(33.33%)*	9
4.4	Antivirus software	7 *(100%)*	0	0	0	7

5. Discussion

During the COVID-19 pandemic, consumers were more affected by cybercrime (e.g., identity theft, malware) than businesses [7]. While businesses have been limiting their residual cyber risks through cyber insurance for several years, this way of transferring risk at the consumer level is still largely unexplored. Cyber insurance allows consumers to protect themselves from the consequences of cybercrime even when many technical, human, and organizational approaches to information security fail. We intend to deliver both practical and theoretical implications.

5.1. Implications for Research

In distinction to other insurance products, e.g., health insurance, we show that consumer cyber insurance has some peculiarities that interest research in multiple ways. First, we show that consumer cyber insurance inevitably differs from corporate cyber insurance in several terms of coverage, such as IP theft or business interruption [44]. Based on

Franke and Meland [26] and Skarczinski et al. [54], contrary to corporate cyber insurance, we conclude that not only insurance coverage but also the underlying adoption decision-making of private and corporate decision-makers differs.

According to our coverage analysis, cyber risks have so far only been considered in cyber insurance policies as monetary compensation for attempted data recovery, without considering the value of the damaged or lost data. This gives rise to new research approaches for the study of insurance-related phenomena such as moral hazard and adverse selection, which may differ given the underlying IT artifact of the internet and its cyber-specific challenges in case of personal data loss. Although there are various overlaps with the concept of personal identity insurance in terms of coverage, such as attorney fees or mental health counseling [50], consumer cyber insurance takes an even more holistic approach to the transfer of cyber risks, e.g., data recovery costs or compensation for losses on internet purchases/sales.

Researchers should be aware of various synonyms we have identified for cyber insurance in the corporate sector. As a result of merging existing definitions and our latest findings, we introduce the following novel definition for further research in the consumer sector: Consumer cyber insurance (CCI) is the term used to describe insurance products in the private customer segment that cover a range of technical, legal, or psychological cyber risks and are thus intended to protect consumers from financial hardship as well as emotional distress resulting from the use of internet technologies. Besides (preventive) legal and assistance services, consumer cyber insurances aim to cover first- and third-party costs in the event of cyber incidents and to ward off unjustified third-party claims. In addition to stand-alone policies, consumer cyber insurance can also be found affirmative or non-affirmative in traditional consumer insurance lines such as liability insurance, legal protection insurance, and household insurance.

5.2. Implications for Practice

We help the consumers better understand the highly diversified market for CCI policies and its cyber-specific characteristics (e.g., data loss besides typical financial loss) compared to traditional products such as a car or health insurance. Our findings can guide consumers in their decision-making about CCI. Based on the devices (e.g., tablets) as well as the applications (e.g., social media) used by the particular consumer, a needs-based, risk-by-risk cyber insurance policy can then be identified to, e.g., trigger deletion and prosecution in the likely event of posts that are damaging to personal reputation. Specifically, consumers can benefit from our coverage overview if their insurance agent uses it as a tool in the consultation process. Furthermore, our findings help the insurance industry (i.e., claims adjusters, underwriters, insurers, brokers) to have a common understanding of CCI products and optimize CCI continuously (e.g., coverage, size of premiums, advice, service). This is crucial for insurers to sell these complex but value-adding products on the demand side in simple language.

5.3. Limitations and future work

A limitation of this study relates to the sampling of CCI policies to be investigated, which in this case originate exclusively from the whole DACH region. Although the selection bias has been reduced compared to previous studies, following Woods [50], a further expansion of the insurance markets under study appears beneficial.

Based on the findings of this paper, further research is also needed to determine whether the CCI products currently available on the market cover the diverse and dynamically changing cyber risks of consumers. Knowing that there is a high number of unreported cases in the field of cybercrime, a comparison with the crime statistics of the federal and state governments could be made for an initial estimation of the necessary coverage of current cyber risks.

Also, our paper lays the groundwork for subsequent research that examines the impact of relationships between CCIs on consumers. In particular, discussions on the reasons for adopting consumer cyber insurance are of strong interest. Apart from coverage, insurance products can also be distinguished by directly observable or indirectly existing features such as premium setting strategy, premium payment, claim handling, and insurer solvency [55]. Therefore, the study of its cyber-specific features must first be expanded for consumer research related to cyber insurance.

Thereby, research questions arise that empirically investigate the adoption of CCI and the possibly changed risk behavior after taking out CCI. This allows us to contribute to cyber risk IS research (e.g., consumer risk assessment method) and bridge the gap to cyber insurance economics research (e.g., effects like moral hazard, adverse selection). In addition to Woods [50], we suggest that a reduction in cyber risk exposure would be possible through a mandatory competency-based cyber risk assessment before taking out CCI, which thus could lead to higher cyber risk awareness.

6. Conclusion

This paper addresses the research question of *which currently available insurance products can cover consumer cyber losses*. We contribute to cyber insurance research by investigating the coverage options for cyber risks for private households. Consumers can choose the most convenient CCI for them based on their cyber risk profile (e.g., occasional internet users, or frequent surfers). Thereby, our study delivers empirical evidence on the significant deficiencies in the coverage of cyber losses based on traditional insurance lines. Instead, only consumer cyber insurance in the form of stand-alone policies covers the broadest possible range of current cyber risks.

To conclude, although consumer cyber insurance is still in its infancy in terms of both research and practice, this insurance product appears worthy of research given the recent highly dynamic market development in the corporate sector. Given the increasing cyber risks for private households, which can vary depending on their internet usage habits (cf. devices, apps, etc.), the demand for such policies will most likely increase. We, therefore, see this paper as a first and, at the same time, a meaningful step towards transferring this emerging cyber insurance approach valued by companies into private households. This paper serves as an impulse for future improvement of CCI.

References

[1] Zheng Y, Wei D, Li J, Zhu T, Ning H. Internet Use and Its Impact on Individual Physical Health. *IEEE Access* 2016;**4**:5135–5142, doi:10.1109/ACCESS.2016.2602301.

[2] Kumar N, Chaudhary P. Minimize Cyber Losses in Cyber World through the Optimization Technique. *International Journal of Computer Applications* 2014;**96**(20):18–22, doi:10.5120/16910-6993.

[3] International Telecommunication Union (ITU). *Measuring digital development: Facts and figures 2021*. Available at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf; 2021 [accessed 28.08.2022].

[4] Kurniawati MA. Analysis of the impact of information communication technology on economic growth: empirical evidence from Asian countries. *Journal of Asian Business and Economic Studies* 2022;**29**(1):2–18, doi:10.1108/JABES-07-2020-0082.

[5] Fiorillo A, Sampogna G, Giallonardo V, Del Vecchio V, Luciano M, Albert U, et al. Effects of the lockdown on the mental health of the general population during the COVID-19 pandemic in Italy: Results from the COMET collaborative network. *European Psychiatry* 2020;**63**(1):1–11, doi:10.1192/j.eurpsy.2020.89.

[6] Shillair R, Cotten SR, Tsai H-YS, Alhabash S, LaRose R, Rifon NJ. Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior* 2015;**48**:199–207, doi:10.1016/j.chb.2015.01.046.

[7] Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S, Díaz-Castaño N. Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies* 2021;**23**(1):47–59, doi:10.1080/14616696.2020.1804973.

[8] Dreißigacker A, Skarczinski B von, Bergmann MC, Wollinger GR. Cyberangriffe gegen private Internetnutzer*innen. In: Rüdiger T-G, Bayerl PS, editors. *Cyberkriminologie*. Wiesbaden: Springer Fachmedien Wiesbaden; 2020, p. 319–344.

[9] Bolot J, Lelarge M. Cyber Insurance as an Incentive for Internet Security. In: Johnson ME, editor. *Managing information risk and the economics of security*. New York, NY: Springer; 2009, p. 269–290.

[10] Allianz Global Corporate & Specialty (AGCS). *Allianz Risk Barometer: Identifying the major business risks for 2020*. Munich; 2020.

[11] Horten B, Gräber M. Cyberkriminalität. *Forensische Psychiatrie, Psychologie, Kriminologie* 2020;**14**(3):233–241, doi:10.1007/s11757-020-00605-0.

[12] European Insurance and Occupational Pensions Authority (EIOPA). *Understanding Cyber Insurance: A Structured Dialogue with Insurance Companies*. Luxembourg: Publications Office of the EU; 2018.

[13] Monteith S, Bauer M, Alda M, Geddes J, Whybrow PC, Glenn T. Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current psychiatry reports* 2021;**23**(18):1–9, doi:10.1007/s11920-021-01228-w.

[14] Sukwong O, Kim H, Hoe J. Commercial Antivirus Software Effectiveness: An Empirical Study. *Computer* 2011;**44**(3):63–70, doi:10.1109/MC.2010.187.

[15] European Network and Information Security Agency (ENISA). *Commonality of risk assessment language in cyber insurance: Recommendations on Cyber Insurance*. Heraklion; 2017.

[16] Strupczewski G. Current state of the cyber insurance market. In: *Proceedings of the 10th Economics & Finance Conference, Rome:* International Institute of Social and Economic Sciences; 2018.

[17] Romanosky S, Ablon L, Kuehn A, Jones T. Content analysis of cyber insurance policies: how do carriers price cyber risk? *Journal of Cybersecurity* 2019;**5**(1):1–19, doi:10.1093/cybsec/tyz002.

[18] Bitkom. *Können Sie sich vorstellen, eine Versicherung abzuschließen, um sich bei kriminellen Vorfällen im Internet abzusichern?* Available at: https://de.statista.com/statistik/daten/studie/760322/umfrage/versicherung-gegen-cybercrime-schaeden-in-deutschland/; 2017 [accessed 28.08.2022].

[19] Smidt G de, Botzen W. Perceptions of Corporate Cyber Risks and Insurance Decision-Making. *The Geneva Papers on Risk and Insurance - Issues and Practice* 2018;**43**(2):239–274, doi:10.1057/s41288-018-0082-7.

[20] Zeller G, Scherer M. A comprehensive model for cyber risk based on marked point processes and its application to insurance. *European Actuarial Journal* 2021;**12**:33–85, doi:10.1007/s13385-021-00290-1.

[21] Biener C, Eling M, Matt A, Wirfs JH. *Cyber risk: Risikomanagement und Versicherbarkeit*. St. Gallen: Institut für Versicherungswirtschaft der Universität St. Gallen; 2015.

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

doi:10.1108/JRF-09-2016-0122.
[23] Böhme R, Kataria G. On the Limits of Cyber-Insurance. *Lecture Notes in Computer Science* 2006;**4083**:31–40, doi:10.1007/11824633_4.
[24] Oğüt H, Raghunathan S, Menon N. Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis* 2011;**31**(3):497–512, doi:10.1111/j.1539-6924.2010.01478.x.
[25] Cebula JJ, Popeck ME, Young LR. *A Taxonomy of Operational Cyber Security Risks Version 2:* Carnegie Mellon University Software Engineering Institute; 2014.
[26] Franke U, Meland PH. Demand side expectations of cyber insurance. In: *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA):* IEEE; 2019, p. 1–8.
[27] Xie X, Lee C, Eling M. Cyber insurance offering and performance: an analysis of the U.S. cyber insurance market. *The Geneva Papers on Risk and Insurance - Issues and Practice* 2020;**45**(4):690–736, doi:10.1057/s41288-020-00176-5.
[28] Bahşi H, Franke U, Friberg EL. The cyber-insurance market in Norway. *Information & Computer Security* 2019;**28**(1):54–67, doi:10.1108/ICS-01-2019-0012.
[29] Xu M, Hua L. Cybersecurity Insurance: Modeling and Pricing. *North American Actuarial Journal* 2019;**23**(2):220–249, doi:10.1080/10920277.2019.1566076.
[30] Böhme R, Schwartz G. Modeling Cyber-Insurance: Towards A Unifying Framework. In: *Proceedings of the 9th Workshop on the Economics of Information Security (WEIS 2010)*. Cambridge, USA: Harvard University; 2010, p. 1–36.
[31] Elnagdy SA, Qiu M, Gai K. Cyber Incident Classifications Using Ontology-Based Knowledge Representation for Cybersecurity Insurance in Financial Industry. In: *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing:* IEEE; 2016, p. 301–306.
[32] Sigholm J, Larsson E. Cyber Vulnerability Implantation Revisited. *MILCOM 2021* 2021:464–469, doi:10.1109/MILCOM52596.2021.9652921.
[33] Böhme R. IT-Risiken im Schadenversicherungsmodell: Implikationen der Marktstruktur. In: Federrath H, editor. *Sicherheit 2005: Haupttagung "Sicherheit - Schutz und Zuverlässigkeit"; Workshop "Qualifizierte elektronische Signaturen in Theorie und Praxis" (QSIG 2005); Beiträge der 2. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 5.-8. April 2005 in Regensburg*. 1st ed. Bonn: Ges. für Informatik; 2005.
[34] Tonn G, Kesan JP, Zhang L, Czajkowski J. Cyber risk and insurance for transportation infrastructure. *Transport Policy* 2019;**79**:103–114, doi:10.1016/j.tranpol.2019.04.019.
[35] Lemnitzer JM. Why cybersecurity insurance should be regulated and compulsory. *Journal of Cyber Policy* 2021;**6**(2):118–136, doi:10.1080/23738871.2021.1880609.
[36] Marotta A, Martinelli F, Nanni S, Orlando A, Yautsiukhin A. Cyber-insurance survey. *Computer Science Review* 2017;**24**:35–61, doi:10.1016/j.cosrev.2017.01.001.
[37] Kshetri N. The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy* 2020;**44**(8):27402-6165, doi:10.1016/j.telpol.2020.102007.
[38] Gordon LA, Loeb MP, Sohail T. A framework for using insurance for cyber-risk management. *Communications of the ACM* 2003;**46**(3):81–85, doi:10.1145/636772.636774.
[39] Kuru D, Bayraktar S. The effect of cyber-risk insurance to social welfare. *Journal of Financial Crime* 2017;**24**(2):329–346, doi:10.1108/JFC-05-2016-0035.
[40] Bentz TH. Is Your Cyber Liability Insurance Any Good? A Guide for Banks to Evaluate Their Cyber Liability Insurance Coverage. *North Carolina Banking Institute* 2017;**21**(1):39–53.
[41] Low P. Insuring against cyber-attacks. *Computer Fraud & Security* 2017;**2017**(4):18–20, doi:10.1016/S1361-3723(17)30034-9.
[42] Trang MN. Compulsory Corporate Cyber-Liability Insurance Outsourcing Data Privacy Regulation to Prevent and Mitigate Data Breaches-annotated. *Minnesota Journal of Law,* 2017;**18**(1):389–425.
[43] Bodin LD, Gordon LA, Loeb MP, Wang A. Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy* 2018;**37**(6):527–544, doi:10.1016/j.jaccpubpol.2018.10.004.
[44] Wrede D, Stegen T, Graf von der Schulenburg J-M. Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the German insurance market. *The Geneva Papers on Risk and Insurance - Issues and Practice* 2020;**45**(4):657–689, doi:10.1057/s41288-020-00183-6.
[45] Organisation for Economic Cooperation and Development (OECD). *Supporting an effective cyber insurance market: OECD report for the G7 Presidency*; 2017.
[46] Risk Management Solutions. *Managing Cyber Insurance Accumulation Risk: Report prepared in collaboration with and based on original research by the Centre for Risk Studies*. University of Cambridge; 2016.
[47] Labunets K, Pieters W, van Eeten M, Branley-Bell D, Coventry L, Briggs P, et al. The Cyber Insurance Landscape. In: Ríos Insua D, Baylon C, Vila J, editors. *Security risk models for cyber insurance*. Boca Raton: Chapman & Hall/CRC; 2020, p. 11–26.
[48] Piquero NL, Cohen MA, Piquero AR. How Much is the Public Willing to Pay to be Protected from Identity Theft? *Justice Quarterly* 2011;**28**(3):437–459, doi:10.1080/07418825.2010.511245.
[49] Lynch J. Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. *Berkeley Technology Law Journal* 2005;**20**(1):259–300.
[50] Woods DW. Quantifying Privacy Harm via Personal Identity Insurance. *SSRN Electronic Journal* 2021, doi:10.2139/ssrn.3984005.
[51] Franke U. The cyber insurance market in Sweden. *Computers & Security* 2017;**68**:130–144, doi:10.1016/j.cose.2017.04.010.
[52] Moher D, Liberati A, Tetzlaff J, Altman DG. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *The BMJ* 2009;**339**(b2535):1-8, doi:10.1136/bmj.b2535.
[53] Kuckartz U. Qualitative Text Analysis: A Systematic Approach. In: Kaiser G, Presmeg N, editors. *Compendium for early career researchers in mathematics education*. Cham: Springer International Publishing; 2019, p. 181–197.
[54] Skarczinski BS von, Boll L, Teuteberg F. Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side. *ECIS 2021 Research Papers* 2021;(72):1–19.
[55] Schlesinger H, Schulenburg JMG von der. Search Costs, Switching Costs and Product Heterogeneity in an Insurance Market. *Journal of Risk and Insurance* 1991;**58**(1):109–119, doi:10.2307/3520051.