European Actuarial Journal (2020) 10:303–333
https://doi.org/10.1007/s13385-020-00250-1

SURVEY PAPER

Cyber risk research in business and actuarial science

Martin Eling[1]

Received: 11 August 2020 / Revised: 26 September 2020 / Accepted: 30 September 2020 /
Published online: 14 October 2020

Abstract
We review the academic literature on "cyber risk" and "cyber insurance" in the fields of business (management, economics, finance, risk management and insurance) and actuarial science. Our results show that cyber risk is an increasingly important research topic in many disciplines, but one that so far has received little attention in business and actuarial science. Business research has documented the manifold detrimental effects of cyber risks using event studies and scenario analyses, while economic research is especially concerned with trade-offs between different risk management activities. Quantitative research including papers published in actuarial journals mainly focuses on loss modelling, especially taking dependencies and network structure into account. We categorize the empirical literature on cyber risk to filter out what we know on the frequency, severity and dependence structure of cyber risk. Finally, we list open research questions which demonstrate that cyber risk research is still in its infancy and that there is ample room for future research.

Keywords Cyber risk · Cyber insurance · Event studies · Dependence modelling · Network modelling

1 Cyber risk research in business and actuarial science

1.1 Motivation

Cyber risks are operational risks to information and technology assets that have consequences for the confidentiality, availability, and integrity of information and information systems (Cebula and Young [16]). Despite its increasing relevance for businesses and society, research on cyber risk remains very limited. Some papers have been published in the computer science domain, but little research has been done in the fields of business and actuarial science. Existing articles emphasize the lack of data and modelling challenges (e.g., Maillart and Sornette [54]; Biener et al.

✉ Martin Eling
martin.eling@unisg.ch

[1] University of St. Gallen, St. Gallen, Switzerland

[10]), the complexity and dependent risk structure (e.g., Hofmann and Ramaj [44]), and adverse selection and moral hazard problems (e.g., Gordon et al. [40]). More applied research is concerned with the potentially huge losses from worst-case scenarios such as the breakdown of critical infrastructure (e.g., World Economic Forum [82]; Lloyd's [52]; Long Finance [35]). The literature thus highlights challenges in the risk management and insurability of cyber risks.

The intention of this paper is to review the academic literature on "cyber risk" and "cyber insurance" in the fields of business (i.e. journals in the field of management, economics, finance, risk management and insurance) and actuarial science. The results document that cyber risk is an increasingly important research topic in many disciplines,[1] but still has received scant attention in the business and actuarial science literature to date; we also document that research efforts have been stymied by interdisciplinary barriers (e.g., Falco et al. [34]). In the field of risk management, insurance and actuarial science, leading journals (such as the *Journal of Risk and Insurance*, *Insurance: Mathematics and Economics*) have published a few articles on aspects of risk modelling, while in general interest journals (e.g., *American Economic Review*, *Journal of Finance*) the topic is not mentioned. Our results show that the literature in business and actuarial science is policy-oriented and that a lot of work has been published by institutions such as Lloyd's, Cambridge Risk Center or the World Economic Forum to increase the awareness of the economic and societal relevance of the topic.

The remainder of this article is structured as follows. In Sect. 2 we present our search strategy. Section 3 shows the search results structured in business and actuarial science. Here we also review the empirical literature on cyber risk and filter out what we know about the frequency, severity and dependence structure of cyber risk. Finally, we provide conclusions and an outlook on potential future research questions in Sect. 4.

2 Search strategy

To identify the papers to be included in literature review, we screened the academic literature with the keywords "cyber risk" and "cyber insurance" in a structured search process implemented on March 30, 2020. In a first step the Web of Science was consulted, providing 217 hits for "cyber risk" and 95 for "cyber insurance". Figure 1 shows that most of these hits come from the field of computer science, indicating that cyber risk is not a new research topic, but has been an evergreen computer science research topic in information security (see "Appendix B" for visualization treemap for "cyber insurance"). We also find, however, 48 papers from the fields of

[1] As shown in "Appendix A", research on cyber risk and cyber insurance was scarce until 2010, but since then it has grown exponentially, emphasizing the increasing practical and academic relevance of the topic. We also note a number of working parties studying cyber risk from a more applied perspective for professional organizations, such as the Society of Actuaries (SOA), the International Actuarial Association (IAA) or the Canadian Institute of Actuaries.

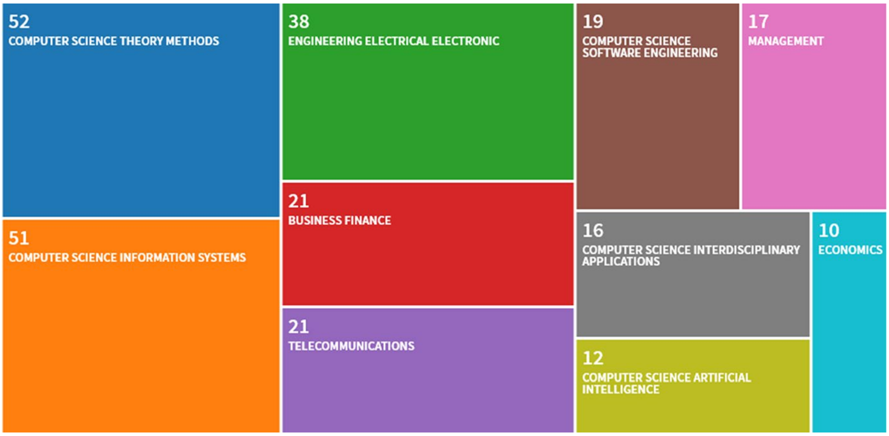

Fig. 1 Visualization treemap for 217 papers on "cyber risk" in the Web of Science as of March 30, 2020

finance, management and economics, emphasizing the increasing relevance of cyber risks in these academic fields.

We then screen the top journals in the fields of business (management, economics, finance, risk management and insurance) and actuarial science (Table 1).[2] The results show that the topic is virtually absent in the top journals in the fields of finance, economics, and even in the field of risk management and insurance.[3] Actuarial science is more receptive to the new research topic, given that most of the top actuarial journals have already published two or three articles on cyber risk.

Table 2 lists the papers which are included in the literature review. Panels A and B show the 10 most-cited papers in the fields of "cyber risk" and "cyber insurance" from the Web of Science. Panel C presents the papers identified in Table 1, i.e. all papers published in the top journals in business and actuarial science. This adds up to a selection of 40 academic papers published from 2003 to 2020.[4]

3 Search results

We start our review with a short description of the three most widely cited articles on cyber risk in the Web of Science: Gordon et al. [40], Mukhopadhay et al. [58], and

[2] The selection of journals in management, finance and economics is based on the journal ranking of the German Academic Association of Business Research (VHB-Jourqual 3; see https://vhbonline.org/vhb4you/vhb-jourqual). The journals are presented in alphabetical order.

[3] The only exception is the *Geneva Papers on Risk and Insurance* which published a special issue on cyber risk in 2018 and will publish another special issue this year.

[4] The search strategy certainly has limitations, so our selection of papers should not necessarily be considered comprehensive. One example is that articles that do not contain the words "cyber risk" or "cyber insurance" in the title, abstract or key words are not included in the list. One example is the often-cited article on data breaches by Romanonsky et al. [66]. Still the selection of papers should provide a good overview of research in the different fields.

Table 1 Results of literature review

Field	Journals	Hits
Management	Academy of Management Journal (AMJ)	0
	Administrative Science Quarterly (ASQ)	0
	Academy of Management Review (AMR)	0
	Management Science (MS)	1
	Science	2
Economics	American Economic Review (AER)	0
	Econometrica	0
	Journal of Political Economy (JPE)	0
	Quarterly Journal of Economics (QJE)	0
	Review of Economic Studies (RES)	0
Finance	Journal of Finance (JF)	0
	Journal of Financial and Quantitative Analysis (JFQA))	0
	Journal of Financial Economics (JFE)	1
	Review of Financial Studies (RFS)	0
	Review of Finance (RoF)	0
Risk Management and Insurance	Geneva Papers on Risk and Insurance (GPRI)	5
	Geneva Risk and Insurance Review (GRRI)	0
	Journal of Insurance Issues (JII)	1
	Journal of Risk and Insurance (JRI)	0
	Journal of Risk and Uncertainty (JRU)	1
	Risk Management and Insurance Review (RMIR)	2
	Risks	2
Actuarial Science	ASTIN Bulletin (AB)	2
	British Actuarial Journal (BAJ)	2
	European Actuarial Journal (EAJ)	0
	Insurance: Mathematics and Economics (IME)	3
	North American Actuarial Journal (NAAJ)	2
	Scandinavian Actuarial Journal (SAJ)	0

Biener et al. [10].[5] Starting with these three papers is also a useful way to develop a playing field of problem areas and topics that are important for cyber risk and cyber insurance research. We present the literature in three subchapters. First, we discuss results from the field of business (i.e., management, economics, finance,

[5] Bai [5] focuses on sentiment analysis from online texts and is the only one in the set of 40 articles that is just loosely related to the topic of cyber risk. The author proposes a Markov blanket model to capture dependencies among words and provide a vocabulary for extracting sentiments. The advantages of their approach compared to other state-of-the-art algorithms for sentiment analysis is illustrated in two applications (online movie reviews, online news). The article is included in the review, because the authors position their tool not only to gauge online customers' preferences for economic or marketing research, but also for detecting cyber risk and security threats.

Table 2 Results of literature review

Paper	Authors	Title	Year	Citations/Journal*
Panel A: Top 10 cited papers from the Web of Science—Search term “cyber risk”				
1	Bai [5]	Predicting consumer sentiments from online text	2011	88
2	Gordon et al. [40]	A framework for using insurance for cyber-risk management	2003	67
3	Biener et al. [10]	Insurability of cyber risk: an empirical analysis	2015	45
4	Mukhopadhyay et al. [58]	Cyber-risk decision models: to insure IT or not?	2013	35
5	McQueen et al. [57]	Time-to-compromise model for cyber risk reduction estimation	2006	21
6	Shackelford [71]	Should your firm invest in cyber risk insurance?	2012	14
7	Vishwanath et al. [79]	Suspicion, cognition, and automaticity model of phishing susceptibility	2016	14
8	Eling and Schnell [29]	What do we know about cyber risk and cyber risk insurance?	2016	13
9	Gai et al. [37]	A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance	2016	13
10	Dondossola et al. [22]	Cyber risk assessment of power control systems—a metrics weighed by attack experiments	2011	13
Panel B: Top 10 cited papers from the Web of Science- Search term “cyber insurance”				
11	Biener et al. [10]	Insurability of cyber risk: an empirical analysis	2015	45
12	Mukhopadhyay et al. [58]	Cyber-risk decision models: to insure IT or not?	2013	35
13	Hoang et al. [43]	Charging and discharging of plug-in electric vehicles (PEVs) in vehicle-to-grid (V2G) systems: a cyber insurance-based Model	2017	32
14	Bandyopadhyay et al. [6]	Why IT managers don’t go for cyber-insurance products	2009	30
15	Pal et al. [62]	Will cyber-insurance improve network security? A market analysis	2014	29
16	Shetty et al. [72]	Competitive cyber-insurance and internet security	2010	24
17	Romanosky [64]	Examining the costs and causes of cyber incidents	2016	20
18	Marotta et al. [56]	Cyber-insurance survey	2017	17
19	Srinidhi et al. [75]	Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors	2015	17
20	Johnson et al. [49]	Security Games with Market Insurance	2011	16
Panel C: Results on Review Focused on Business and Actuarial Science				
21	Jevtić and Lanchier [48]	Dynamic structural percolation model of loss distribution for *cyber risk* of small and medium-sized enterprises for tree-based LAN topology	2020	IME
22	Eling and Loperfido [27]	Data breaches: goodness of fit, pricing, and risk measurement	2017	IME

Table 2 (continued)

Paper	Authors	Title	Year	Citations/Journal*
23	Eling and Jung [26]	Copula approaches for modeling cross-sectional dependence of data breach losses	2018	IME
24	Eling and Schnell [30]	Capital requirements for cyber risk and cyber risk insurance: an analysis of solvency II, the US Risk-Based Capital Standards, and the Swiss Solvency Test	2019	NAAJ
25	Xu and Hua [83]	Cybersecurity insurance: modeling and pricing	2019	NAAJ
26	Egan et al. [24]	Cyber operational risk scenarios for insurance companies	2019	BAJ
27	Cartagena et al. [14]	Silent cyber assessment framework	2020	BAJ
28	Fahrenwaldt et al. [33]	Pricing of cyber insurance contracts in a network model	2018	AB
29	Kamiya et al. [50]	Risk management, firm reputation, and the impact of successful cyberattacks on target firms	In press	JFE
30	August et al. [4]	Market segmentation and software security: pricing patching rights	2019	MS
31	Marotta and McShane [55]	Integrating a proactive technique into a holistic cyber risk management approach	2018	RMIR
32	Hovav and D'Arcy [46]	The impact of denial-of-service attack announcements on the market value of firms	2003	RMIR
33	Eling and Zhu [32]	Which insurers write cyber insurance? Evidence from the US property and casualty insurance industry	2018	JII
34	Biener et al. [10]	Insurability of cyber risk: an empirical analysis	2015	GPRI
35	Ashby et al. [2]	Emerging IT risks: insights from german banking	2018	GPRI
36	Pooser et al. [63]	Growth in the perception of cyber risk: evidence from US P&C Insurers	2018	GPRI
37	Shetty et al. [73]	Reducing informational disadvantages to improve cyber risk management	2018	GPRI
38	de Smidt and Botzen [20]	Perceptions of corporate cyber risks and insurance decision-making	2018	GPRI
39	Anderson and Moore [1]	The economics of information security	2006	Science
40	Falco et al. [34]	Cyber risk research impeded by disciplinary barriers	2019	Science
41	Bentley et al. [7]	A multivariate model to quantify and mitigate cybersecurity risk	2020	Risks
42	Dal Moro [19]	Towards an economic cyber loss index for parametric cover based on IT security indicator: a preliminary analysis	2020	Risks

For Panels A and B, the column reports the number of citations in the Web of Science as of March 30, 2020, for Panel C the name of the journal (see Table 1 for abbreviations). The articles are ordered according to number of citations in Panels A and B and according to journals in Panel C

Table 3 Research fields and research topics summarized in the literature review

Business research	Quantitative research/actuarial science
Event studies	Loss modelling
Scenario analyses	Modelling of dependence
Economic analysis of externalities	Modelling of network structure

risk management and insurance). Then, we present quantitative research results, especially from the field of actuarial science. Finally, to encourage future empirical research, we summarize what is known from empirical studies on the frequency, severity and dependence structure, not limited to a particular discipline (Table 5). Table 3 summarizes the main research topics from our literature review across the two fields.

Gordon et al. [40] develop a framework for cyber risk management, including insurance. They discuss the limitations of current cyber risk management and the challenges in implementing cyber insurance, which are especially the lack of data for pricing, adverse selection and moral hazard. The authors emphasize that there is a trade-off between the amount of money that should be spent on cybersecurity and the amount of money used to buy cyber insurance. The paper by Gordon et al. [40] is also closely related to the Gordon and Loeb [39] model, which is one of the most-discussed models in information security, claiming that the optimal investment in information security should be less than or equal to 37% of the expected loss amount.

Mukhopadhay et al. [58] propose a Bayesian belief networks model with copulas to assess cyber risk. Based upon the results they also propose cyber insurance products to minimize the financial loss of security breaches and to complement existing security technology. Collective risk and utility theory is used to compute premiums for cyber insurance products. To assist cyber insurers in effective product design, the authors propose a utility-based preferential pricing model that takes into account risk profiles and wealth of the prospective insured firm before proposing the premium.

Biener et al. [10] published one of the first empirical papers in the field that uses a real loss dataset. The authors extract 994 cyber losses from the SAS operational loss database and analyze their statistical properties. Based on the results and a literature review, the authors then investigate the insurability of cyber risk by systematically reviewing the set of criteria introduced by Berliner [8]. The results emphasize the distinctive characteristics of cyber risks compared with other operational risks and illustrate significant insurability problems resulting from interrelated losses, lack of data and information asymmetries.

3.1 Business literature

In the field of business, the manifold detrimental effects of cyber risks have been analyzed, typically using event studies and scenario analyses. The results of the event studies show that the major part of the economic losses are indirect costs (i.e. the reputational damage for example through the loss of trust). Several studies investigate the effects of cyber risk incidents on companies' stock prices. For example, Cavusoglu et al. [15] show in an event study that a security breach negatively affects a company's stock price. They estimate the loss to be 2.1% of the market value or US$1.65 billion per security breach.[6] A major part of the value reduction can be explained by the reputational damage (Sinanaj and Muntermann [74]). In contrast, Campbell et al. [13] as well as Hovav and D'Arcy [46] find only limited evidence that data breaches or DoS attacks negatively influence the company's stock price. However, Campbell et al. [13] provide evidence that a breach of confidential data has a larger negative effect on the stock price than a breach of non-classified information; Hovav and D'Arcy [46] show a negative price effect for companies with an internet-based business model. It thus seems that the markets behaves rationally, as the discount is proportional to the expected loss associated with different data. Besides the sensitive customer data of a company, intellectual property such as copyrights, trademarks, industrial designs and patents also might be at stake.

In the event study literature, Kamiya et al. [50] develop a model where a firm has an optimal exposure to cyber risk. With rational, fully informed agents and no hysteresis, a successful cyberattack should not affect the target's reputation or its post-attack policies. In contrast, the authors document that when a successful attack involves the loss of personal financial information, there is also a significant loss of shareholder wealth, which is much larger than the attack's out-of-pocket costs. This shareholder wealth loss is higher when the attack decreases sales growth more, and lower when the board pays more attention to risk management before the attack. The authors also show that an attack decreases a firm's risk appetite, as it beefs up its risk management and information technology and decreases the risk-taking incentives of management. Finally, successful cyberattacks adversely affect the stock price of firms in the target's industry. Overall, the results imply that successful attacks that entail the loss of personal financial information provide adverse information about cyber risk to target firms, their stakeholders, and their competitors.

As an alternative to empirical studies and to raise awareness among policymakers, media, the public, and executives, a variety of scenarios have been proposed in the applied business literature and industry studies (see e.g., Kelly et al. [51]; Risk Management Solutions Inc. [65]; Ruffle et al. [68]). These worst-case scenarios include various incidents that lead to a disruption of critical infrastructure and thus to economic losses. One often-discussed scenario is the monocultures in software and hardware markets that result in potential loss accumulation in the wake of a cyber incident (see e.g., Eling and Schnell [29]). The projected economic effects of the scenarios show some extreme variations, ranging from 0.2 to 2% of the GDP in the year of the event. However, as the studies lack common approaches, objectives, and thematic areas, the comparability of the scenarios and a comparative economic impact analysis is not really possible (see e.g., Nikolakopoulos et al. [60]). All this leaves managers and policymakers with a vague idea on potential frequency and severity of extreme cyber risks, resulting in ambiguous risk management strategies.

[6] They also show that stock prices of information security providers increase on average in value by 1.36% or US$1.06 billion after the announcement of another company's security breach.

Economic research is especially concerned with the trade-off between different risk management activities for cyber risk. Investments in self-protection technologies such as firewalls typically have positive externalities—with the benefits of such investments spilling over onto others by reducing the levels of risk they face. The availability of insurance contracts can change the efficiencies associated with these risk spillovers, as purchasing a formal insurance contract substitutes for an individual's self-protection efforts but does not induce any of the positive spillovers associated with those efforts. Hofmann and Rothschild [45] develop a model on the insurance and self-protection decisions for a market of individuals with heterogeneous self-protection costs and risk spillovers. They show that competitive insurance markets and markets served by a perfectly price discriminating monopolist always feature over-insurance and underinvestment in self-protection relative to socially efficient levels. Insurance markets served by a non-price discriminating monopolist, in contrast, can feature too much, too little, or the socially optimal amount of insurance.

Economic research is also much concerned about potentially misaligned incentives in cybersecurity, leading to negative externalities. Systems are particularly vulnerable to failure when the person guarding them is not the one who suffers a loss when they fail; in this context Anderson and Moore [1] present applications of economic theories and ideas to practical information security problems. They first consider misaligned incentives in the design and deployment of computer systems. Next, they study the impact of network externalities: people who connect insecure devices to the internet do not bear the full consequences of their actions. They also write that the difficulty in measuring information security risks presents as another challenge.[7]

3.2 Quantitative research/actuarial science

Quantitative research including papers published in actuarial journals focuses on loss modelling, also taking dependencies and network structure into account. To outline some of the potential modelling topics, we first review four often-cited papers that model cyber risk with stochastic modelling techniques (Table 4).

Maillart and Sornette [54] study statistical properties of data breaches between 2000 and 2008. Data breaches are often considered in empirical research, because in the US mandatory data reporting requirements since the early 2000's. Their descriptive and graphical analysis reveals two distinct phases for the breach frequency over time: (1) an explosive growth up to about July 2006; and (2) a stable rate thereafter. For the breach size (severity), they find that it follows a heavy-tailed power-law

[7] Other analyses on related topics are Srinidhi, Yan and Tayi [75]; Johnson, Böhme and Grossklags [49] and Pal et al. [62]. Srinidhi, Yan and Tayi [75] show that cyber insurance has the effect of reducing managers' overinvestment in specific security-enhancing assets. Johnson, Böhme and Grossklags [49] present security games with market insurance. Pal et al. [62] ask whether cyber insurance can improve the security in a network and show that in equilibrium insurers cannot make more than zero expected profits, again questioning the insurability of cyber risk.

Table 4 Selected papers on cyber risk loss modelling

	Maillart and Sornette [54]	Edwards et al. [23]	Wheatley et al. [80]	Eling and Wirfs [31]
Data				
Type of data	Data breaches	Data breaches	Data breaches	Actual losses from cyber risks (data breaches are used as robustness test)
Dataset	Open Security Foundation's DataLossDB	Privacy Rights Clearinghouse (PRC)—Chronology of Data Breaches	Combination of Open Security Foundation's DataLossDB and PRC's Chronology of Data Breaches	Cyber incidents extracted from the SAS Global OpRisk dataset PRC's Chronology of Data Breaches
Number of observations	956	2,234	6,422	1,579 (SAS Global OpRisk) (3,327 for PRC)
Observation period	2000–Nov. 2008	Jan. 1st, 2005–Feb. 23rd, 2015	Jan. 1st, 2000–Apr. 16th, 2015	Jan. 1st, 1995–2014 (Jan. 1st, 2005–2014for PRC)
Regional focus	USA	USA	Mainly USA, with some non-US observations	Global for SAS data (USA for PRC data)
Modelling				
Methodology	Extreme Value Theory (EVT)	Bayesian Generalized Linear Model	Generalized Linear Model (GLM) for Poisson distribution, EVT with POT, additive quantile regression	GLM for Poisson and negative binomial distribution (frequency), EVT with POT + dynamic extension for severity
Modelling focus	Main: severity distribution Minor: tail analysis, frequency (descriptive and graphically), and cumulative losses	Main: severity and frequency of whole distribution Minor: analysis of tails ($\geq$ 500,000 records)	Main: severity and cumulative losses of tail events ($\geq$ 50,000 records) Minor: frequency analysis	Severity and frequency of the whole distribution and tail events Non-linear relationships and interaction effects
Results				

Table 4 (continued)

	Maillart and Sornette [54]	Edwards et al. [23]	Wheatley et al. [80]	Eling and Wirfs [31]
Main results	Explosive growth in frequency until July 2006 and stable rate thereafter Severity remained stable over time, and shows no effect for size and sector Severity follows heavy-tailed power-law distribution Faster-than-linear growth of largest data breaches with size	Neither size nor frequency dependent on time (for the whole and tail distribution) Severity is log-normally distributed, frequency negative binomial Company size is important for severity (positive relation) Malicious breaches decreased in size over time	Frequency of large events independent of time for the US, but grows for non-US Severity can be modelled by a GPD with shape $\xi \leq 0$ → maximal loss exists, and increases sub-linearly by time; tails also become heavier over time Both frequency and severity increase with firm size, and vary significantly by sector	Better information on extreme cyber events and the diversification properties of cyber risks Comprehensive empirical study on potential heavy tails and non-linear dependencies

distribution. Furthermore, they show that breach severity remained stable over time and does not depend on the organization's type (business, education, government, medical) or size. However, they find a size effect for the largest possible data breaches per event, which grow faster than linearly with company size.

Edwards et al. [23] analyze time trends for the size and frequency of malicious and negligent data breaches. Their analysis of the complete sample shows that neither size nor frequency of breaches has increased over the past years. Furthermore, they identify that the breach size is distributed log-normally and the frequency follows a negative binomial distribution (both for malicious and negligent breaches). They further show that size of malicious and negligent breaches remained constant from 2005 to 2015. For the frequency they could not observe any time effects.

Wheatley et al. [80] extend Maillart and Sornette [54] by enlarging the dataset and an extended analytical approach. Their focus is on the tail of the distribution (i.e., incidents with more than 50,000 records breached). They show that the frequency of large events is independent of time for US firms and increases over time for non-US firms. Furthermore, they show that the severity can be modelled by a Generalized Pareto Distribution (GPD) under which losses exhibit a maximal size that is increasing sub-linearly with time. The tail exponent parameter (Pareto index) decreased from 0.57 in 2007 to 0.37 in 2015, emphasizing that the large breaches grew larger (i.e., the tail became heavier) over time. Finally, their results indicate that both frequency and severity increase with company size and vary significantly by sector.

Eling and Wirfs [31] build upon and extend these papers in that they analyze the actual costs of cyber risks (instead of number of records affected by data breaches),[8] a global dataset (instead of US data only), a longer time period (1995 to date), and the whole range of cyber risks (not solely data breaches). For this purpose, the authors identify cyber losses from an operational risk database and analyze these with methods from statistics and actuarial science. They use the peaks-over-threshold method from extreme value theory to identify "cyber risks of daily life" and "extreme cyber risks". Human behavior is the main source of cyber risk and cyber risks are very different from those of other risk categories. The models can be used to yield consistent risk estimates, depending on country, industry, size, and other variables.[9]

In addition to the modelling literature presented in Table 4, a second stream of research is the literature on the dependence structure. Also, here a few papers discuss a potential correlation of cyber risk, for example on information systems or infected computers (Böhme and Kataria [11]; Herath and Herath [42]; Mukhopadhyay et al. [58]; Eling and Jung [26]; see Table 5). Only Böhme and Kataria [11] consider a broader dataset (the number of potential attacks measured by honeypots),

[8] Romanosky [64] provides a first attempt to quantify the costs of cyber events considering US data from Advisen; he mainly presents descriptive statistics that can be used to validate and verify the plausibility cyber loss estimates; moreover, he presents a logistic regression model to analyze the costs of cyber events, but for data breaches only. Furthermore, a few industry studies exist (NetDilligence [59]; Ponemon [47]) that also are of descriptive nature.

[9] Another related modelling paper is Eling and Loperfido [27] who consider the PRC dataset and use multidimensional scaling and goodness-of-fit tests to analyze the distribution of data breach information.

but they do not consider loss data and focus on the t-copula to capture potential tail dependencies. Herath and Herath [42] and Mukhopadhyay et al. [58] rely either on smaller datasets or on simulations.

Eling and Jung [26] consider 3327 data breach events from 2005 to 2016 and identify a significant asymmetric dependence of monthly losses in two cross-sectional settings: cross-industry losses in four categories by breach types (hacking, lost electronic device, unintended disclosure and insider breach) and cross-breach type losses in five categories by industry (banking and insurance, government, medical service, retail/other business and educational institution). To identify the method that best fits the dependence structure of the dataset, the authors implement copula modelling by separating the dependence into pairwise non-zero losses and zero loss arrivals. They model the former by pair copula construction (PCC) allowing for the flexible choice of copula functions, whereas the latter is modeled by Gaussian copula. The paper illustrates the usefulness of the results in two applications to risk measurement and pricing.

Related to the research topic of dependence modelling, but increasingly constituting a research field in its own right is the use of network models in cyber risk research. Fahrenwaldt et al. [33] consider the pricing of cyber insurance contracts in a network model. The spread of the cyber infection is modeled by an interacting Markov chain. Conditional on the underlying infection, the occurrence and size of claims are described by a marked point process. The authors introduce and analyze a new polynomial approximation of claims together with a mean-field approach that allows to compute aggregate expected losses and prices of cyber insurance. Numerical case studies demonstrate the impact of the network topology and indicate that higher-order approximations are indispensable for the analysis of non-linear claims.

Jevtić and Lanchier [48] propose a structural model of aggregate cyber loss distribution for small and medium-sized enterprises under the assumption of a tree-based local area network (LAN) topology. It is the first paper to present a theoretical model of an aggregate loss distribution for cyber risk in this setting. The authors contextualize the problem in the probabilistic graph-theoretical framework using percolation models. They assume that the IT network topology is represented by a random graph allowing for heterogeneous loss topology and provide instructive numerical examples. The results lead to a robust pricing mechanism for cyber risk.

Schnell [69] analyzes the dependence between cyber risk policies and considers potential systemic risk for insurance companies when portfolios of such risks are constructed. A network model represents the insurer's cyber underwriting portfolio. The network's nodes represent policies and the links the connection to each policyholder. Then, the spreading of cyber threats is simulated on this network and losses are aggregated to derive the portfolio distribution. The paper contributes to the literature by providing improved estimates for the frequency and dependence of cyber

Footnote 9 (continued)

The results show that different types of data breaches need to be modeled as distinct risk categories. For severity modeling, the log-skew-normal distribution provides promising results. The findings add to the discussion on the use of skewed distributions in actuarial modeling (Vernic [30]; Bolancé et al. [12]; Eling [25]) and provide insights for actuaries working on the implementation of cyber insurance policies.

Table 5 Selected papers on cyber risk dependence modelling

	Böhme and Kataria [11]	Herath and Herath [42]	Mukhopadhyay et al. [58]	Eling and Jung [26]
Modeling				
Data type	Honeypot data (worms and virus infection)—183,000 data points (Feb. 2003 – Sep. 2005)	Survey on number of viral infected computers and dollar loss (15 cases)	Log data from security appliances (unclear on the detail of data)	Data breaches (PRC)—3327 data points (Jan. 2005–Dec. 2016) Other data, if possible (see above)
Focus of study	Simulation-based estimation on premiums considering different correlations Empirical estimation of correlation on loss arrival	Focusing on specifying Copula-based pricing models in the actuarial aspect	Theoretical modeling by Copula-based Bayesian Belief Network (CBBN) and suggesting pricing model with utility theory	High-dimensional risk structures with Pair copula construction
Focus of Copula modeling	t-copula to model cross-firm risks	Archimedean copula (Clayton & Gumbel)	Gaussian copula with normality and linear correlation of Bayesian nodes	Pair copula construction (D-Vine, C-Vine, R-Vine) with different copulas to model dependencies
Copula-dimension	Multivariate (High-dimension)	Bivariate	Bivariate	Multivariate (High-dimension)
Evaluated dependence	Cross-attack risks Cross-industry risks	Cross-attack risks	Cross-network vulnerability dependence	Cross-attack risks Cross-industry risks
Results				
Main results	Risk-averse firms are inclined to insure risks if intra-firm correlation is high and cross-firm correlation is low Small shape parameters of t-copula worsen insurable regions, meaning stronger extreme cross-firm (industry) correlation	The marginal distributions of two variables, the number of infected computer and the dollar loss, are Weibull (non-normal) Independence assumption in cyber insurance pricing can make pricing errors substantial	Four different nodes about security elements are evaluated; the firewall is the most vulnerable By utility-based preferential pricing (UBPP), a risk-averse entity is willing to transfer its cyber risk to an insurer and pay a higher premium	Information on data breach events has been classified in the different categorization settings and analyzed in different dependent structures It shows how different high-dimensional dependence constructions influence on cyber insurance premiums and risk measures

Table 5 (continued)

	Böhme and Kataria [11]	Herath and Herath [42]	Mukhopadhyay et al. [58]	Eling and Jung [26]
Implication & limitation	The more reliable outcomes and accurate risk measures can be realized by more appropriate and abundant data. Especially, longitudinal data on different risk classes are essential for further research	The size of the data is too small to obtain the meaningful result of copula modelling	This study makes some contributions to vulnerability assessment and pricing cyber insurance with utility theory under Bayesian decision tree, but does not cover different types of attack risks and the curse of dimensionality is implied in the model	A comprehensive analysis on dependence structure of data breach risks is suggested, which might reveal non-linear dependency between risks proved by significant upper tail dependency

threats, which is still notoriously difficult due to the lack of respective data. The results show that the frequently used actuarial dependence models, such as copulas, and frequency distribution, such as Poisson distribution, do not always describe cyber risks well. This implies also that regulatory capital models underestimate the strength and nonlinearity of dependence. Insurers should differentiate premiums based on the connectivity and IT security levels of the policyholder. Finally, an analysis of network pandemics allow for a consideration of systemic events and worst-case scenarios.

3.3 Summary of empirical literature

Table 6 categorizes the empirical literature on cyber risk in order to filter out what we know about the frequency, severity and dependence structure of cyber risk. The results of the table might be useful to identify possible ways of calibrating cyber risks in the context of risk models. We systematically review empirical studies based on real data (Part A) and scenario analysis (Part B). Since extreme cyber events have not yet been observed, pure empirical papers to estimate parameters are both rare and limited.[10] Scenarios that coherently describe possible future developments based on expert judgments, can be used to quantify worst-case hits, for example to an insurer's capital. For example, Ruffle et al. [68] define a scenario where a systemic technology company is compromised and estimate the frequency of occurrence (1%), the resulting financial market returns (– 4%) and the percentage of businesses that is affected worldwide (50%). Another example is the blackout scenario by Lloyd's [52] which analyzes the effect of a power outage on the east coast of the United States. It allows an insurer (if an exposure to this market exists) to investigate how the different lines of business are simultaneously affected by a single event. Similarly, Daffron et al.'s [18] scenario, the Bashe attack, investigates global malware infection. They estimate the costs for the insurance industry 1.2–1.4 times the global insurance premiums. The authors also show how the losses would be distributed over different lines of business.

4 Conclusion and discussion

Cyber risk research is still in its infancy, so much more needs to be done to understand this increasingly relevant part of the economy and society. Several fundamental research topics are still missing, such as a consistent theory and methodology of cyber risk management, instruments of risk management, information-sharing

[10] The largest cyber loss has been WannaCry which resulted in a US$8 billion economic loss (Gallin [38]). Mahalingam et al. [53] illustrate that for an event to have an impact on the capital market, at least an economic loss of US$1 trillion (or at least 1–2% world GDP) is necessary. This extreme magnitude that is necessary to create a systematic impact is very likely also the reason why event studies for other catastrophic events come to more mixed and inconclusive results.

Table 6 Overview of empirical literature on cyber risk

Authors	Description	Frequency	Severity	Dependence
Panel A: empirical studies				
Schnell [69]	Studies dependence in network models to better estimate frequency and severity of cyber risks	Distribution: negative binomial; Poisson, network model	Distribution: Network model; Value at Risk and Tail Value at Risk twice as high for network model compared to iid	Network model
Eling and Schnell [30, 28]	Use SAS operational risk data to model insurer's cyber underwriting portfolio; based on SAS Operational Risk Database	Mean: 2.6% of companies are affected	Distribution: generalized beta, Levy & stable	Clayton copula
Kamiya et al. [50]	Event study to analyze the effect of cyberattacks on public corporations and their stock price; based on Privacy Rights Clearinghouse (PRC) data	n.a.	Abnormal return: cyberattacks with personal financial information loss are associated with negative stock market reactions (– 1.09% in the 3-day window around the attack; large reputation costs)	n.a.
Eling and Wirfs [31]	Estimate dynamic severity and frequency distributions models based on SAS data	Distribution: negative binomial; report different frequency parameters for different cyber risks	Distribution: peaks-over-threshold (threshold: 56%) & generalized Pareto; report different distribution parameters for different cyber risks	n.a.
Woods et al. [81]	Reconstruct the severity distribution of cyber risk for firms; based on the pricing information of US regulatory filings	n.a.	Distribution: gamma; derive parameters for different distributions (Lognormal, Pareto, Burr) Mean: expected cyber liability loss of $428 k per firm	n.a.

Table 6 (continued)

Authors	Description	Frequency	Severity	Dependence
Eling and Jung [26]	Copula approach for modeling cross-sectional dependence of data breach losses; based on PRC data	Distribution: negative binomial	Distribution: lognormal; $1bn monthly breach records at 99.5% critical level for US	Pair copula construction (R-) vine copula; correlation and copula parameters for different industries and breach types
Ponemon Institute [47]	Cost of a data breach study; based on interviews of global companies	n.a.	Mean: data breach costs $3.86 m per company; each stolen record costs $148	n.a.
Verizon LLC [77]	Data breach investigation; based on proprietary data	n.a.	n.a.	n.a.
Xu et al. [84]	Report a statistical analysis of a breach incident data set corresponding to 12 years (2005–2017) of cyber hacking activities that include malware attacks; based on PRC data	Breach incident inter-arrival times modeled by stochastic process; autocorrelation observed	Breach sizes modeled by stochastic process rather than by distributions because they exhibit autocorrelation	n.a.
Biancotti [9]	Evidence on the price of cyber security; based on Bank of Italy survey data	n.a.	Mean: most breached firms suffered damages less than €10 k; 1% reported costs of at least €200 k	n.a.
Ceross and Simpson [17]	Use data protection regulatory actions (fines) to estimate costs of data breaches; based on UK Information Commissioner's Office data for private and public entities	n.a.	Mean: 168 k data breaches; fines around £110 K, upper limit of £500 k per entity Other: no strong positive relationship between fines and number of breached records	n.a.

Table 6 (continued)

Authors	Description	Frequency	Severity	Dependence
Eling and Loperfido [27]	Use multidimensional scaling and goodness-of-fit tests to analyze the distribution of data breaches; based on PRC data	Distribution: Poisson	Distribution: log-skew-normal; different model for different breach types	n.a.
Edwards et al. [23]	Study Bayesian Generalized Linear Models to investigate trends in data breaches based on the data from PRC	Distribution: negative binomial	Distribution: lognormal; in the next 3 years breaches could cost up to \$179bn (95%-VaR) in the US	n.a.
Heitzenrater and Simpson [41]	Analyze cyber security disclosures for small and medium sized companies; based on UK information security breaches survey	Mean: In 2015 60% of companies suffered a malicious security incident (and 50% a serious breach)	Mean: loss due to virus and hacker attacks was in 2014 in the UK in the range of £75.2 k to £311 k per company	n.a.
Romanosky [64]	Estimates costs for incidents for different cyber risk types and industry; based on several sources, one of them is Advisen	Distribution: negative binomial	Mean: Cost of a typical cyber incident is less than \$200 k or 0.4% of firm revenues	n.a.
Wheatley et al. [80]	Analyze the properties of personal data breaches (PRC & OPS DatalossDB)	Poisson generalized linear model	Distribution: Extremely heavy-tailed Pareto; maximum breach size of about \$200 m per incident and is expected to growth by 50% over 5 years	n.a.

Table 6 (continued)

Authors	Description	Frequency	Severity	Dependence
Biener et al. [10]	Analyze the insurability of cyber risk; based on SAS OpRisk database	n.a.	Mean: $41 m; Std. dev.: $444 m; 95%-VaR $90 m; 95%-TVaR: $677 m; report values for different industry, cyber risk type, regions & business size	n.a.
Franke et al. [36]	The distribution of time to recovery of enterprise IT services; based on Nordic bank's event log	n.a.	Distribution: lognormal	n.a.
Romanosky et al. [67]	Empirical analysis of data breach litigation; based on US court dockets	n.a.	n.a.	n.a.
Maillart and Sornette [54]	Estimate statistical property and trend of theft of personal information; based on Open Security Foundation Data-lossDB	Frequency increased strongly up to 2006; stationary between 2006 and 2010	Distribution: power law	n.a.
Schroeder and Gibson [70]	A large-scale study of failures in high-performance computing systems; based on research institute's event log	n.a.	Distribution: lognormal	n.a.
Böhme and Kataria [11]	Honeypot data (registered attacks at internet nodes)	Distribution: beta-binomial	n.a.	Linear correlation: 0.18; t-copula; stronger dependency in the tails

Table 6 (continued)

Authors	Description	Frequency	Severity	Dependence
Cavusoglu et al. [15]	Event study: analyze how security breaches affect the market value of firms in the US; based on global news database (CNET, ZDNET, Lexis/Nexis)	n.a.	Abnormal return: security breaches negatively affect stock price (-2.1% or $-1.65bn of market value). Meanwhile, stock prices of information security providers increase (1.36% or $1.06bn of market value) after the announcement of another company's security breach	n.a.
Campbell et al. [13]	Event study examine the economic effect of information security breaches on publicly traded US corporations; based on newspaper reports (Wall Street Journal, New York Times, Washington Post, Financial Times, and USA Today)	n.a.	Abnormal return: highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information	n.a.
Hovav and D'Arcy [46]	Event study for the impact of denial-of-service attack announcements on the market value of firms; based on newspaper reports (Lexis-Nexis database)	n.a.	Abnormal return: The market does not penalize companies that experience a denial of service attack. However, there is an indication that the market penalizes "internet-specific" companies more than other companies	n.a.

Table 6 (continued)

Authors	Description	Frequency	Severity	Dependence
Panel B: Scenarios				
Ruffle et al. [68]	Scenario where a systemic technology company is compromised	Frequency of occurrence: 1%	Financial market returns: – 4%; 50% of businesses are affected worldwide	n.a.
Lloyd’s [52]	Analyzes the effect of a power outage on the US east coast	n.a.	The total impact to the US economy is estimated at $243 bn	n.a.
Daffron et al. [18]	Investigates global malware infection (Bashe attack)	n.a.	Estimate the costs for the insurance industry 1.2–1.4 times the global insurance premiums	n.a.
Risk Management Solutions Inc.[65], Dejung [21]	Distributed Denial of Service (DDoS) attack: disables websites and disrupt online business activity across multiple companies	50% of major US companies experienced a DDoS attack in 2015 and 1/8 of those attacks rendered their websites unavailable	Average cost is reported to be $52 k per incident for SME and $440 k per incident for larger businesses; 0.03% to 0.2% of Swiss GDP (Dejung [21])	n.a.
Risk Management Solutions Inc.[65], Dejung [21]	Cloud service provider failure: business operations of many companies are disrupted due to unavailability of major cloud service provider (CSP) company	Very low; CSP typically achieve over 99.9% reliability of service	It is expected that 17 k companies are unable to access cloud services for a few hours up to one month	n.a.

Table 6 (continued)

Authors	Description	Frequency	Severity	Dependence
Oughton et al. [61]	Helios solar storm: solar flares produce radiation across the electro-magnetic spectrum. Exceptionally high levels could turn out some electronic components including those in satellites and communication grids	Peak activity of solar flares occurs every eleven years	The indirect impact of a solar storm is on the supply chain is estimated at 0.8%-3.9% of GDP	n.a.
Risk Management Solutions Inc [65]	Financial transaction cyber compromise: cyberattacks on multiple enterprises that carry out financial transactions	n.a	The theft amounts to $10bn (from several financial institutions in different countries)	n.a.
Dejung [21]	Health sector and hospitals scenarios: a cyberattack that infiltrates several hospitals, resulting in non-availability of hospitals for two to three weeks	Likelihood of successful attacks that affect more than 10% of a country’s hospitals is assumed to be low to medium	Max. economic impact is assumed to be 0.2% of GDP	n.a.
Trautman and Ormerod [76]	Municipal services compromised: malware is deployed on a city’s administrative service systems, disabling civil services functions for an entire city	n.a.	Estimates from the SamSam ransomware attack on the city of Atlanta indicate that the total cost of disturbance was around $20 m	n.a
Dejung [21]	Telecommunication scenarios: malware targets e.g., a router or modem with 50% market share and results in the deletion of the firmware whereby the devices must be replaced	n.a.	0.35% of GDP in the first scenario and 0.03% in the second scenario	n.a.

Table 6 (continued)

Authors	Description	Frequency	Severity	Dependence
Risk Management Solutions Inc.[65], Ruffle et al. [68]	Strategic cross-sector attack scenario; take hostage of many companies by disabling IT functionality to obtain ransom payments	Ruffle et al. [68]: 1%	According to Ruffle et al. [68] the overall global loss is estimated between $4.5 to $15 tn	They predict a plunge of the financial markets similarly to the financial crisis in 2008
Dejung [21]	SCADA/ICS; simple process variables are maliciously modified to change the product properties. Victims are e.g., critical infrastructure providers (i.e., electric grid, oil/gas/water networks)	n.a.	Economic impact is estimated at 0.05–0.3% of GDP, caused mainly by business interruption, loss of profit, and physical damages including accidents and fatalities	n.a.

platforms and regulation (see Augsburger-Bucheli et al. [3]). Given that cyber risks are highly complex and dynamic, it is hard to measure their likelihood and impact. Unlike other more standard types of risk from the property and casualty domain, historical information on cyber loss events are scarce and it is far from clear whether existing databases are useful for an analysis of potential future cyber risks. Research thus needs to evaluate the potential and limits of approaches to risk analysis and risk management in the field of cyber risks. For example, it needs to be investigated if and how cyber risks can be compared to other risks and thus be integrated in the established risk management frameworks. More research is also needed on potential instruments for risk analysis such as risk cartography, scenarios, or simulations.

Other important questions are how to measure cyber risks and how to measure the efficiency and effectiveness of countermeasures. A major challenge for risk management in the field of cyber risks is the lack of information on the risks as well as on the effectiveness of countermeasures. In response to this problem, information-sharing platforms have been established such as MELANI in Switzerland and BSI in Germany. Research might be helpful to identify efficient and effective ways to govern such platforms. A special focus should be put on information-sharing between public and private actors, in form of public–private partnerships. Better information will help to measure the risk more accurately and thus make cyber risk more insurable. More precise measurements could also aid managers to determine the acceptable level of risk for their organization. The main databases (such as the PRC database for the US) are limited to coverage of data breaches and little is known about other cyber events; furthermore, the economic magnitude of the events is difficult to estimate, given that most databases do not report loss amounts, but the number of breached data points.

As documented by the introduction of the new European Union data protection requirements (GDPR), risk management is highly influenced by the regulatory environment. Governments can enforce practices and standards of risk management by regulation. The most prominent example for regulation with respect to risk management is the introduction of mandatory reporting requirements of incidents. Research should assess whether and under which conditions regulation can improve the risk management of companies and individuals. Another critical aspect that needs consideration in the macroeconomic context is the extent to which an extensive writing of cyber insurance could give rise to systemic risk, especially if IT systems are increasingly connected. The systemic risk might also depend on the type of cyber risk covered in cyber insurance policies. Some risks, such as viruses or phishing, might show a high correlation between different firms, while for other types of risks such as insider attacks or hardware failures the correlation might be rather low. Risk pooling is clearly expected to work better in the latter case, while the former case might show undesirable accumulation risks, at least in extreme scenarios. We also note that insurance companies are affected by cyber risk in two distinct ways: in their underwriting when new cyber insurance policies are sold; and the operational cyber risk stemming from their own IT systems also needs critical consideration in an industry that is built upon trust, reputation and sensible data.

This also calls for regulation of cyber risk within insurance companies, a regulation which very likely must acknowledge that the current treatment of cyber risks and cyber insurance is insufficient. For example, regulatory models should consider heavy tails and tail dependence among cyber risk, which are not the considered in the current regulation. This might lead to a separate risk category for cyber risk when the cyber insurance market becomes larger and cyber risk underwriting thus more significant. Certainly, such a proposal is a double-edged sword and needs careful consideration by researchers, because imposing additional requirements might improve security of insurance companies, but it might also hinder the development of a cyber insurance market and thus lead to socially and economically inefficient outcomes.

Overall, the number and level of open questions raised here clearly demonstrate that cyber risk research is still in its early stages; there is ample opportunity for future research and especially more interdisciplinary work is needed to better understand the risk (Falco et al. [34]). Information security experts, for example, might collaborate with people from business or from actuarial science. While information security researchers will bring the necessary technical knowhow, scholars from business and actuarial science can assess and evaluate the underlying risks in terms of business and economics impact. The contributions of legal scholars and psychologists might also be needed, because most cyber risks are man-made. Overcoming the interdisciplinary research barriers will prove to be especially useful for cyber risk research and practice.

Acknowledgements I thank Sebastian Kimm-Friedenberg and Werner Schnell for their assistance in preparing this paper.

Funding None.

Compliance with ethical standards

Conflict of interest The author(s) declare that they have no conflicts of interest.

Appendix A: Google Scholar Citations

See Table 7 and Fig. 2.

Table 7 Google Scholar citations as of April 09, 2020

Year	"Cyber Risk"	"Cyber Insurance"
2000	185	5
2001	240	14
2002	192	13
2003	199	31
2004	228	23
2005	226	47
2006	217	52
2007	273	36
2008	296	46
2009	258	57
2010	306	69
2011	467	74
2012	530	90
2013	503	127
2014	698	190
2015	899	298
2016	1160	390
2017	1290	482
2018	1840	634
2019	2320	655
2020	480	138

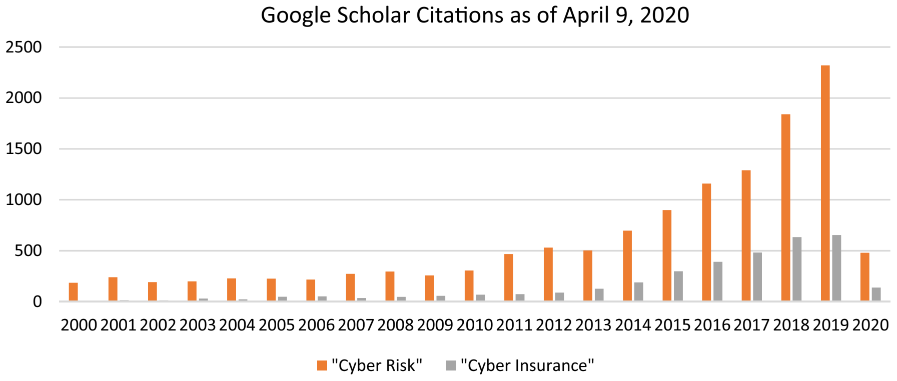

Fig. 2 Google Scholar citations as of April 09, 2020

Appendix B: Visualization Treemap on "Cyber Insurance"

See Fig. 3.

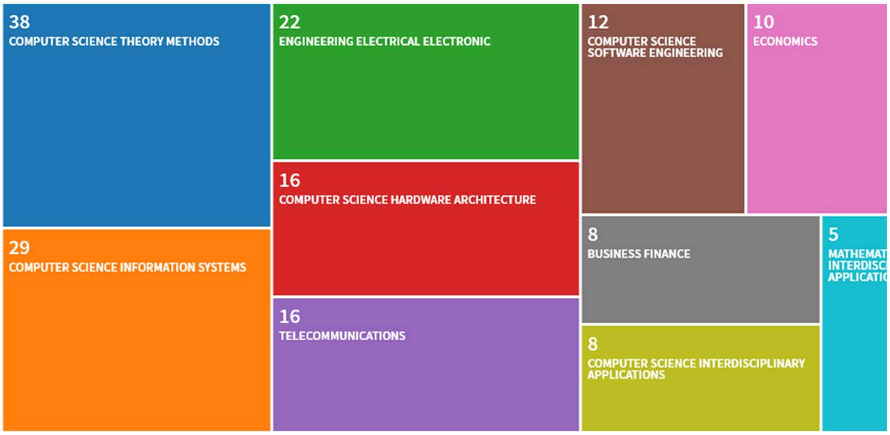

Fig. 3 Visualization Treemap for 95 hits on "cyber insurance" in the Web of Science as of March 30, 2020

References

1. Anderson R, Moore T (2006) The economics of information security. Science 314:610–613
2. Ashby S, Buck T, Nöth-Zahn S, Peisl T (2018) Emerging IT risks: Insights from German banking. Geneva Pap Risk Insur Issues Pract 43:180–207
3. Augsburger-Bucheli I, Bangerter E, Brunoni L et al (2017) Forschung zu Cyber-Risiken in der Schweiz. Bern. https://www.isb.admin.ch/dam/isb_kp/de/dokumente/themen/ncs/Expertenbericht_forschung.pdf.download.pdf/Expertenbericht_forschung.pdf
4. August T, Dao D, Kim K (2019) Market segmentation and software security: pricing patching rights. Manage Sci 65:4575–4597
5. Bai X (2011) Predicting consumer sentiments from online text. Decision Support Syst 50:732–742
6. Bandyopadhyay T, Mookerjee V, Rao R (2009) Why IT managers don't go for cyber-insurance products. Commun ACM 52:68–73
7. Bentley M, Stephenson A, Toscas P, Zhu Z (2020) A multivariate model to quantify and mitigate cybersecurity risk. Risks 8:61
8. Berliner B (1982) Limits of insurability of risks. Englewood Cliffs, New Jersey
9. Biancotti C (2017) The price of cyber (in)security: evidence from the Italian private sector. In: Bank of Italy occasional paper
10. Biener C, Eling M, Wirfs JH (2015) Insurability of cyber risk: an empirical analysis. Geneva Pap Risk Insur Issues Pract 40:131–158
11. Böhme R, Kataria G (2006) Models and measures for correlation in cyber-insurance. Boston. https://www.econinfosec.org/archive/weis2006/docs/16.pdf
12. Bolance C, Guillen M, Pelican E, Vernic R (2008) Skewed bivariate models and nonparametric estimation for the CTE risk measure. Insur Math Econ 43:386–393
13. Campbell K, Gordon LA, Loeb MP, Zhou L (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market. J Comput Secur 11:431–448

14. Cartagena S, Gosrani V, Grewal J, Pikinska J (2020) Silent cyber assessment framework. Br Actuarial J 2020:25
15. Cavusoglu H, Mishra B, Raghunathan S (2004) The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers. Int J Electron Commerce 9:69–104
16. Cebula J, Young L (2010) A taxonomy of operational cyber security risks. Carnegie Mellon, https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395
17. Ceross A, Simpson A (2017) The use of data protection regulatory actions as a data source for privacy economics. In: Tonetta S, Schoitsch E, Bitsch F (eds) Computer safety, reliability, and security. Springer International Publishing, Cham, pp 350–360
18. Daffron J, Ruffle S, Andrew C, et al (2019) Bashe attack: Global infection by contagious malware. Cambridge Centre for Risk Studies, Lloyd's of London and Nanyang Technological University. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack
19. Dal Moro E (2020) Towards an economic cyber loss index for parametric cover based on IT security indicator: a preliminary analysis. Risks 8:45
20. de Smidt G, Botzen W (2018) Perceptions of corporate cyber risks and insurance decision-making. Geneva Pap Risk Insur Issues Pract 43:239–274
21. Dejung S (2017) Economic impact of cyber accumulation scenarios. Swiss Insurance Association SVV Cyber Working Group, Zürich. https://www.vvb-alumni.de/wp-content/uploads/2020/03/Economic_impact_Cyber_loss_accumulation_scenarios_SVV.pdf
22. Dondossola G, Garrone F, Szanto J (2011) Cyber risk assessment of power control systems—a metrics weighed by attack experiments. In: 2011 IEEE power and energy society general meeting, pp 1–9
23. Edwards B, Hofmeyr S, Forrest S (2016) Hype and heavy tails: a closer look at data breaches. J Cybersecur 2:3–14
24. Egan R, Cartagena S, Mohamed R et al (2019) Cyber operational risk scenarios for insurance companies. Br Actuarial J 2019:24
25. Eling M (2012) Fitting insurance claims to skewed distributions: are the skew-normal and skew-student good models? Insur Math Econ 51:239–248
26. Eling M, Jung K (2018) Copula approaches for modeling cross-sectional dependence of data breach losses. Insur Math Econ 82:167–180
27. Eling M, Loperfido N (2017) Data breaches: goodness of fit, pricing, and risk measurement. Insur Math Econ 75:126–136
28. Eling M, Schnell W (2020) Extreme cyber risks and the nondiversification trap. Working Paper University of St. Gallen. https://www.alexandria.unisg.ch/260004/
29. Eling M, Schnell W (2016) What do we know about cyber risk and cyber risk insurance? J Risk Financ 17:474–491
30. Eling M, Schnell W (2019) Capital requirements for cyber risk and cyber risk insurance: an analysis of solvency II, the US Risk-based capital standards, and the swiss solvency test. N Am Actuarial J 2019:1–23
31. Eling M, Wirfs J (2019) What are the actual costs of cyber risk events? Eur J Oper Res 272:1109–1119
32. Eling M, Zhu J (2018) Which insurers write cyber insurance? Evidence from the US property and casualty insurance industry. J Insur Issues 41:22–56
33. Fahrenwaldt MA, Weber S, Weske K (2018) Pricing of cyber insurance contracts in a network model. ASTIN Bull J IAA 48:1175–1218
34. Falco G, Eling M, Jablanski D et al (2019) Cyber risk research impeded by disciplinary barriers. Science 366:1066–1069
35. Long Finance (2015) Financing the transition: sustainable infrastructure in cities. Z/Yen Group, London. https://www.longfinance.net/media/documents/Financing_the_transition_March2015.pdf
36. Franke U, Holm H, König J (2014) The distribution of time to recovery of enterprise it services. IEEE Trans Reliab 63:858–867
37. Gai K, Qiu M, Elnagdy S (2016) A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance. In: 2016 IEEE 2nd international conference on big data security on cloud (BigDataSecurity), IEEE international conference on high performance and smart computing (HPSC), and IEEE international conference on intelligent data and security (IDS, pp 171–176

38. Gallin L (2017) Re/insurance to take minimal share of $8 billion WannaCry economic loss: A.M. Best. In: ReinsuranceNews. https://www.reinsurancene.ws/reinsurance-take-minimal-share-8-billion-wannacry-economic-loss-m-best/. Accessed 31 Jul 2020
39. Gordon LA, Loeb M (2002) The economics of information security investment. ACM Trans Inf Syst Secur 5:438–457
40. Gordon L, Loeb M, Sohail T (2003) A framework for using insurance for cyber-risk management. Commun ACM 46:81–85
41. Heitzenrater CD, Simpson AC (2016) Policy, statistics and questions: Reflections on UK cyber security disclosures. J Cybersecur 2:43–56
42. Herath H, Herath T (2011) Copula-based actuarial model for pricing cyber-insurance policies. Insur Markets Companies Anal Actuarial Comput 2:7–20
43. Hoang DT, Wang P, Niyato D, Hossain E (2017) Charging and discharging of plug-in electric vehicles (pevs) in vehicle-to-grid (v2g) systems: a cyber insurance-based model. IEEE Access. https://doi.org/10.1109/ACCESS.2017.2649042
44. Hofmann A, Ramaj H (2011) Interdependent risk networks: the threat of cyber attack. Int J Manage Decision Making 11:312–323
45. Hofmann A, Rothschild C (2019) On the efficiency of self-protection with spillovers in risk. Geneva Risk Insur Rev 44:207–221
46. Hovav A, D'Arcy J (2003) The impact of denial-of-service attack announcements on the market value of firms. Risk Manag Insur Rev 6:97–121
47. Ponemon Institute (2017) 2017 cost of data breach study. Traverse City. https://www.ibm.com/downloads/cas/ZYKLN2E3
48. Jevtić P, Lanchier N (2020) Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology. Insur Math Econ 91:209–223
49. Johnson B, Böhme R, Grossklags J (2011) Security games with market insurance. In: Baras JS, Katz J, Altman E (eds) Decision and game theory for security. Springer, Berlin, Heidelberg, pp 117–130
50. Kamiya S, Kang J-K, Kim J et al (2020) Risk management, firm reputation, and the impact of successful cyberattacks on target firms. J Financ Econ. https://doi.org/10.1016/j.jfineco.2019.05.019
51. Kelly S, Leverett E, Copic J et al (2016) Integrated infrastructure: cyber resiliency in society: mapping the consequences of an interconnected digital economy. In: Centre for Risk Studies, University of Cambridge. https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/integrated-infrastructure-cyber-resiliency-in-society/
52. Lloyd's (2015) Business blackout: The insurance implications of a cyber attack on the US power grid. https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout. Accessed 31 Jul 2020
53. Mahalingam A, Coburn AW, Jung CJ, et al (2018) Impacts of severe natural catastrophes on financial markets. Centre for Risk Studies, University of Cambridge. https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/natural-catastrophe-and-climate/impacts-of-severe-natural-catastrophes-on-financial-markets/
54. Maillart T, Sornette D (2010) Heavy-tailed distribution of cyber-risks. Eur Phys J B 75:357–364
55. Marotta A, McShane M (2018) Integrating a proactive technique into a holistic cyber risk management approach. Risk Manag Insur Rev 21:435–452
56. Marotta A, Martinelli F, Nanni S et al (2017) Cyber-insurance survey. Comput Sci Rev 24:35–61
57. McQueen M, Boyer W, Flynn M, Beitel G (2006) Time-to-compromise model for cyber risk reduction estimation. In: Gollmann D, Massacci F, Yautsiukhin A (eds) Quality of protection. Springer, New York, pp 49–64
58. Mukhopadhyay A, Chatterjee S, Saha D et al (2013) Cyber-risk decision models: to insure IT or not? Decision Support Syst 56:11–26
59. NetDiligence (2016) 2016 cyber claims study. Gladwyne, PA. https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf
60. Nikolakopoulos T, Darra E, Tofan D (2016) The cost of incidents affecting CIIsSystematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII). In: ENISA, Herklion. https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis
61. Oughton E, Copic J, Skelton A et al (2016) Helios solar storm scenario. Centre for Risk Studies, University of Cambridge. https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/helios-solar-storm-scenario/

62. Pal R, Golubchik L, Psounis K, Hui P (2014) Will cyber-insurance improve network security? A market analysis. In: IEEE INFOCOM 2014—IEEE conference on computer communications, pp 235–243
63. Pooser DM, Browne MJ, Arkhangelska O (2018) Growth in the perception of cyber risk: evidence from US P&C insurers. Geneva Pap Risk Insur Issues Pract 43:208–223
64. Romanosky S (2016) Examining the costs and causes of cyber incidents. J Cyber Secur 2:121–135
65. Risk Management Solutions Inc. (2016) Managing cyber insurance accumulation risk. In: Centre for Risk Studies, Cambridge. https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/cyber-risk-outlook/managing-cyber-insurance-accumulation-risk-2016/
66. Romanosky S, Telang R, Acquisti A (2011) Do data breach disclosure laws reduce identity theft? J Policy Anal Manag 30:256–286
67. Romanosky S, Hoffman D, Acquisti A (2014) Empirical analysis of data breach litigation. J Empir Legal Stud 11:74–104
68. Ruffle SJ, Bowman G, Caccioli F et al (2014) Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe. In: Centre for Risk Studies, University of Cambridge. https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/sybil-logic-bomb-cyber-catastrophe-stress-test-scenario/
69. Schnell W (2020) Does cyber risk pose a systemic threat to the insurance industry? Working Paper University of St. Gallen. https://www.alexandria.unisg.ch/260003/
70. Schroeder B, Gibson GA (2010) A large-scale study of failures in high-performance computing systems. IEEE Trans Depend Secure Comput 7:337–350
71. Shackelford SJ (2012) Should your firm invest in cyber risk insurance? Bus Horiz 55:349–356
72. Shetty N, Schwartz G, Felegyhazi M, Walrand J (2010) Competitive cyber-insurance and internet security. In: Moore T, Pym D, Ioannidis C (eds) Economics of information security and privacy. Springer, Boston, pp 229–247
73. Shetty S, McShane M, Zhang L et al (2018) Reducing informational disadvantages to improve cyber risk management. Geneva Pap Risk Insur Issues Pract 43:224–238
74. Sinanaj G, Muntermann J (2013) Assessing corporate reputational damage of data breaches: an empirical analysis. BLED 2013 Proc 2013:29
75. Srinidhi B, Yan J, Tayi GK (2015) Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors. Decision Support Syst 75:49–62
76. Trautman LJ, Ormerod P (2019) Wannacry, ransomware, and the emerging threat to corporations. Tennessee Law Rev 86:505–556
77. Verizon LLC (2018) 2018 data breach investigations report. New York. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf
78. Vernic R (2006) Multivariate skew-normal distributions with applications in insurance. Insur Math Econ 38:413–426
79. Vishwanath A, Harrison B, Ng YJ (2018) Suspicion, cognition, and automaticity model of phishing susceptibility. Commun Res 45:1146–1166
80. Wheatley S, Maillart T, Sornette D (2016) The extreme risk of personal data breaches and the erosion of privacy. Eur Phys J B 89:7
81. Woods DW, Moore T, Simpson AC (2019) The county fair cyber loss distribution: drawing inferences from insurance prices. Boston, MA
82. World Economic Forum (2010) The global competitiveness report 2010–2011. World Economic Forum, Geneva. https://www3.weforum.org/docs/WEF_GlobalCompetitivenessReport_2010-11.pdf
83. Xu M, Hua L (2019) Cybersecurity insurance: modeling and pricing. N Am Actuarial J 23:220–249
84. Xu M, Schweitzer KM, Bateman RM, Xu S (2018) Modeling and predicting cyber hacking breaches. IEEE Trans Inf Forensics Secur 13:2856–2871