

Essays on Modeling, Management, and Regulation of Cyber Risk

DISSERTATION
of the University of St.Gallen,
School of Management,
Economics, Law, Social Sciences
and International Affairs
to obtain the title of
Doctor of Philosophy in Finance

submitted by
Werner Schnell
from
Maienfeld (Graubünden)

Approved on the application of
Prof. Dr. Martin Eling
and
Prof. Dr. Angelo Ranaldo

Dissertation no. 5019

Difo-Druck GmbH, Untersiemaun 2020

The University of St.Gallen, School of Management, Economics, Law, Social Sciences and International Affairs hereby consents to the printing of the present dissertation, without hereby expressing any opinion on the views herein expressed.

St.Gallen, May 25th, 2020

The President:

Prof. Dr. Bernhard Ehrenzeller

Acknowledgement

Without the continuous support of many people this doctoral thesis would not have been possible and thus I am grateful to everyone who contributed. First, I would like to express my gratitude to my supervisor and co-author, Prof. Martin Eling, for his tremendous support and guidance. His dedication to high-quality research has motivated me to improve the way I conduct research and greatly enhanced the quality of my doctoral thesis. I also thank Prof. Angelo Ranaldo for his dedicated co-supervision and insightful comments on how to improve my research and PD Christian Biener for his much-appreciated contribution as a third committee member.

Additionally, I am grateful to my colleagues at the Institute of Insurance Economics (I.VW) for their support and our many fruitful discussions. The environment at I.VW was exceptionally inspiring, supportive, and motivating for my endeavors. I also want to acknowledge the countless conference participants who gave me feedback on my papers even if it was only a nod or a smile. In addition, I am grateful for the financial support received from the Swiss National Science Foundation.

Finally, I dedicate this doctoral thesis to my family and friends for accompanying me on this journey. They have been a reliable source of motivation, strength, and confidence over the years.

St.Gallen, August 4th, 2020, Werner Schnell

Content

List of figures.....	V
List of tables.....	VIII
Overview of the doctoral thesis.....	IX
Summary.....	X
Zusammenfassung.....	XII
Essay I What do we know about cyber risk and cyber risk insurance?.....	14
1 Motivation and aim of the paper.....	16
2 Research approach	17
3 Research results	18
3.1. Definition and categorization of cyber risk	18
3.2. Costs and detrimental effect caused by cyber risk	20
3.3. How to find data on cyber risk	21
3.4. How to model cyber risk	22
3.5. How to organize cyber risk management	24
3.6. Is cyber risk a threat to the global economy and society?.....	25
3.7. What does the cyber insurance market look like, and what are the main insurability challenges?.....	27
4 Derivation of potential future work	30
4.1. Practical perspective	31
4.2. Academic perspective.....	33
5 References.....	34
6 Appendices	42
Essay II 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	74
1 Introduction.....	76
2 Cyber risk: definition and properties	78
3 Data and methodology	80

4	Operational cyber risk.....	88
4.1.	Solvency II.....	88
4.2.	US risk-based capital standards.....	91
4.3.	Swiss solvency test	91
5	Underwriting cyber risk.....	91
5.1.	Solvency II.....	92
5.2.	US risk-based capital standards.....	98
5.3.	Swiss solvency test	102
6	Conclusions.....	106
7	References.....	108
8	Appendices	115
Essay III Is cyber risk insurable?.....		134
1	Introduction.....	136
2	Methodology.....	138
3	Data and parameter choice.....	145
4	Results.....	148
5	Conclusions.....	157
6	References.....	160
7	Appendices	167
Essay IV Epidemic cyber risk		186
1	Introduction.....	188
2	Literature review.....	190
3	Methodology.....	194
4	Parameter choice.....	199
5	Results.....	200
5.1.	Sensitivity analysis	206

5.2.	Pricing.....	208
5.3.	Diversification	210
5.4.	Scenario analysis	212
6	Conclusion	217
7	References.....	219
8	Appendices	227
	Curriculum Vitae	237

List of figures

Essay I What do we know about cyber risk and cyber risk insurance?.....	14
Figure A1. Google scholar citations as of 28 February 2016.....	42
Essay II 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	74
Figure 1. QQ plot: empirical vs. lognormal	84
Figure 2. Expected exceedance	84
Figure 3. Operational cyber risk.....	90
Figure 4. SII survival probability contours	95
Figure 5. SII survival probability	97
Figure 6. RBC survival probability contours	100
Figure 7. RBC survival probability	101
Figure 8. SST survival probability contour	105
Figure 9. SST survival probability	106
Figure A1. SII survival probability (different cover limits)	115
Figure A2. RBC survival probability (different cover limits).....	116
Figure A3. SST survival probability (different cover limits)	117
Figure B1. Cover limit vs. limited support.....	118
Figure C1. SII survival probability contours.....	120
Figure C2. RBC survival probability contours.....	121
Figure C3. SST survival probability contours.....	122
Figure D1. SII survival probability contours.....	123
Figure D2. RBC survival probability contours	124
Figure D3. SST survival probability contours.....	125
Figure E1. SII model	127
Figure F1. SST survival probability contour (US\$1 million threshold).....	128

Figure G1. SII survival probability contour (loss ratio 0.8).....	129
Figure G2. RBC survival probability contour (loss ratio 0.8).....	130
Figure H1. SII survival probability contour (frequency 2.6%)	131
Figure H2. RBC survival probability contour (frequency 2.6%).....	132
Figure H3. SST survival probability contour (frequency 2.6%)	133
Essay III Is cyber risk insurable?.....	134
Figure 1a. Premium versus WTP.....	149
Figure 1b. Premium components.....	149
Figure 2. Premium ratio for single insurer	150
Figure 3. Premium ratio for different cover limits	151
Figure 4. Premium ratio for insurance pools.....	152
Figure 5. Premium composition for insurance pools	153
Figure 6. Parameter uncertainty with respect to the Pareto index.....	155
Figure 7. Modeling uncertainty	157
Figure A1. Premium ratio for PRC data	169
Figure B1. Pareto index stability	172
Figure C1. Premium ratio for different distributions	173
Figure C2. Premium ratio for different correlations.....	174
Figure C3. Premium ratio for different loss frequency	175
Figure C4. Premium ratio for TVaR.....	176
Figure C5. Premium ratio for alternative confidence levels	177
Figure C6. Premium ratio for different cost functions	178
Figure C7. Premium ratio for different frictional capital costs	178
Figure C8. Premium ratio for alternative cover limits	179
Figure C9. Premium ratio for risk neutrality	180
Figure C10. Premium ratio for different CARA	181

Figure C11. Premium ratio for isoelastic utility	182
Figure C12. Comparison of different models.....	183
Figure E1. Tail behavior and cover limits	185
Essay IV Epidemic cyber risk	186
Figure 1. Distribution of cyber portfolio loss frequency.....	201
Figure 2. Distribution of cyber portfolio loss.....	203
Figure 3. Sensitivity of the risk factor	208
Figure 4. Diversification for network risks	212
Figure 5. Portfolio distribution for systemic institution.....	213
Figure 6. Portfolio distribution for pandemic spreading	214
Figure 7. Capital requirements for different scenarios.....	215
Figure A1. Cyber underwriting network	227
Figure B1. Sensitivity of final infection frequency.....	230
Figure C1. Statistics for increasing number of simulations	231
Figure D1. Statistical sensitivity to contagion and infection probability.....	233
Figure E1. Frequency distribution based on copula.....	235
Figure F1. Correlation distribution for the insurer's portfolio	236

List of tables

Essay I What do we know about cyber risk and cyber risk insurance?	14
Table 1. Summary of results	29
Table A1. Google scholar citations as of 28 February 2016	42
Table C1. List of cyber risk literature.....	44
Table D1. Definitions of cyber risk	69
Table E1. Data sources	71
Essay II 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	74
Table 1. Cyber risk statistics and parameters (sample size n: 1,579).....	83
Table 2. Cyber risk insurance portfolio statistics and parameters.....	85
Table 3. Aggregation of risk factors	94
Table 4. SST parameters	104
Table D1. Cyber risk parameters (in million US\$).....	123
Essay III Is cyber risk insurable?	134
Table 1. Parameter choice.....	146
Table A1. Fitted distributions	168
Table B1. Fitted distributions	170
Essay IV Epidemic cyber risk	186
Table 1. Cyber network properties	197
Table 2. Parameter choice.....	199
Table 3. Statistics of cyber portfolio loss	205
Table 4. Sensitivity to infection and contagion probability.....	206
Table B1. Literature on network parameters	228

Overview of the doctoral thesis

This cumulative doctoral thesis consists of the following four essays:

	Essay I	Essay II	Essay III	Essay IV
Title	What do we know about cyber risk and cyber risk insurance?	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	Extreme cyber risks and the non-diversification trap	Does cyber risk pose a systemic threat to the insurance industry?
Author(s)	Martin Eling, Werner Schnell	Martin Eling, Werner Schnell	Martin Eling, Werner Schnell	Werner Schnell
Methodology	Comprehensive and systematic literature review and interviews with experts from the insurance industry.	Numerical loss distribution approach to model the aggregate cyber losses of an insurer's portfolio.	Development and simulation of a complete market model for cyber risk and the investigation of its failure.	Proposal for a network pandemic model to better represent dependence between cyber policies and simulation of the insurer's portfolio loss distribution.
Contribution	Finds that cyber risk is not understood well and establishes the need for further research into cyber risk.	Finds that the specific properties of cyber risk might not be adequately reflected in regulatory frameworks.	High costs, heavy tails, strong tail dependence, asymmetric information, and modeling risk hinder the development of a cyber risk market.	Network model leads to multimodal and heavy-tailed frequency distributions. The findings need to be considered for premium calculation, diversification, and regulation.
Status	Published 2016 in <i>Journal of Risk Finance</i> , 17(5), 474 – 491. https://doi.org/10.1108/JRF-09-2016-0122	Published 2019 in <i>North American Actuarial Journal</i> (online). https://doi.org/10.1080/10920277.2019.1641416 Presented at <i>ARIA, DFA, IRF conferences & PiF Research Seminar</i>	Presented at <i>EGRIE, ARIA, DVfVW, WRIE conference & PiF Research Seminar</i>	Presented at <i>WRIE conference</i>

Summary

While new information technologies (IT) have brought opportunities and prosperity, the flip side of the coin is that these technologies have increased society's reliance on and vulnerability to them. Every interruption in the confidentiality, integrity, and availability of data and services can have severe consequences. Such threats, termed cyber risk, can comprise large-scale data breaches or the breakdown of critical IT systems and can spread quickly around the globe. Due to its emerging nature, the extant academic literature on cyber risk is scarce and our knowledge is quite limited. My doctoral thesis is composed of four essays, all aiming to improve our understanding of cyber risk and derive recommendations for action.

The first essay sets the stage by providing an in-depth discussion of cyber risk. Starting with a systematic literature review, we derive what we know about cyber risk, how it can be modeled, and the obstacles when it comes to insuring against cyber risk. We find that the data quality with respect to cyber risk is not satisfactory and, consequently, academics and practitioners lack sound risk models. Managing and pricing cyber risk especially hinders the development of a cyber insurance market. Moreover, we find that cyber insurance peculiarities such as small portfolio sizes, heavy tails, high and potentially non-linear correlations, and risks of change (parameter and model risk) additionally present obstacles to the development of a cyber insurance market. This paper has been published in the *Journal of Risk Finance*.

The second essay uses the findings of the first one and analyzes the consequences for risk management. It contrasts the characteristics in cyber risk data with the regulatory models Solvency II, US risk-based capital (RBC), and Swiss solvency test. We identify the shortcomings of the regulatory models from both an operational and underwriting cyber risk perspective. The models applied to cyber risk do not guarantee the shortfall probability the regulator aims for. Especially for small portfolio sizes and high cover limits, the heavy-tailedness and high dependency in cyber risk reduce the merits of diversification and consequentially lead to lower survival probabilities. In general, we find that the current regulatory models are not well equipped to handle cyber risk.

The third essay models the cyber insurance market and analyzes the interaction of demand and supply as a function of the portfolio (and market) size. We show that previously identified cyber risk characteristics, such as strong tail dependence, high costs,

information asymmetries, and modeling risk, lead to a market trap. This describes a situation in which it is not optimal for insurers and insurees to start transferring cyber risks and a market does not develop. Since beyond a minimum market size the trap can resolve, insurers are advised to pool their risks with other insurers, and governments should incentivize such behavior. Moreover, sharing data on cyber risk can reduce the modeling risk, and IT security standards can mitigate asymmetric information.

The last essay analyzes the dependence between cyber risks (policy) and systemic components in more detail. Due to incomplete datasets, modeling dependence and frequency distributions is challenging. Because the inductive approach of network pandemics allows one to model the spreading of threats across entities (policyholders), it can fill in the missing data with model estimates. Our results show that the existing actuarial dependence models, such as linear correlation and copulas, and frequency distribution, such as binomial and Poisson distribution, systematically misjudge cyber risks. This implies that regulatory capital models underestimate the strength and nonlinearity of dependence. Moreover, network pandemics allow for analysis of systemic events and worst-case scenarios. In addition, insurers can differentiate premiums based on the connectivity and IT security levels of the policyholder. This enables risk adequate pricing and internalization of systemic costs.

Zusammenfassung

Der Einsatz neuer Informationstechnologien (IT) hat das Leben der Menschen in weiten Bereichen verbessert. Die Kehrseite der Medaille ist jedoch, dass die Gesellschaft stärker von IT abhängig geworden ist. Neue Bedrohungen, die die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Services beeinflussen, sind eminent und werden unter dem Begriff Cyberrisiken zusammengefasst. Aufgrund ihrer Neuartigkeit wurden Cyberrisiken weder in der Forschung detailliert untersucht, noch konnten Versicherer damit bereits Erfahrung sammeln. Diese Dissertation setzt hier an, indem sie in vier kumulativen Beiträgen Cyberrisiken näher analysiert und Handlungsempfehlungen für Versicherer und Aufsichtsbehörden herleitet.

Der erste Essay setzt den Rahmen für die weiteren Arbeiten, indem er einen umfangreichen Überblick über die bestehende Literatur zu Cyberrisiken liefert und offene Forschungsfragen identifiziert. Über 200 wissenschaftliche Artikel, Beiträge und Interviews mit der Versicherungsindustrie wurden strukturiert und ausgewertet. Das Ergebnis zeigt, dass spezifische Charakteristiken von Cyberrisiken, wie Verteilungen mit dicken Enden und starke, nicht-lineare Abhängigkeiten, Ursachen für die fehlende Versicherbarkeit sind. Weiter Hindernisse für die Versicherbarkeit sind fehlende Daten und als Folge unzulängliche und unsichere Modelle. Der Artikel wurde 2016 im *Journal of Risk Finance* publiziert.

Der zweite Essay befasst sich mit der Frage, ob die aktuellen regulatorischen Kapitalanforderungen für Versicherer der Bedrohung durch Cyberrisiken gerecht werden. Dazu wird ein prototypisches Versicherungsportfolio bestehend aus einzelnen Cyber-Policen modelliert, aggregiert und mit den regulatorischen Risikomassen ausgewertet. Diese werden anschließend mit den regulatorischen Kapitalerfordernissen verglichen. Die Analysen zeigen, dass die herkömmlichen regulatorischen Modelle den neuartigen Cyberrisiken nicht gerecht werden. Dazu berücksichtigen sie die Verteilungen mit dicken Enden und starken Abhängigkeiten zu wenig. Das Paper wurde 2019 im *North American Actuarial Journal* (online) publiziert.

Im dritten Essay wird der Cyberversicherungsmarkt in seiner Gesamtheit modelliert. Indem die Interaktion zwischen Nachfrage und Angebot analysiert wird, wird auf die mögliche Existenz eines Cyberversicherungsmarkts geschlossen. Damit wird erklärt, warum der Markt für Cyberversicherungen hinter den Erwartungen geblieben ist. Wir

finden, dass die hohen Kosten, Informationsasymmetrien, Modellierungsrisiken, die allesamt mit der Neuartigkeit von Cyberrisiken verbunden sind, sowie starke Korrelationen in extremen Ereignissen das Marktversagen erklären können.

Der letzte Essay befasst sich mit der Analyse von Abhängigkeiten zwischen einzelnen Cyberrisiken (-policen). Unvollständige Datensätze machen das Modellieren von Abhängigkeiten und Häufigkeiten schwierig. Der induktive Ansatz eines Netzwerkepidemiomodells, der die Ausbreitung von Bedrohungen zwischen einzelnen Entitäten modelliert, ermöglicht die unzulänglichen Daten mit Modellschätzungen zu ergänzen. Die Analysen zeigen, dass die gängigen aktuariellen Modelle für Abhängigkeiten, wie lineare Korrelation, Copulas, sowie für Häufigkeiten, wie die Binomial- und Poisson-Verteilungen, Cyberrisiken systematisch falsch einschätzen. Unter anderem impliziert dies, dass die regulatorischen Modelle die Stärke und Nicht-Linearität der Abhängigkeiten unterschätzen. Zudem ermöglichen Netzwerkepidemiomodelle das Analysieren von systemischen Ereignissen. Versicherungen können Prämien aufgrund der Netzwerk-Zentralität und Sicherheitsvorkehrungen einzelner Kunden differenzieren und so systemische Kosten internalisieren.

Essay I

What do we know about cyber risk and cyber risk insurance?

Martin Eling & Werner Schnell

Abstract

Purpose – This paper aims to provide an overview of the main research topics in the emerging fields of cyber risk and cyber risk insurance. The paper also illustrates future research directions, from both academic and practical points of view.

Design/methodology/approach – The authors conduct a literature review on cyber risk and cyber risk insurance using a standardized search and identification process that has been used in various academic articles. Based upon this selection process, a database of 209 papers is created. The main research results findings are extracted and organized in seven clusters.

Findings – The results illustrate the immense difficulties to insure cyber risk, especially due to a lack of data and modelling approaches, the risk of change and incalculable accumulation risks. The authors discuss various ways to overcome these insurability limitations, such as mandatory reporting requirements, pooling of data or public–private partnerships in which the government covers parts of the risk.

Originality/value – Despite its increasing relevance for businesses at present, research on cyber risk is limited. Many papers can be found in the IT domain, but relatively little research has been done in the business and economics literature. The authors illustrate where research stands currently and outline directions for future research.

Keywords

Risk management, accumulation risk, cyber insurance, cyber risk, insurability

Status

This paper has been published 2016 in *Journal of Risk Finance*, 17(5), 474–491. <https://doi.org/10.1108/JRF-09-2016-0122>. It was prepared as part of the Geneva Association Cyber Stocktaking Initiative. An extended version of this paper, including all supplemental material, is available on the website of the Geneva Association.

Acknowledgements

This paper greatly profited from discussion with numerous academics and practitioners. The authors are especially grateful to Daljitt Barn, Nick Beecroft, Maya Bundt, Eric Durand, José Fidalgo, David Ho, Ruo Jia, Kwangmin Jung, Benno Keller, Martin Lehmann, Philipp Lienau, Patrick Smolka, Fabian Sommerrock and Jan Wirfs for their valuable feedback and comments.

1 Motivation and aim of the paper

Despite its increasing relevance for businesses today, research on cyber risk is limited.¹ Many papers can be found in the IT domain, but relatively little research has been done in the business and economics literature. The existing articles emphasize the lack of data and modelling challenges (see, e.g., Maillart & Sornette, 2010; Biener, Eling, & Wirfs, 2015a), the complexity and dependent risk structure (see, e.g., Hofmann & Ramaj, 2011; Ögüt, Raghunathan, & Menon, 2011), and adverse selection and moral hazard issues (see, e.g., Gordon, Loeb, & Sohail, 2003). More applied research is concerned with the potentially huge losses from worst-case scenarios such as the breakdown of critical infrastructure (see, e.g., WEF, 2010; CCRS, 2014; Lloyd's, 2015b; Long Finance, 2015). In short, the existing studies highlight the challenges in the risk management and insurability of cyber risks.

The aim of this paper is to establish a database on studies, articles, and working papers on cyber risk and cyber risk insurance². Based on this goal, we provide insurance practitioners and academics with an overview on the main research topics and future research directions in the field. The focus of the analysis is on the business and economics literature in the field of risk and insurance. In order to provide a structured discussion, we pursue seven core topics:

1. Definition and categorization of cyber risks
2. Costs and detrimental effect caused by cyber risk
3. How to find data on cyber risk
4. How to model cyber risk
5. How to organize cyber risk management
6. Whether cyber risk is a threat to the global economy and society
7. What does the cyber insurance market look like, and what are the main insurability challenges?

We first present a short description of the methodology (Section 2). Then we provide a

¹ As shown in Appendix A, research on the topics of cyber risk and cyber insurance has been very limited until the year 2010, but since then it has grown exponentially. This emphasizes the increasing relevance of the topic, from both a practical and an academic perspective.

² In this paper, we use the terms cyber risk insurance and cyber insurance interchangeably.

structured review of the existing literature considering the above seven research topics (Section 3). Finally, we consider what the insurance industry and the government³ might do to prevent cyber risk and to support cyber insurance. Potential research questions for academics are also formulated (Section 4).

2 Research approach

We conduct our review on cyber risk and cyber risk insurance using a standardized search and identification process that has already been used in various academic articles (see, e.g., Biener & Eling, 2012; Biener et al., 2015a, 2015b). First, we search for the terms “cyber risk,” “cyber risk insurance,” and “cyber insurance” in the journal databases EBSCOhost (Business Source Premier and EconLit) and ABI/INFORM Complete. In addition, we search for the same terms in the Social Science Research Network (SSRN) and via Google Scholar. We then review journal issues from January 2000 to December 2015 from a predefined list of journals⁴ and also review all working papers from the annual meetings of the American Risk and Insurance Association (ARIA) for 2011, 2012, and 2013, the 2010 and 2015 World Risk and Insurance Congress, and other relevant conferences in the fields (EGRIE, APRIA). Finally, we review citations in the identified papers to explore additional relevant materials.

Based upon this selection process, a database of 209 papers is created, and the main research results findings are extracted. In Appendix C, we structure the papers by year, author (academic, industry), discipline (Economics, Finance/Insurance/Risk Management, IT, Law, Management), and methodology (Empirical, Theoretical, Data Collection, Qualitative). We also classify the studies within the risk management process by a set of selected key words. The review contains papers published between January 2000 and May 2016. On the highest hierarchical level, we identify seven different research clusters (or core topics) that form the structural basis for the discussion presented in

³ Our view on the government includes all potential activities by public authorities, including legislation, regulation, and other work of the authorities.

⁴ Journal of Finance, American Economic Review, Journal of Risk and Insurance, Insurance: Mathematics and Economics, Geneva Papers on Risk and Insurance - Issues and Practice, and The Geneva Risk and Insurance Review. Other journals from the field of risk and insurance are also reviewed (Journal of Insurance Regulation, Risk Management & Insurance Review, ASTIN Bulletin, North American Actuarial Journal, European Actuarial Journal).

Section 3.

3 Research results

3.1. Definition and categorization of cyber risk

We scan all 209 references for different definitions of cyber risk and systematically compare them (see Appendix D). Since our focus is on cyber risk from an insurance perspective, we propose a definition comprising all risks that show similar characteristics (e.g., with respect to distribution, correlation, and mitigation instruments) in order to facilitate the modelling and management of such risks.

Cyber risks can be classified according to the activity (e.g., criminal and non-criminal), the type of attack (e.g., malware, insider attack, spam, distributed denial of service, and botnet), and the source (e.g., terrorists, criminals, government). The attacks depend mainly on criminal activity and are reinforced by network effects (e.g., worms). The **vulnerability** of the company then determines whether an attack is successful. As the vulnerability is determined to some extent by organization-specific parameters such as technology, processes, and people, it is characterized by an idiosyncratic risk component, and an insurer potentially faces moral hazard. Moreover, due to the public good character of IT security investments (the security level of a company depends on security measures of other partners in the supply chain), companies tend to invest less than the amounts optimal for the economy (Biener et al., 2015a). Finally, regarding the **consequences**, depending on the aim of the attackers (e.g., espionage, sabotage, extortion, and exploiting information), the attack might compromise the availability of IT services, the integrity and confidentiality of data that in turn lead to monetary loss, reputational damage, business interruption (see CRO Forum, 2014), and even damage to humans.

The term “cyber” has **two constitutive elements**, i.e., it relates to electronic communication **networks** and **virtual reality**. Both characteristics fundamentally distinguish cyber risk from other types of risks. Firstly, the virtual reality emphasizes the intangible nature and therefore the difficulties in assessing the losses. Secondly, networks are closely connected to the term cyberspace, which is frequently used synonymously with the Internet. While the Internet might be the main source of cyber threats (due to its public domain), cyberspace describes every network that connects IT systems (e.g., LAN, WAN). Several other definitions emphasize the significance of networks (Swiss

Re, 2014; CRO Forum, 2014; Lloyd's, 2015a, 2015b; Willis, 2013a).

In comparison, other authors do not stress the term “network” explicitly as constitutive and use **broader definitions**. For example, Cebula and Young (2010) define cyber risks as “operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems”. Similarly, the National Association of Insurance Commissioners (2013) lists identity theft, disclosure of sensitive information, and business interruption as examples of cyber risk. Other researchers investigate **only one particular type** of cyber risk, such as data breaches (Böhme & Kataria, 2006). Others see the **motivation of the attacker** as relevant. For instance, Mukhopadhyay et al. (2005, 2013) concentrate only on malicious events.

Another relevant aspect with respect to insurance is that cyber risk can affect insurance companies in two fundamentally different ways. Firstly, since an insurance company relies critically on its IT infrastructure, it is highly vulnerable to cyber risk. This exposure is treated by a regulatory framework as part of the operational risk category (**operational cyber risk**). Secondly, writing cyber risk policies seems to be an attractive business opportunity for insurance companies (**underwriting cyber risk**). Both aspects should be considered in risk management and the regulation of insurance companies.

Overall, it must be emphasized that **cyber risk's characteristics** are distinct from those of most other common risks. While most insurers have historically provided protection mainly for rather uncorrelated risk (e.g., motor insurance), cyber risks might be significantly correlated with each other (e.g., Ögüt, Raghunathan, & Menon, 2011). The global interconnection of different IT systems causes geographical boundaries that would potentially provide some segmentation to vanish. Moreover, as the production of IT systems is characterized by huge economy of scales, the variety of products in the market is limited. Thus, if a security leak is spotted, it can be exploited in a multitude of systems. This homogeneity is especially true for the systems that should provide IT security (e.g., antivirus software). Eling and Wirfs (2016a) derive the main characteristics of cyber risk as follows: Cyber risks are highly correlated and global, result in first- and third-party losses, and can be both short-tail and long-tail. Eling and Wirfs (2016a) also distinguish between the “cyber risks of daily life,” such as the usual hacker attack on a single company which is insurable today, and extreme risks, in which cyber losses are not independent (leading to potential accumulation risk).

3.2. Costs and detrimental effect caused by cyber risk

Estimating the costs caused by cyber risk is difficult, as there is high uncertainty and no accepted source of information. Some types of cybercrime might even generate no costs at all or cannot be quantified (e.g., spreading of racism, mobbing, or trading of illegal drugs). However, several industry contributions try to estimate the overall costs, costs per incidence, and cost per record of a data breach (see Appendix E for an overview). The **global costs of cyber risk** are generally estimated to be above one hundred billion US\$, which emphasizes the economic significance of cyber risk. However, depending on the definition applied, the estimates vary quite substantially. While Symantec (2013; estimating 113 billion US\$) takes only direct costs into account, McAfee (2014; estimating 445 billion US\$) also incorporates indirect costs such as the reputational costs for the hacked company. The wide range provided by Kshetri (2010; estimating between 100 and 1,000 billion US\$) is based on secondary literature and emphasizes the considerable uncertainty present when estimating cyber risk costs. The costs per data breach a hacked company faces show less variation and are estimated to be between 2.1 to 3.8 million US\$. Moreover, the loss of each record (e.g., credit card number) generates costs from 217 to 956 US\$. McAfee (2014) also provides estimates of the cyber risk costs for different countries, showing strong variations between different countries (e.g., 0.64% (1.60%) of GDP for the US (for Germany)).

Given these extreme ranges, it seems that the existing cost estimates are far from perfect. Moreover, the numbers must be interpreted with caution, as most of them have been estimated by security firms and consulting companies that might have **incentives to inflate the cost estimates** to benefit their business. Anderson et al. (2013) discuss the methodological flaws of such estimates and suggest an improved alternative, which, however, in aggregate also yields a number in the hundreds of billions of US dollars.⁵ Anderson et al. (2013) also argue that a majority of cyber costs are **indirect losses** (e.g., loss of trust) and defence costs (e.g., antivirus software, insurance), excluding direct losses (e.g., theft of money).

As a way to comprehensively evaluate both direct and indirect effects, several studies investigate the effects that cyber risk incidences have on companies' **stock prices**. For

⁵ The authors, however, explicitly say that an aggregation is not meaningful.

example, Cavusoglu et al. (2004) show in an event study that a security breach negatively affects a company's stock price. They estimate the loss to be as high as 2.1% of the market volume or 1.65 billion US\$ per security breach.⁶ A major part of the discount is explained by the reputational damage (Sinanaj & Muntermann, 2013). On the contrary, Campbell et al. (2003) as well as Hovav and Arcy (2003) find only limited evidence that data breaches or denial of service attacks negatively influence the company's stock price. However, Campbell et al. (2003) show that a breach of confidential data has a larger negative effect on the stock price than non-classified information; Hovav and Arcy (2003) show a negative price effect for companies with a business model that is heavily based on the Internet. Thus, market participants seem to behave rationally, as the discount is proportional to the expected loss associated with different data.

3.3. How to find data on cyber risk

The **availability of data** on cyber risk is rather **scarce**. This might be because institutions that have been compromised do not disclose incidences (Symantec, 2016). However, since 2002, US entities that experienced security breaches are required to report the incidence to their customers and other parties (NCSL, 2016), which enhances data availability. But even if historical data are available, the **fast-changing environment** for cyber risk might render these data useless (CRO Forum, 2014). Some sources for aggregated cyber risk statistics have already been discussed in the previous section. In Panel A of Appendix E, we list all sources for aggregated cyber risk data we found in our review. The usefulness of aggregated statistics is, however, limited. The most useful data for modelling would be the claims an insurer actually faces, as recorded by NetDiligence (2014). In Panel B of Appendix E, we list all additional alternative sources of **raw data** potentially suitable for **actuarial modelling**.

⁶ Interestingly, Cavusoglu et al. (2004) also show that stock prices of information security providers increase on average in value by 1.36%, or 1.06 billion US\$, after the announcement of another company's security breach.

3.4. How to model cyber risk

Maybe due to lack of data, there is no established method to model cyber risk, and not much research has been done so far. Some authors also suggest avoiding the use of the classical stochastic modelling, and rather relying on scenario approaches instead (Lloyd's, 2015b). Rakes, Deane, and Rees (2012) argue that, especially for sparse but high-impact IT security breaches, it might be better to rely on an expert's judgement in defining worst-case scenarios and their likelihood.

Two of the few papers that model cyber risks with stochastic modelling techniques are Maillart and Sornette (2010) and Wheatley, Maillart, and Sornette (2016). The first one investigates personal **data breaches** (e.g., credit card, social security numbers, banking accounts, or medical files) and finds that the frequency of such incidences has been exponentially growing during the period from 2001 to 2006. However, from 2006 onwards, the development reached a plateau. Moreover, the authors find that the severity per incidence is extremely **heavy-tailed-distributed** (Pareto index of 0.7) and that the laws governing its distribution have been stable over time. While personal data breaches are only one type of cyber risks, the authors argue that this finding is representative for other types of cyber risks originating from the Internet. Building upon this work but with up-to-date and broader data set, Wheatley, Maillart, and Sornette (2016) conduct a similar analysis and find that the number of breached items per incidence has been even heavier-tailed-distributed since 2007 (Pareto index of 0.37 for 2015). The size of data breaches is expected to double in the next five years, from an estimated 2 billion personal items to 4 billion.⁷

The results show that the laws governing the properties of cyber risk, whether frequency or severity, are highly dynamic. Also, the **fast-changing technology environment** requires continuous revisions of modelling approaches. The quality of available data also

⁷ Similarly, Edwards, Hofmeyr, and Forrest (2015) investigate trends in data breaches between 2006 and 2015. However, they find no evidence for an increasing trend in frequency or in severity (number of records per incident). They argue that the widespread intuition that frequency and severity of data breaches increase might be just an artefact of heavy-tailed loss distributions (while severity is best described by the log-normal distribution, the frequency follows a negative binomial distribution). Eling and Wirfs (2016b) apply a dynamic version of the peaks over threshold approach from extreme value theory and consider a self-constructed database of cyber loss incidents.

limits the improvements that can be made in modelling. Especially for insurance purposes, the number of data breaches is not sufficient to calculate premiums, capital, or reserves. Instead, to each data breach, a price tag corresponding to the potential claim must be allocated. Finally, classical risk or premium measures based on mean and variance might fail to be applicable, and the merits of diversification might vanish due to the infinite moments that characterize cyber risks (see, e.g., Chavez-Demoulin, Embrechts, & Nešlehová, 2006).

In addition to modelling the marginal distribution of cyber risk, the second challenge is their **aggregation**, especially when the risks are correlated, as is the case with cyber risk. Indeed, correlation of cyber risks has been discussed as being detrimental to the development of a cyber insurance market. Böhme and Kataria (2006) systematically investigate correlations on two levels. Firstly, an event could affect several systems within a single entity (e.g., company). Secondly, there is a correlation across different entities (e.g., an insurer's portfolio of policies). The authors build a model describing that insurance is especially suited for risks that show **high internal and low global correlation**. The implication is that low internal correlation would allow a company to eliminate the risk by self-protection more efficiently. Moreover, a high global correlation is detrimental to the insurer's diversification merits and would drive the charged premium up. The authors suggest that increasing diversity of the system platforms could reduce internal and external correlation. For example, the government should use competition laws to increase the diversity of available software products.

Due to rather **complex dependencies**, aggregation of different cyber risks can be quite challenging. The use of copulas has an advantage in that it allows for any potential marginal distribution (what might be especially helpful for the diverse cyber risk classes) and accounts for non-linear dependencies. Böhme and Kataria (2006) suggest the t-copula, as it is suitable for modelling the correlation of extreme events. However, these researchers employ the t-copula purely for simulation exercises and emphasize that better data would be required in order to estimate suitable copulas and parameters empirically. However, they also conduct empirical tests and estimate a correlation coefficient for global attacks of only 0.03 and 0.18 depending on the model applied. Moreover, their estimates for the internal correlation coefficient are smaller than 0.1. Herath and Herath (2011) analyze losses due to virus incidents and find that the marginal distributions are not normal and the risks are correlated in a non-linear fashion. As a remedy, the authors

suggest using Archimedean copulas (Clayton and Gumbel) and conduct simulation exercises. Mukhopadhyay et al. (2013) use the normal copula to aggregate the number of failures (frequency) and the loss given default (severity), which can finally derive the overall loss distribution on a cyber risk portfolio. To conclude, as more data on cyber risk become available, research should be aimed at improving the understanding and modelling of the rather complex and interdependent cyber risk.

3.5. How to organize cyber risk management

The first and maybe most important aspect for sound cyber risk management is that cyber risk management is not the responsibility of the IT department; it requires an overarching dialog between different departments (e.g., sensitization, trainings). Moreover, the institutional commitment – demonstrated by having a person responsible for information security – is also very essential. Firms with a Chief Information Security Officer (CISO) or a similar position have lower average costs when a breach occurs (US\$ 157 per record vs. US\$ 236 per record for firms without strategic security leadership; see Shackelford, 2012).

The first step in the classical risk management process is to define the **initial situation and goals** of the cyber risk management. By now there exist a multitude of industry standards, in particular from the field of IT, which can serve as templates for cyber risk management (e.g., the family of ISO/IEC 2700x standards, the BSI-IT-Grundschutz (BSI, 2008), or the Cyber Security Best Practices (Allianz, 2011)).⁸ There also exists an opportunity to achieve certifications according to the above standards.

For the **risk identification**, relevant assets with their corresponding business processes must be identified. Afterwards, potential threats and their sources must be determined. A detailed list of current threats is provided by ISO 27005. A potential first indicator for the risk identification can be provided by a cyber-risk self-assessment (e.g., Marsh, 2016). Those tools can help to determine the risk exposure and risk awareness of a company and provide indications for unidentified risks.

A popular tool for **risk analysis** is the Business Impact Analysis. First, direct costs for

⁸ Similarly, UK's Department for Business, Innovation & Skills and Cabinet Office (2014) provides an IT security framework and a certification of its implementation.

particular scenarios are calculated, and the expected total loss of an incident can be estimated while considering the dependencies between different scenarios. The analysis must incorporate indirect effects such as potential reputational effects. Since cyber risk is a relatively new risk category, there is a lack of data for an adequate estimation of probability. Furthermore, since cyber risk is very dynamic and subject to significant risk of change, the evaluations of past statistical surveys about the future must be viewed carefully.⁹

For the actual **risk management** (avoidance, mitigation, transfer, and retention), risk avoidance (meaning no use of IT) is in many cases not plausible. Mitigating risks seems to be more effective and is most widespread with instruments to reduce the probability of occurrence (e.g., anti-virus software, firewalls, and so on) or the size of losses (e.g., emergency guidelines).¹⁰ Rakes et al. (2012) point out that most companies do not have a sound decision-making process to select the optimal security measures. Thus, they propose a framework in which different countermeasures are compared based on their suitability in reducing cyber threats. Also, the risk transfer is possible by purchasing insurance; this will be discussed in more detail later.

Since cyber risk is highly dynamic, **risk monitoring** is another key in cyber risk management. Given that the attack strategies change constantly, the risk management has to be consistently improved. A thorough communication and information sharing are of high interest for cyber risk in order to reinforce the security know-how and awareness in the whole company.

3.6. Is cyber risk a threat to the global economy and society?

One of the most striking questions when it comes to discussing cyber risk is an extreme scenario in which a breakdown of the critical infrastructure takes place due to technical failure or criminal activity. In theory, it could lead to massive economic losses (see WEF, 2015) and to a breakdown of any cyber insurance market due to the huge accumulation risk. Numerous scenarios were developed and widely discussed both among academics

⁹ See also Office of the Superintendent of Financial Institutions (2013).

¹⁰ See CIS (2016) or ASD (2014) for guidance on how IT security measures, such as access control, authorization of devices and software, malware defense, and network configuration, should be used.

and practitioners (see, e.g., RMS, 2016; CCRS 2014, 2016).¹¹ But how likely is such an extreme event?

Although many experts are convinced that a (global) breakdown of the Internet is unlikely¹², in the past, regional but large-sized breakdowns have been possible. For example, in March 2013, a truncation of several submarine cables led to an incident in which almost the whole African continent was disconnected from the Internet for almost a day.¹³ The exact cause is unclear, but it might be as simple as fishing nets becoming entangled in the cable. At least partial failure of the Internet is thus possible. This is problematic, especially against the background that there is relatively little contingency planning for such a scenario today. Although today many states have defined first national strategies to protect critical infrastructure, a real plan in case of a widespread failure does not exist.

Such a plan is also very important in light of the potential consequences of an extreme event, such as the breakdown of the Internet. For example, the World Economic Forum (2010) estimates a breakdown of critical information infrastructure at 10% probability in the next decade and the financial consequences (losses) within the first few days after the breakdown at about US\$ 250 billion. Such a scenario would stop all general communication such as text-messaging services or emails. Cloud systems and online banking are no longer available, and the data stored in the systems are no longer accessible

¹¹ Worst-case scenarios in which IT systems, data, networks, and services are affected on a large scale (e.g., critical infrastructures) are sometimes called “Cybergeddon”. The scenario, “Cybergeddon”, described by WEF (2014), features an unruly cyber space in which attackers have gained the upper hand for good. The permanent disruptions would finally impair trust and individuals, and organizations would seek to reduce their reliance on ICT.

¹² This assessment is usually justified by the architecture of the Internet; it is highly decentralized, is distributed over many servers and devices in different places, and is very robust and resilient (see, e.g., Ahamad, 2012; Beckstrom, 2012). However, a few recent research papers question the robustness of the Internet. Bashan et al. (2013) show in a network model that a failure of the Internet is certainly possible. Moreover, Hochstätter and Masiero (2009) argue that the Internet Exchange Points (IXPs) are especially very vulnerable to attack from cyber-terrorists due to the dominant position of the router manufacturer for these IXPs. Another danger can be seen in attacks on Domain Name System (DNS) servers.

¹³ A second example was the breakdown of the Korean Internet in December 2013. Recently, also the majority of the Swiss commercial Internet services broke down for almost a full business day (on May 24, 2016) after a software failure.

(see Strickland, 2010). In addition, all websites are offline, so there is no online-based business activity anymore (e.g., with Amazon). Furthermore, the failure of the Internet can lead to far-reaching problems in the supply chains of industries. Manufacturing companies are increasingly connected with suppliers and customers via the Internet so as to enable an efficient just-in-time production (see, e.g., Hochstätter & Masiero, 2009). Moreover, the capital market on exchanges and Internet platforms cannot be executed (see, e.g., Hochstätter & Masiero, 2009).

3.7. What does the cyber insurance market look like, and what are the main insurability challenges?

Commercial property and liability insurance are available in most insurance markets worldwide.¹⁴ However, most policies only cover damage to physical assets such as production facilities and exclude cyber risk. Also, the contract terms sometimes do not include information regarding whether cyber events might be relevant (Lloyd's, 2015b). While the customer might think that cyber incidents are covered, the insurer assumes that they are not. As this ambiguity might cause legal disputes, the judge's discretion and the legal costs increase the insurers' financial risk. As a consequence, insurers seek to state more explicit contract terms in two ways. Either the insurer could adapt its policies by explicitly excluding them from traditional policies and providing dedicated policies (standalone cyber policy) or it could explicitly include them and adjust the premiums accordingly (affirmative cyber policy).¹⁵

Recently, a specialized market providing coverage for cyber risks has emerged, most prominently in the US. As of yet, however, market coverage is small. Moreover, outside the US, cyber insurance coverage is not well known and little used. In Europe, many corporations are not even aware that this type of insurance exists, and only few have purchased coverage (Marsh, 2013). Figures for the US show a similarly low average level of coverage at about 6%, but large variations exist between industries among the

¹⁴ Note that the majority of the discussion on cyber insurance refers to commercial insurance. Cyber insurance for retail customers is a new field with only few applications and examples. For this reason, the majority of the discussion in this paper focuses on the commercial insurance market.

¹⁵ See London Institute clause 380, ISO Electronic Data Exclusion (2004), Data Breach Exclusion (2014), NMA 2912, 2914, and 2915 clauses (2001). This approach also has its limitations, especially as the digital world and the physical world are converging more and more.

Fortune 1000 companies (Willis, 2013b). According to Betterley (2015), the current annual gross premiums for cyber insurance in the US are US\$ 2.75 billion and growing by 26-50% on average per year. Advisen (2015) estimates the premium volume for the US market in 2015 at US\$ 2.4 billion. The premium volume in continental Europe is estimated to be around US\$ 192 million, but this figure is expected to reach US\$ 1.1 billion in 2018 (NAIC, 2013). Swiss Re expects an increase of the global cyber insurance premium volume to US\$ 5.9 billion until 2023 (Swiss Re, 2014).

The US market is much more developed than its European counterpart, partly because the US has had reporting requirements in place for cyber-attacks for several years with relatively heavy fines for violations. The new regulations have considerably increased the awareness of cyber risk and increased the demand, especially for third-party coverage. The few policies that already exist in Europe focus more on first-party coverage. In 2018, obligations to report data breaches will be also introduced in the European Union, which might be an important driver in the development of the European cyber insurance market.

Biener, Eling, and Wirfs (2015) discuss cyber risk beyond the background of the insurability criteria by Berliner (1982), outlining three major insurability problems of cyber risk. The first problem is that the independence and predictability of losses are not given; thus, the risk pooling might not always work appropriately. A second significant problem is information asymmetry. Companies that have experienced a serious cyber-attack are more likely to buy insurance (Shackelford, 2012), thus resulting in adverse selection. Insurers alleviate adverse selection effects through screening (e.g., up-front audits), self-selection (e.g., underwriting questionnaires), and signaling (e.g., certificates for IT-compliance). In addition, there is moral hazard, i.e., the change of behavior after purchasing insurance. One example is the insured's reduced incentive to invest in self-protection measures following the purchase of insurance if full coverage is offered. Insurers use screening (e.g., audits) and risk sharing (e.g., deductibles, cover limits) to reduce moral hazard. The third essential problem for the development of an insurance market is that the existing policies only cover small losses (US\$ 10 million to US\$ 50 million, depending on the product and provider, see Biener et al. (2015a); in some cases even up to US\$ 100 million, see Finkle, 2015) and contain several exclusions (e.g., self-inflicted losses, access to unsecure websites, or terrorism). Potential extreme scenarios can thus not be well covered by existing insurance policies. Given the large number of exclusions

and the dynamic nature of cyber risk, there is uncertainty about what the cyber policy actually covers. The policies in the market also have no agreed-upon terminology, which makes the offerings very difficult to compare. So overall, the available policies do not really cover what the supply side is looking for: efficient protection not for the small risks, but for the extreme cases which might lead to big losses.

The cyber insurance market is thus still in its early stages. But as market development continues, the risk pools will become larger and more data will be available. Several new competitors have entered the market and have also started collecting data; more are planning to do so. This will increase insurance capacity and competition and push prices down. Additionally, it will lead to more uniform terminology and standardization of products. In light of our discussion, it might also be important to establish standards on definitions, coverage, and pre-coverage risk assessment, all of which will help to reduce some of the problems of insuring cyber risk.

Table 1. Summary of results

1. Definition and categorization of cyber risk
- Any risk emerging from the use of IT that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology eventually leads to business disruption, infrastructure break down, and physical damage to humans and properties. - Cyber risk is either caused naturally or man-made, where the latter can emerge from human failure, cyber criminality (e.g., extortion, fraud), cyber war, and cyber terrorism. It is characterized by interdependencies, potential extreme events, high uncertainty with respect to data and modeling approach, and risk of change.
2. Costs and detrimental effect caused by cyber risk
- The enormous global cost estimates (up to 1000 b US\$ per year) published by software firms and consultants are rough estimators that need to be critically questioned. - The manifold detrimental effects have been analyzed, e.g., using event studies and scenario analyses. The major part of the effects is indirect (reputation, loss of trust).
3. How to find data on cyber risk?
- Data on cyber risk is scarce, e.g., because the victims are reluctant to report such events. - Most empirical papers on cyber risk rely on data breach information (not loss information), but recently first loss databases have been set up (NetDiligence in the US; Biener, Eling and Wirfs, 2015, globally).
4. How to model cyber risk?

- Frequency and severity modelling of cyber risk can be done by applying extreme value theory and the peaks over threshold approach. Heavy tail distributions have been proposed, e.g., the power law or the log-normal distribution for the severity and negative binomial distribution for the frequency. - The aggregation of cyber risk needs to take nonlinear dependence into account (typically applying copulas). The few existing modelling papers emphasize the immense modelling difficulties and risk of change. Scenario analysis is a popular tool in such situations.
5. How to organize cyber risk management?
- There are special standards and tools for cyber risk management. In each step of the classical risk management process, cyber risks show special features. - Institutional commitment; effective crisis management; risk communication with employees, customers, and suppliers; and continuous monitoring are fundamental. Cyber risk management today focuses on risk mitigation, while the risk transfer so far plays only a minor role.
6. Is cyber risk a threat to the global economy and society?
- A global failure of the Internet is rather unlikely, but regionally limited breakdowns have already occurred; given the globally connected economy and society, the potential consequences of such extreme scenarios on companies and individuals are massive. - The same holds for other cyber scenarios, such as the blackout of energy systems. For insurers, such scenarios pose enormous accumulation risk and hamper insurability.
7. What does the cyber insurance market look like, and what are the main insurability challenges?
- The cyber insurance market is very small at present but is expected to increase significantly in the next years. The US is far ahead Europe, e.g., because of reporting requirements. - The main insurability problems are the lack of data, risk of change, accumulation risk, and potential moral hazard problems.

4 Derivation of potential future work

Table 1 summarizes the main results for the seven core topics. Based on these results, we now discuss the potential areas of future work both from an academic as well as from a practical perspective. First, we consider what the insurance industry and what the government might do to prevent cyber risk and to support cyber insurance. We also acknowledge the important role of other fields (e.g., IT security) in developing the topic of cyber risk and cyber insurance, which are partly discussed but are not the main focus of this paper.

4.1. Practical perspective

One of the current problems in the management of cyber risk is the lack of standards, common language, and best practices. The insurance industry could be an important lever by which to **collect** and spread such **information**. One first approach could be to publish methods (or standards or good practices) for cyber risk assessment. One element, for example, could be to provide a common scheme to classify cyber-related loss events. The insurance industry can also further intensify the analysis of extreme loss scenarios in order to identify a better sense of potential probabilities and loss severities given such an event. Risk management approaches for complex crises, i.e., methodologies, models, or tools for mastering complexity, are needed. Such approaches are useful not only for the insurance industry itself, but also for their clients and society in general. One important activity could also be that the insurance industry initiates or further intensifies the dialogue on cyber risk with the relevant stakeholders, one of which is the government. For example, the insurance industry could support the government in the preparation of national cyber risk strategies.

Another aspect on the technical side is the continuous tracking of the **technological development**. This is especially important, given that new technologies might accelerate cyber risk. One example is cloud computing, and the question one must address is then how to protect the cloud. The integrity and confidentiality of outsourced data can be highly questioned. Moreover, as the Internet of Things develops, another question arises regarding how to prevent attacks on autonomous systems such as smart grids. The Internet of Things will increase the vulnerability of the operational technology. Another example might be the blockchain technology, e.g., in the context of the bitcoin-technology, which is increasingly used by Fintecs, but also by traditional banks. In general, it seems that there is a high dependence on a few platform providers (e.g., cloud service providers like Amazon, Google, and Microsoft) and software firms (e.g., Microsoft, Oracle, and SAP). If one of them fails, it would have a significant impact on millions of people and organizations simultaneously. From a risk management point of view, one important issue to be addressed is thus what architectural improvements of a company's IT system might increase resilience to cyber risk. From the governmental side, regulation could also be directly aimed at the technology firms, e.g., by expanding product liability for IT products. Increasing diversity of IT solutions could be a way to increase overall resilience (see, e.g., Böhme, 2005).

Regarding cyber insurance, an anonymized **data pool** might be the easiest way to intervene in the insurance market. Common knowledge can be collected, standards could be established, and – most importantly – data can be collected. The implementation will thus reduce uncertainties with respect to data and to modelling. An anonymous data pool could be developed as a public-private partnership; that is, the industry can self-create and manage the pool. But before setting up the data pool, the government has to set the legal framework, especially regarding competitive law, since combining data might breach existing laws. The first types of such pools already exist in the US in the context of cyber liability insurance, although the samples are relatively small (e.g., NetDiligence, 2015, reports 160 data breach insurance claims).¹⁶

The implementation of a data pool might be connected with the creation of an **insurance pool** (see, e.g., Long Finance, 2015; Eling & Wirfs, 2016a). This approach could resolve the problems with relatively small insurance portfolios and diversification issues. One major advantage of such an insurance pool is the opportunity to accumulate risks of the same type in one portfolio, thereby guaranteeing a critical size, which is needed to benefit from diversification effects. Aside from risk sharing, the main advantage of a pool is the sharing of data and expertise in order to better understand and calculate the risks. However, from an economic point of view, the introduction of an insurance pool constitutes a severe intervention into the free markets, which can be justified only in the presence of severe market failures. A lack of insurability might be one such market failure to justify an intervention. However, the empirical question remains whether the existing risk capacity is so small that a strict intervention like pooling can be justified. Some market participants rather argue that the existing capacity is already sufficiently high so that pooling for purpose of capacity creation is not really needed.¹⁷

Finally, the insurance industry also plays an important role in **raising awareness** of

¹⁶ Also, a governmental institution could support the establishment of cyber risk databases. An example would be the National Vulnerability Database (NIST) in the US that collects reported software vulnerabilities. A central institution would be able to provide quickly relevant information on new developments so that people responsible for IT risk management can act in time.

¹⁷ The creation of a pool for cyber risk has already been discussed for the UK, specifically in the context of a reinsurance pool (Long Finance, 2015). They suggest a public-private partnership in which the insurer's retention levels and the pool's funds must be exhausted before the state enters the risk transfer as a Reinsurer of Last Resort. The UK has already adopted such schemes for other risk categories (e.g., Pool Re for terrorism and Flood Re for natural catastrophes; see Long Finance, 2015).

cyber risk and educating clients on how to deal with it. Moreover, it is also important that insurers build up the required knowledge and competences. For example, sales and risk management need to acquire specific technical IT knowledge in order to fully understand cyber risk. It might even be advisable to hire people with an IT background for such positions. Biener et al. (2015a) mention that the lack of understanding, both on the demand and supply side, is one of the main limitations in the cyber insurance market.

Looking at the role of government more specifically, these might introduce **reporting obligations** to prevent cyber risk and to promote the development of the cyber insurance market. One reason why the US insurance market is far more developed than the European insurance market is that reporting obligations for cyber-attacks have been in place for several years. The reporting obligations are connected with heavy penalties for violations and have significantly enhanced the sensitivity for cyber risks. Every manager gets the incentive to do his or her best to prevent cyber risk, because in the event of a cyber-attack, significant market discipline from investors, analysts, and customers can be expected. Reporting obligations in the European Union already passed legislation, and we believe that other countries should also discuss the introduction. It remains an empirical question whether reporting obligations might cause the same trigger effect as in the US cyber insurance market (also with differences in legal systems, risk culture, and so on when comparing Europe with the US), but we believe that it is more likely to foster the development of the insurance market.

Another measure could be the definition of **minimal standards** for risk mitigation. Minimal standards for risk mitigation will reduce moral hazard, which is one of the main insurability challenges of cyber risk. Furthermore, it might help to provide a minimal level of security, which then reduces contagion (both within a firm and outside the firm) and as such mitigates problems with dependence of losses. A regulatory intervention like this could be justified on economic grounds, given that cyber security is a public good with positive externalities.

4.2. Academic perspective

The existing research in the risk and insurance domain mainly focuses on the supply side aspects of insurability. The demand side, however, has not been subject to much research yet. More could be done, e.g., to analyze the risk perception of customers both in commercial as well as in retail business. One interesting behavioral element in this

context is the latent fatalism many people demonstrate with respect to cyber risk (“it will not happen to me”; “my data is not interesting enough”). Identifying the underlying drivers of this perception and increasing the awareness might help to create more demand for cyber risk insurance. It might also be interesting to compare the risk perception and risk aversion in the field of cyber risk insurance with other types of insurances or other types of risks (e.g., from the capital market).

In general, more empirical research is needed, both on the demand and the supply sides. Under which conditions is insurance or self-protection the more efficient risk management tool for cyber risk? What capital standards are needed for both operational and underwriting cyber risk? The link between new technologies and insurance will also give rise to research questions. For example, what should liability insurance look like in the context of self-driving cars or in the context of the Internet of Things? And what does the Internet of Things mean for the insurance idea to provide solidarity in a community of good and bad risks?

Regarding the macro perspective, more scenarios for measurement and management of accumulation risk are needed. Another question related to the macro-perspective is whether the sales of cyber insurance lead insurance companies to become systemic. Finally, the academic community should also be part of the global dialogue on how to prevent cyber risk and how to promote cyber insurance in order to provide its point of view in the discussions.

5 References

- Advisen. (2015). Cyber risk insights conference February 10th, 2015 in London. Retrieved May 4, 2016, from <http://www.advisenltd.com/wp-content/uploads/london-cyber-risk-insights-conference-slides-2015-02-17.pdf>
- Ahamad, M. (2012). What if there was a large-scale internet failure?. Retrieved May 4, 2016, from <https://www.weforum.org/agenda/2012/10/what-if-there-was-a-large-scale-internet-failure>
- Allianz. (2011). How long can a company survive without a functioning IT system?. Retrieved June 29, 2016, from https://www.allianz.com/en/press/news/company/point_of_view/news_2011-09-27.html/
- Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore,

- T., & Savage, S. (2013). Measuring the cost of cybercrime. *In the economics of information security and privacy* (pp. 265-300). Springer.
- Australian Signals Directorate (ASD). (2014). Strategies to mitigate targeted cyber intrusions. Retrieved June 29, 2016, from http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf
- Beckstrom, R. (2012). What if a hacker caused a large-scale Internet outage?. Retrieved May 5, 2016, from <https://www.weforum.org/agenda/2012/06/what-if-a-hacker-caused-a-large-scale-internet-outage>
- Berliner, B. (1982). Limits of insurability of risks. Prentice-Hall.
- Betterley (2015). The betterley report - cyber/privacy insurance market survey 2015. Retrieved May 5, 2016, from <http://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf>
- Biener, C., & Eling, M. (2012). Insurability in microinsurance markets: An analysis of problems and potential solutions. *Geneva Papers on Risk and Insurance-Issues and Practice*, 37(1), 77-107.
- Biener, C., Eling, M., & Wirfs, J. H. (2015a). Insurability of cyber risk: an empirical analysis. *Geneva Papers on Risk and Insurance - Issues and Practice*, 40(1), 131–158.
- Biener, C., Eling, M., Matt, A., & Wirfs, J. H. (2015b). Cyber Risk: Risikomanagement und Versicherbarkeit. *Institut für Versicherungswirtschaft der Universität St. Gallen*.
- Böhme, R. (2005). Cyber-insurance revisited. *Workshop on the Economics of Information Security (WEIS)*.
- Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. *Workshop on the Economics of Information Security (WEIS)*.
- Bundesamt für Sicherheit in der Informationstechnik (BSI). (2008). BSI-Standard 100-2: IT-Grundschutz: Vorgehensweise. Retrieved June 28, 2016, from <https://www.bsi.bund.de>
- Cambridge Center for Risk Studies (CCRS). (2014). Stress test scenario: sybil logic bomb cyber catastrophe. *Cambridge Risk Framework Series, Center for Risk*

Studies, University of Cambridge.

- Cambridge Center for Risk Studies (CCRS). (2016). Cyber insurance exposure data schema v1.0. Retrieved May 19, 2016, from <http://cambridgeriskframework.com/getdocument/38>
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431-448.
- 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. *International Journal of Electronic Commerce*, 9(1), 70-104.
- Chavez-Demoulin, V., Embrechts, P., & Nešlehová, J. (2006). Quantitative models for operational risk: extremes, dependence and aggregation. *Journal of Banking & Finance*, 30(10), 2635-2658.
- Cebula, J. J., & Young, L. R. (2010). *A taxonomy of operational cyber Security risks* (Technical note CMU/SEI-2010-TN-028). Software Engineering Institute, Carnegie Mellon University.
- Center for Internet Security (CIS). (2016). CIS critical security controls. Retrieved May 19, 2016, from <https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf>
- CRO Forum (2014). Cyber resilience - the cyber risk challenge and the role of insurance. Retrieved May 5, 2016, from <http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance>
- CRO Forum (2016). *CRO Forum concept paper on a proposed categorisation methodology for cyber risk* (Forthcoming).
- Department for Business, Innovation & Skills and Cabinet Office. (2014). Cyber essentials scheme: summary. Retrieved May 5, 2016, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf
- Edwards, B., Hofmeyr, S., & Forrest, S. (2015). *Hype and heavy tails: a closer look at data breaches* (Working paper). Presented at the 14th Annual Workshop of the

Economics of Information Security.

- Eling, M., & Wirfs, J. H. (2016a). Cyber risk: too big to insure? Risk transfer options for a mercurial risk class. Retrieved May 5, 2016, from <http://www.ivw.unisg.ch/~media/internet/content/dateien/institute-undcenters/ivw/studien/cyberrisk2016.pdf>
- Eling, M., & Wirfs, J. H. (2016b). *Modelling and management of cyber risk* (Working Paper).
- Finkle, J. (2015). Ace offers \$100 million cyber policies with added services, scrutiny. Retrieved: November 5, 2015, from <http://www.reuters.com>
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, 44(9), 70-75.
- Hackmageddon. (2016). Cyber attacks timeline master index. <https://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/>
- Herath, H., & Herath, T. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2(1), 7-20.
- Hochstätter, H., & Masiero, M. (2009). Angriffe auf das Internet: Wie realistisch ist der Totalausfall? Retrieved May 5, 2016, from <http://www.zdnet.de/41005661/an-griffe-auf-das-internet-wie-realistisch-ist-der-totalausfall>
- Hofmann, A., & Ramaj, H. (2011). Interdependent risk networks: the threat of cyber attack. *International Journal of Management and Decision Making*, 11(5/6), 312-323.
- Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, 6(2), 97-121.
- Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *The Journal of Strategic Information Systems*, 22(2), 175-186.
- Institute of Risk Management. (2014). IRM's cyber risk executive summary. <https://www.cgma.org/resources/reports/downloadabledocuments/irm-cyber-risk-report-executive-summary.pdf>

- Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.
- Lloyd's (2015a). A quick guide to cyber risk. Retrieved May 5, 2016, from <https://www.lloyds.com/news-and-insight/news-and-features/emerging-risk/emerging-risk-2015/a-quick-guide-to-cyber-risk>
- Lloyd's (2015b). Business blackout - the insurance implications of a cyber attack on the US power grid. Retrieved November 6, 2015, from <https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/businessblackout>
- Long Finance. (2015). Promoting UK cyber prosperity: public-private cyber-catastrophe reinsurance. Retrieved September 16, 2015, from http://www.long-finance.net/images/Promoting_UK_Cyber_Prospersity_28July2015.pdf
- National Association of Insurance Commissioners (NAIC). (2013). Cyber risk. Retrieved May 4, 2016, from http://www.naic.org/cipr_topics/topic_cyber_risk.htm
- National Conference of State Legislatures (NCSL). (2016). Security breach notification laws. Retrieved May 4, 2016, from <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>
- National Institute of Standards and Technology (NIST). (2014). Framework for improving critical infrastructure cybersecurity. Retrieved May 4, 2016, <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>
- National Institute of Standards and Technology (NIST). (2016). National vulnerability Database. Retrieved May 4, 2016, from <https://nvd.nist.gov/>
- NetDiligence. (2014). 2014 - cyber claims study. Retrieved May 5, 2016, from http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf
- Maillart, T., & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *European Physical Journal, B* 75, 357-364.
- Marsh. (2013). Cyber risk survey 2013. Retrieved May 4, 2016, from www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/partner/Partnerbeitrag_Marsh_Cyber-Risk_Survey.pdf?__blob=publicationFile

- Marsh. (2016). Marsh launches new cyber risk assessment solutions. Retrieved August 7, 2016, from <https://www.marsh.com/us/media/marsh-launches-new-cyber-risk-assessment-solutions.html>
- McAfee. (2014). Net losses: estimating the global cost of cybercrime. Retrieved March 16, 2015, from <http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf>
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukan, S. K. (2013). Cyber-risk decision models: to insure it or not?. *Decision Support Systems*, 56(1), 11–26.
- Mukhopadhyay, A., Saha, D., Mahanti, A., & Chakrabarti, B. B. (2005). Insurance for cyber-risk: a utility model. *Decision*, 32(1), 153–169.
- Office of the Superintendent of Financial Institutions. (2013). Cyber security self-assessment guidance. Retrieved June 10, 2016, from <http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx>
- Ögüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: public policy implications of correlated risk: imperfect ability to prove loss, and observability of self-protection. *Risk Analysis*, 31(3), 497–512.
- Ponemon Institute. (2015a). 2015 cost of cyber crime study – global. Retrieved March 3, 2016, from <http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report>
- Ponemon Institute. (2015b). 2015 cost of data breach study - global analysis. Retrieved March 3, 2016, from <https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF>
- Rakes, T. R., Deane, J. K., & Rees, L. P. (2012). IT security planning under uncertainty for high-impact events. *Omega*, 40(1), 79–88.
- Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber-risk management*. Springer International Publishing.
- Risk Management Solutions, Inc. (RMS). (2016). *Managing cyber insurance accumulation risk*. Centre for Risk Studies, University of Cambridge.

- Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.
- Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance. *Business Horizon*, 55, 349-356.
- Sinanaj, G., & Muntermann, J. (2013). Assessing corporate reputational damage of data breaches: an empirical analysis. *Proceedings of the 26th International Bled eConference*, 78-89.
- Strickland, J. (2010). What would happen if the internet collapsed?. Retrieved May 5, 2016, from <http://computer.howstuffworks.com/internet/basics/internet-collapse.htm>
- Swiss Re. (2014). Working together with clients to find cyber risk solutions. Retrieved May 5, 2016, from http://www.swissre.com/reinsurance/insurers/casualty/smarter_together/working_smarter_together_for_cyber_risk_solutions_in_EMEA.html
- Symantec Corporation. (2013). 2013 Norton report. Retrieved March 16, 2015, from http://www.symantec.com/content/de/de/about/downloads/2013_Norton_Report_Deck.pdf
- Symantec Corporation. (2016). 2016 Internet security threat report. Retrieved May 4, 2016, from <https://www.symantec.com/security-center/threat-report>
- Verizon. (2016). 2016 data breach investigations report. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
- Wheatley, S., Maillart, T., & Sornette, D. (2016). *The extreme risk of personal data breaches & the erosion of privacy* (Working paper) Cornell University Library. Retrieved May 5, 2016, from <http://arxiv.org/abs/1505.07684>
- Willis. (2013a). Insurance - cyber risk. Retrieved May 5, 2016, from <http://www.pwc.dk/da/arrangementer/assets/cyber-tineolsen.pdf>
- Willis. (2013b). Willis fortune 1000 cyber disclosure report. Retrieved May 5, 2016, from http://blog.willis.com/wp-content/uploads/2013/08/Willis-Fortune-1000-Cyber-Report_09-13.pdf
- World Economic Forum (WEF). (2010). Global risk report 2010 - a global risk network

report. Retrieved May 5, 2016, from <http://www.weforum.org/pdf/global-risk/globalrisks2010.pdf>

World Economic Forum (WEF). (2012). Risk and responsibility in a hyperconnected world: pathways to global cyber resilience. <https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience>

World Economic Forum. (WEF). (2014) Global risks 2014—ninth edition. Retrieved June 17, 2016, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

World Economic Forum (WEF). (2015). Global risks report 2015 - tenth edition. Retrieved May 5, 2016, from http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf

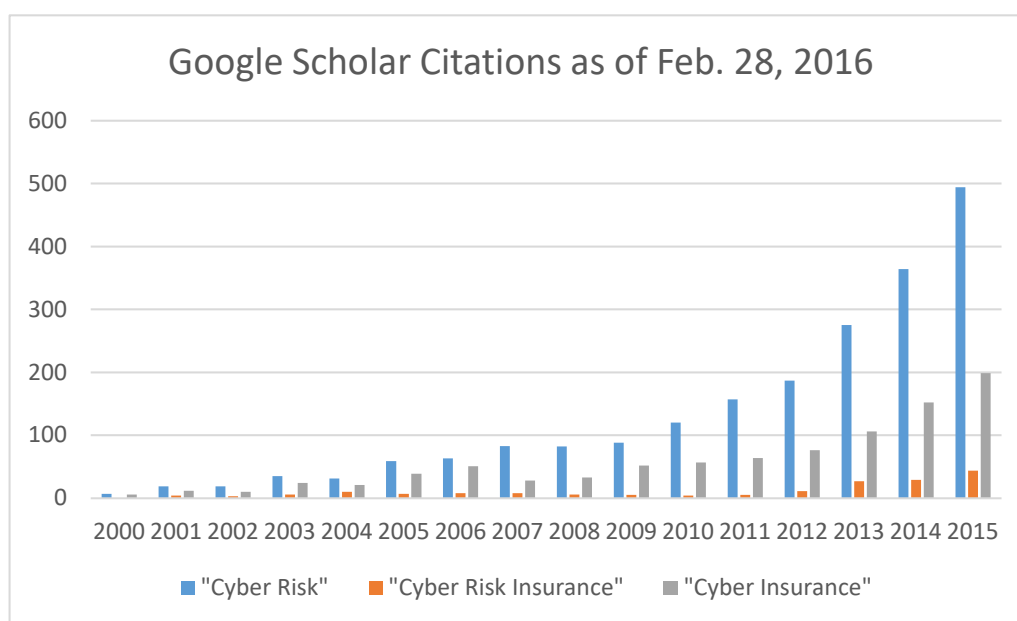
6 Appendices

Appendix A. Relevance of cyber risk and cyber risk insurance

Table A1. Google scholar citations as of 28 February 2016

Year	'Cyber Risk'	'Cyber Risk Insurance'	'Cyber Insurance'
2000	7	0	6
2001	19	4	12
2002	19	3	10
2003	35	6	24
2004	31	10	21
2005	59	7	39
2006	63	8	51
2007	83	8	28
2008	82	6	33
2009	88	5	52
2010	120	4	57
2011	157	5	64
2012	187	11	76
2013	275	27	106
2014	364	29	152
2015	494	44	199

Figure A1. Google scholar citations as of 28 February 2016



Note: Papers that contain the words 'cyber risk' or 'cyber insurance' do not necessarily discuss this topic as main field, but also might cover it as a side aspect.

Appendix B. Search and identification strategy

- We search for the terms ‘cyber risk’, ‘cyber risk insurance’ and ‘cyber insurance’ in the journal databases EBSCOhost (Business Source Premier and EconLit) and ABI/INFORM Complete. In addition, we searched for the terms in the Social Science Research Network (SSRN) and via Google Scholar.
- We review journal issues from January 2000 to December 2015 of the following journals: Journal of Finance, American Economic Review, Journal of Risk and Insurance, Insurance: Mathematics and Economics, The Geneva Papers on Risk and Insurance—Issues and Practice, and The Geneva Risk and Insurance Review. Other journals from the field of risk and insurance are also reviewed (Journal of Insurance Regulation, Risk Management & Insurance Review, ASTIN Bulletin, North American Actuarial Journal, European Actuarial Journal).
- We review all working papers from the annual meetings of the American Risk and Insurance Association (ARIA) for 2011, 2012, and 2013, the 2010 and 2015 World Risk and Insurance Congress, and other relevant conferences in the fields (EGRIE, APRIA).
- We reviewed citations in relevant studies to identify additional relevant material.

The search and identification strategy described here has been used in various projects and articles (see, e.g., www.casact.org/rpp2).

Appendix C. List of cyber risk literature

Table C1. List of cyber risk literature

ID	Title	Author(s)	Year	Journal	Source	Discipline	Method	Field RM	Keywords
1	If most of your revenue is from e-commerce, then cyber-insurance makes sense	Luzwick, P.	2001	Comput. Fraud. Secur.	Industry	Management	Qualitative	Risk Management (Mitigation, Insurance)	
2	Convention on cybercrime	Council of Europe	2001	online	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation
3	Cyber-risk management: technical and insurance controls for enterprise-level security	Siegel, C. A., Sagalow, T. R., Serritella, P.	2002	Information Systems Security—Security Management Practices	Academia	IT	Qualitative	Risk Management (Mitigation, Insurance)	IT Security
4	Risk management guide for information technology systems	Stoneburner, G., Goguen, A., Feringa, A.	2002	National Institute of Standards and Technology	Industry	IT			
5	A framework for using insurance for cyber-risk management	Gordon, L. A., Loeb, M. P., Sohail, T.	2003	Communications of the ACM	Academia	Management	Qualitative	Risk Management (Mitigation, Insurance)	Asymmetric Information, Cyber Insurance
6	The economic cost of publicly announced information security breaches: empirical evidence from the stock market	Campbell, K., Gordon, L. A., Loeb, M. P., Zhou, L.	2003	J. Comput. Secur.	Academia	Finance, Insurance, RM	Empirical	Risk Monitoring	
7	The impact of denial-of-service attack announcements on the market value of firms	Hovay, A., D'Arcy, J.	2003	Risk. Manage. Insur. Rev.	Academia	Management	Empirical	Risk Monitoring	Event Study
8	Creation of a global culture of cybersecurity, resolution 57/239 adopted by the General Assembly	United Nations (UN)	2003	online	Industry	Economics	Qualitative	Risk Management (broad sense)	Regulation

9	The impact of denial-of-service attack announcements on the market value of firms	Hovav, A., D'Arcy, J.	2003	Risk Management and Insurance Review	Academia	IT	Empirical	Risk Assessment	
10	A model for evaluating IT security investments	Cavusoglu, H., Mishra, B., Raghunathan, S.	2004	Commun. ACM	Academia	IT	Theoretical	Risk Management (Mitigation, Insurance)	IT Security
11	The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers	Cavusoglu, H., Mishra, B., Raghunathan, S.	2004	Int. J. Electron. Comm.	Academia	Finance, Insurance, RM	Empirical	Risk Monitoring	IT Security, Event Study
12	Recognising and preparing loss estimates from cyber-attacks	Smith, G. S.	2004	Inf. Syst. Secur.	Academia	Finance, Insurance, RM			
13	Insurance for cyber-risk: a utility model	Mukhopadhyay, A., Saha, D., Mahanti, A., Chakrabarti, B.	2005	Decision	Academia	Management	Theoretical	Risk Management (Mitigation, Insurance)	Cyber Insurance, Pricing, Risk Modelling
14	Cyber-insurance revisited	Böhme, R.	2005	Fourth Workshop on the Economics of Information Security (WEIS)	Academia	Finance, Insurance, RM	Theoretical	Risk Assessment	Risk Modelling, Cyber Insurance
15	The emerging cyber risks of biometrics	Barton, B., Byciuk, S., Harris, C., Schumack, D., Webster, K.	2005	Risk Management	Academia	Finance, Insurance, RM	Qualitative	Risk Identification	Data Breach
16	The effect of network topology on the spread of epidemics	Ganesh, A., Mas-soulié, L., Towsley, D.	2005	24th Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings	Academia	IT	Theoretical	Risk Assessment	

17	Models and measures for correlation in cyber-Insurance	Böhme, R, Kataria, G.	2006	Workshop on the Economics of Information Security (WEIS)	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	Risk Taxonomy, Risk Accumulation
18	The evolution of cyberinsurance	Majuca, R. P., Yurcik, W., Kesan, J. P.	2006		Academia	Finance, Insurance, RM	Qualitative	Risk Assessment	Cyber Insurance, Insurability, Asymmetric Information
19	Time-to-compromise model for cyber risk reduction estimation	McQueen, M. A., Boyer, W. F., Flynn, M. A., Beitel, G. A.	2006	Springer US	Academia	IT	Theoretical	Risk Management (Mitigation, Insurance)	Self-protection, IT security
20	Quantitative cyber risk reduction estimation methodology for a small SCADA control system	McQueen, M. A., Boyer, W. F., Flynn, M. A., Beitel, G. A.	2006	In System Sciences, 2006. Proceedings of the 39th Annual Hawaii International Conference	Academia	IT	Theoretical	Risk Management (Mitigation, Insurance)	Self-protection, IT security
21	E-risk management with insurance: a framework using copula aided Bayesian belief networks	Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sathukhan, S. K.	2006	39th Hawaii International Conference on System Sciences	Academia	Finance, Insurance, RM	Theoretical	Risk Assessment	Risk Modelling, Interdependent Risks, Risk Accumulation
22	Cyberinsurance in IT security management	Baer, W. S., Parkinson, A.	2007	IEEE Security and Privacy	Academia	Finance, Insurance, RM	Qualitative	Risk Assessment	Asymmetric Information, Self-protection, Risk Accumulation, Externalities
23	Cyber security risk assessment for SCADA and DCS networks	Ralston, P. A., Graham, J. H., Hieb, J. L.	2007	ISA transactions	Academia	IT	Qualitative	Risk Assessment	Risk Accumulation

24	A value-at-risk approach to information security investments	Wang, J., Chaudhury, A., Rao, H. R.	2008	Inf. Syst. Res.	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	
25	An economic modelling approach to information security risk management	Bojanc, R., Jerman-Blažič, B.	2008	International Journal of Information Management	Academia	Economics	Theoretical	Risk Management (Mitigation, Insurance)	IT security
26	BSI-Standard 100-2—IT-Grundschutz-Vorgehensweise	Bundesamt für Sicherheit in der Informationstechnik (BSI)	2008	online	Industry	IT	Qualitative	Risk Management (Mitigation, Insurance)	Operational Cyber Risk, Regulation, IT Security
27	Cyber attacks: cross-country interdependence and enforcement	Wang, Q.-H., Kim, S.-H.	2009	Working paper, National University of Singapore	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	Risk Modelling, Regulation, Risk Accumulation
28	Why IT managers don't go for cyber-insurance products	Bandyopadhyay, T., Mookerjee, V. S., Rao, R. C.	2009	Communications of the ACM	Academia	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Asymmetric Information, Pricing, Cyber Insurance
29	Cyber insurance as an incentive for Internet security	Bolot, J., Lelarge, M.	2009	In Managing information risk and the economics of security	Academia	Finance, Insurance, RM	Theoretical	Risk Management (Mitigation, Insurance)	Self-protection, Risk Modelling, Networks
30	Cyberattacks: does physical boundary matter?	Wang, Q.-H., Kim, S.-H.	2009	ICIS 2009 Proceedings	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	IT Security, Cyber Attacks, Interdependent Risks, Risk Accumulation
31	Supporting cyber risk assessment of power control systems with experimental data	Dondossola, G., Garrone, F., Szanto, J.	2009	Power Systems Conference and Exposition	Industry	IT	Qualitative	Risk Assessment	

32	Cybersecurity guide for developing countries	International Telecommunication Union	2009	online	Industry	Economics	Qualitative	Risk Management (Mitigation, Insurance)	
33	New cyber risk: premises for an insurance coverage	Addessi, M. E., Annibali, A., Barracchini, C.	2009	International Review of Business Research Papers	Academia	Finance, Insurance, RM	Theoretical	Risk Assessment	Risk Modelling
34	A taxonomy of operational cyber security risks	Cebula, J. J., Young, L. R.	2010	Technical Note, Software Engineering Institute, Carnegie Mellon University	Academia	IT	Qualitative	Risk Identification	Risk Taxonomy
35	The global cybercrime industry	Kshetri, N.	2010	Springer	Academia	Economics	Theoretical	Risk Identification	Cybercrime
36	Heavy-tailed distribution of cyber-risks	Maillart, T., Sornette, D.	2010	The European Physical Journal	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	Risk Modelling, Data breach
37	Global risk report 2010—a global risk network report	World Economic Forum	2010		Industry	Politics			
38	Managing risk in information systems	Gibson, D.	2010	Jones & Bartlett Learning, Sudbury	Industry	IT	Qualitative	Risk Management (broad sense)	
39	Competitive cyber-insurance and internet security	Shetty, N., Schwartz, G., Felegyhazi, M., Walrand, J.	2010	Economics of Information Security and Privacy (Springer US)	Academia	Economics	Theoretical	Risk Assessment	IT Security, Externalities, Asymmetric Information
40	A model to analyze the unfulfilled promise of cyber insurance: the impact of secondary loss	Bandyopadhyay, T., Mookerjee, V. S., Rao, R. C.	2010	Working paper	Academia	Finance, Insurance, RM	Theoretical	Risk Management (Mitigation, Insurance)	Asymmetric Information, Pricing, Insurability

41	Cyberwar: concept, status quo, and limitations	Myriam, D. C.	2010	Analysis in Security Policy	Academia	Politics	Qualitative	Risk Identification	Cyberwar
42	Modeling cyber-insurance: towards a unifying framework	Böhme, R., Schwartz, G.	2010	Workshop on the Economics of Information Security (WEIS)	Academia	IT	Theoretical	Risk Assessment	Risk Modelling
43	Interdependent risk networks: the threat of cyber attack	Hofmann, A., Ramaj, H.	2011	International Journal of Management and Decision Making	Academia	Economics	Theoretical	Risk Identification	Externalities, Risk Accumulation
44	Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection	Ögüt, H., Raghunathan, S., Menon, N.	2011	Risk Analysis	Academia	Economics	Theoretical	Risk Management (Mitigation, Insurance)	Cyber Insurance, Self-protection, Externalities, Asymmetric Information
45	Copula-based actuarial model for pricing cyber-insurance policies	Herath, H. S. B., Herath, T. C.	2011	Analyses and Actuarial Computations	Academia	Finance, Insurance, RM	Theoretical	Risk Assessment	Pricing, Risk Accumulation
46	Quantitatively assessing and visualising industrial system attack surfaces	Leverett, E. P	2011	University of Cambridge, Darwin College	Academia	IT	Empirical	Risk Identification	DoS Attack
47	The UK cyber security strategy: protecting and promoting the UK in a digital world	Cabinet Office	2011	online	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation
48	Future global shocks: improving risk governance	OECD Reviews of Risk Management Policies	2011	online	Industry	Trend studies	Qualitative	Risk Identification	
49	Incentives and barriers of the cyber insurance market in Europe	ENISA	2012		Industry				Cyber Insurance

50	10 steps to cyber security	Government Communications Headquarters (GCHQ)	2012	White Paper of the Information Security Arm of GCHG	Industry		Qualitative		
51	Should your firm invest in cyber risk insurance?	Shackelford, S. J.	2012	Business Horizon	Academia	Management	Qualitative	Risk Management (Mitigation, Insurance)	Cyber Insurance, Data breach, Cyber Attacks, Systemic Risk, Data breach
52	COBIT 5. A business framework for the governance and management of enterprise IT	COBIT	2012		Industry	Management	Qualitative	Risk Management (Mitigation, Insurance)	
53	The cyber security threat to U.S. growth and prosperity	Dowdy, J.	2012	in Securing Cyberspace: A New Domain for National Security (eds. Burns, N., and Price, J.)	Industry	Economics	Qualitative		
54	General data protection regulation	European Commission	2012		Industry	Politics			
55	Cyberisiken. Herausforderungen, Strategien und Lösungen für Versicherer	Munich Re	2012	Knowledge Series. Technology, Engineering and Risks	Industry				
56	IT security planning under uncertainty for high-impact events	Rakes, T. R., Deane, J. K., Rees, L. P.	2012	Omega	Academia	IT	Theoretical	Risk Management (Mitigation, Insurance)	Self-protection, IT security
57	Cyber security	European Commission	2012	online	Industry	Law	Qualitative	Risk Assessment	

58	Information technology—security techniques—guidelines for cybersecurity	ISO	2012	online	Industry	Management	Qualitative	Risk Management (Mitigation, Insurance)	
59	Cybersecurity policy making at a turning point, analysing a new generation of national cybersecurity strategies for the Internet economy	OECD Reviews of Risk Management Policies	2012	online	Industry	Trend studies	Qualitative	Risk Identification	Regulation
60	Risk and responsibility in a hyper-connected world: pathways to global cyber resilience	World Economic Forum (WEF)	2012	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Risk Accumulation
61	Measuring the cost of cybercrime	Anderson, R. et al.	2013	The Economics of Information Security and Privacy (Springer)	Academia	Economics	Empirical	Risk Identification	Cybercrime
62	The Betterley report—cyber/privacy insurance market survey 2013	Betterley	2013		Industry		Data collection		Survey
63	Global corporate IT security risks: 2013	Kaspersky Lab	2013		Industry				Survey
64	e-Crime—Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz	Geschonnek et al.	2013	KPMG Forensic Services	Industry				Survey
65	Cyber-risk decision models: to insure IT or not?	Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukan, S. K.	2013	Decision Support Systems	Academia	Management	Theoretical	Risk Management (Mitigation, Insurance)	Cyber Insurance, Pricing, Risk Modelling

66	Cyber risk	National Association of Insurance Commissioners (NAIC)	2013		Industry				
67	Managing cyber security as a business risk: cyber insurance in the digital age	Ponemon Institute	2013		Industry		Data collection		Survey
68	Cyber-Versicherungen haben eine große Zukunft	Behrends, J.	2013	Versicherungswirtschaft	Industry	Management	Qualitative		
69	Managing cyber risk: the trifecta	Francis, T.	2013	Am. Agent. Brok.	Industry	Management	Qualitative	Risk Management (Mitigation, Insurance)	
70	Assessing corporate reputational damage of data breaches: an empirical analysis	Sinanaj, G., Muntermann, J.	2013	Proceedings of the 26th International Bled eConference	Academia	Management	Empirical	Risk Monitoring	IT Security, Data Breach, Event Study, Reputation
71	From information security to cyber security	Von Solms, R., Van Niekerk, J.	2013	Comput. Secur.	Academia	IT	Qualitative	Risk Management (Mitigation, Insurance)	
72	Meeting the cyber risk challenge	Harvard Business Review	2013	Harvard Business School Publishing	Industry		Data collection		Survey
73	Willis fortune 500 cyber disclosure study	Willis	2013		Industry		Data collection		Survey
74	Globally networked risks and how to respond	Helbing, D.	2013	Nature	Academia	IT	Theoretical	Risk Identification	Systemic Risk, Risk Accumulation

75	Cyber risk insurance: a discourse and preparatory guide	Drouin, D.	2013	SANS Institute 2004	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	
76	Cyber resiliency assessment: enabling architectural improvement	Bodeau, D., Graubart, R.	2013	online	Industry	IT	Qualitative	Risk Management (Mitigation, Insurance)	IT Security
77	Cyber-crime, securities markets and systemic risk	Tendulkar, R.	2013	International Organization of Securities Commissions Research Department and World Federation of Exchanges	Industry	Law	Data collection	Risk Identification	Survey
78	Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector	United Nations (UN) Office on Drugs and Crime	2013	online	Industry	Politics	Qualitative	Risk Assessment	Regulation
79	Building resilience in supply chains	World Economic Forum (WEF)	2013	online	Industry	Management	Qualitative	Risk Management (Mitigation, Insurance)	Critical Infrastructure
80	Insurance—cyber risk	Willis	2013	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	
81	Profile of a macro-catastrophe threat type ‘cyber catastrophe’	Ruffle, S., Coburn, A., Ralph, D., Bowman, G.	2013	Cambridge Centre for Risk Studies	Academia	Finance, Insurance, RM	Data collection	Risk Identification	Risk Accumulation

82	The extreme vulnerability of inter-dependent spatially embedded networks	Bashan, A., Berezin, Y., Buldyrev, S. V., Havlin, S.	2013	Nature Physics	Academia	IT	Theoretical	Risk Identification	Networks, Risk Modelling, Inter-dependent Risks
83	The economic impact of cyber terrorism	Hua, J., Bapna, S.	2013	The Journal of Strategic Information Systems	Academia	Economics	Theoretical	Risk Management (Mitigation, Insurance)	Cybercrime, IT Security, Risk Modelling
84	Conflict and negotiation in cyberspace	Lewis, J. A.	2013	Center for Strategic and International Studies (CSIS)	Industry	Politics	Qualitative	Risk Management (Mitigation, Insurance)	Cyberwar
85	Tallinn manual on the international law applicable to cyber warfare	Schmitt, M. N.	2013	Cambridge University Press	Industry	Law	Qualitative	Risk Identification	Regulation, Cyberwar
86	PAS 555 2013 cyber security risk governance and Management	British Standards Institution (BSI)	2013	online	Industry	Politics	Qualitative	Risk Management (Mitigation, Insurance)	IT Security, Self-protection
87	Cyber security self-assessment guidance	Office of the Superintendent of Financial Institutions	2013	online	Industry	Politics	Qualitative	Risk Management (Mitigation, Insurance)	
88	Cyber liability—it's just a click away	Zelle, A. R., Whitehead, S. M.	2014	Journal of Insurance Regulation	Industry	Law	Qualitative	Risk Management (Mitigation, Insurance)	Data breach, Regulation, Contract Design
89	The Betterley Report—cyber/privacy insurance market survey 2014	Betterley	2014		Industry		Data collection		Survey
90	A cloud security risk-management strategy	Choo, K. K. R.	2014	Cloud Computing, IEEE	Academia	IT	Empirical	Risk Management (Mitigation, Insurance)	New Technologies

91	Cyber security—the risk of supply chain vulnerabilities in an enterprise firewall	Kuypers, M. A., Heon, G., Martin, P., Smith, J., Ward, K., Paté-Cornell, E.	2014	Working Paper—Stanford University.	Academia	IT	Empirical	Risk Assessment	Risk Modelling, IT Security
92	Historical development of cyber (re)insurance	Marsh	2014		Industry		Data collection		Survey
93	Net losses—estimating the global cost of cybercrime	McAfee	2014		Industry		Data collection		Survey
94	Cost of data breach study—global analysis	Ponemon Institute	2014		Industry		Data collection		Survey
95	Risky business—lessons for mitigating cyber attacks from the international insurance law on piracy	Shackelford, S., Russell, S. L.	2014	Minnesota Journal of International Law Online (forthcoming)	Academia	Law	Theoretical	Risk Management (Mitigation, Insurance)	Cyber Attacks, Cyber Insurance, Self-protection
96	Working together with clients to find cyber risk solutions	Swiss Re	2014		Industry				
97	Global risks report 2014—ninth edition	World Economic Forum	2014		Industry	Politics			
98	Die Cyber-Versicherung: Unerlässlicher Teil eines effektiven Risikomanagements	Behrends, J.	2014	St. Galler Trendmonitor für Risiko- und Finanzmärkte	Industry	Management	Qualitative		
99	The UK cyber security strategy. Protecting and promoting the UK in a digital world	Cabinet Office	2014		Industry	Law			Regulation
100	Der Cyber-Versicherungsmarkt in Deutschland, Eine Einführung	Choudhry, U.	2014	Springer Gabler Verlag, Wiesbaden	Industry	Management	Qualitative	Risk Management (broad sense)	

101	Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit.	Haas, A., Hofmann, A.	2014	Zeitschrift für die gesamte Versicherungs-wissenschaft	Academia	Management	Qualitative	Risk Identification	New Technologies, Insurability
102	Cyber-Risiken. Marktentwicklung & Risikomanagement	Marsh	2014		Industry				
103	Risk nexus: beyond data breaches: global interconnections of cyber risk	Zurich	2014		Industry			Risk Assessment	Risk Accumulation
104	Cyber resilience—the cyber risk challenge and the role of insurance	CRO Forum	2014	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Risk Taxonomy, Cyber Insurance, Insurability
105	Cyber claims study	NetDiligence	2014	online	Industry	Finance, Insurance, RM	Data collection	Risk Assessment	Data Breach, Underwriting Cyber Risk, Data Collection
106	Framework for improving critical infrastructure cybersecurity	U.S. National Institute of Standards and Technology (NIST)	2014	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Regulation
107	Case study: critical controls that could have prevented Target breach	SANS Institute	2014	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Phishing Attacks
108	Cyber essentials scheme: summary	Department for Business, Innovation & Skills and Cabinet	2014	online	Industry	Law	Qualitative	Risk Management (Mitigation, Insurance)	Regulation
109	Cyber essentials scheme: requirements for basic technical protection from cyber attacks	Department for Business, Innovation & Skills and Cabinet	2014	online	Industry	Law	Qualitative	Risk Management (Mitigation, Insurance)	Regulation, IT Security

110	Assessment methodology for the oversight expectations applicable to critical service providers	Bank for International Settlements and International Organization of Securities Commissions (BIS)	2014	online	Industry	Law	Qualitative	Risk Management (Mitigation, Insurance)	Regulation
111	Principles for effective cybersecurity regulatory guidance	Securities Industry and Financial Markets Association	2014	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	
112	Cyber risks & exposures	Lloyd's	2014	online	Industry	Finance, Insurance, RM	Qualitative	Risk Monitoring	
113	Achieving cyber resilience	AIG	2014	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Operational Cyber Risk, IT security
114	Cyber-risk oversight	National Association of Corporate Directors (NACD)	2014	online	Industry	Management	Qualitative	Risk Management (Mitigation, Insurance)	Operational Cyber Risk, IT security
115	Schadenspiegel: Gefahr aus dem Netz	Munich Re	2014	Magazin für Schadenmanager	Industry	Management	Qualitative		
116	2014 Emerging risk acumen: key findings	AXA	2014	online	Industry	Finance, Insurance, RM	Qualitative	Risk Identification	
117	Cyber risk—a global systemic threat	DTCC	2014	online	Industry	Politics	Qualitative	Risk Identification	Systemic Risk, Interdependent Risks

118	IRM'S cyber risk executive summary	Institute of Risk Management	2014	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	
119	Stress test scenario—Sybil logic bomb cyber catastrophe	Ruffle, S. et. al.; Cambridge Risk Framework series, Centre for Risk Studies	2014	online	Academia	Economics	Qualitative	Risk Identification	Critical Infrastructure, Systemic Risk, Risk Accumulation, Risk Modelling
120	Markets for cybercrime tools and stolen data: hackers' bazaar	Ablon, L., Libicki, M. C., Golay, A. A.	2014	National Security Research Division (RAND)	Academia	Economics	Empirical	Risk Identification	Cybercrime
121	Strategies to mitigate targeted cyber intrusions	Australian signals directorate (ASD)	2014	online	Industry	Politics	Qualitative	Risk Management (Mitigation, Insurance)	IT Security, Self-protection
122	Cyber risk: nightmare or opportunity	RMProfessional	2014	online	Industry	IT	Qualitative	Risk Management (Mitigation, Insurance)	IT Security, Self-protection
123	Monitoring IT operational risks across U.S. capital markets	Friedhoff, J., Mansouri, M.	2015	Journal of Operational Risk	Academia	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Regulation
124	Insurability of cyber risk: an empirical analysis	Biener, C., Eling, M., Wirfs, J. H.	2015	The Geneva Papers	Academia	Finance, Insurance, RM	Empirical	Risk Management (broad sense)	Data collection, Risk Modelling, Cyber Insurance, Risk Accumulation

125	Insurance for cyber risks—a comprehensive analysis of the evolving exposure, today's litigation, and tomorrow's challenges	Podolak, G. D.	2015	Quinnipiac Law Review	Academia	Law	Qualitative	Risk Management (Mitigation, Insurance)	Contract Design, Regulation
126	Cyber risk insights conference	Advisen	2015		Industry				
127	A guide to cyber risk—managing the impact of increasing interconnectivity	Allianz Global Corporate & Specialties (AGCS)	2015		Industry			Risk Management (Mitigation, Insurance)	Risk Accumulation
128	The Betterley report—cyber/privacy insurance market survey 2015	Betterley	2015		Industry		Data collection		Survey
129	Modelling and management of cyber risk	Eling, M., Wirfs, J. H.	2015	Working Paper	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	Risk Modelling, Risk Accumulation
130	Business blackout—the insurance implications of a cyber attack on the US power grid	Lloyd's	2015		Industry				
131	Promoting UK cyber prosperity: public-private cyber-catastrophe re-insurance	Long Finance	2015		Industry				
132	European 2015 cyber risk survey report	Marsh	2015		Industry		Data collection		Survey
133	Share of companies with standalone cyber insurance in the United States from 2013 to 2014, by industry	Statista	2015	online	Industry		Data collection	Risk Identification	

134	The extreme risk of personal data breaches and the erosion of privacy	Wheatley, S., Mail-lart, T., Sornette, D.	2015	Working Paper—Cornell University Library	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	Data breach, Risk Modelling
135	Optimal risk transfer for cyber risk	Wirfs, J. H.	2015	Working Paper	Academia	Finance, Insurance, RM	Empirical	Risk Management (Mitigation, Insurance)	
136	Global risks report 2015—tenth edition	World Economic Forum	2015		Industry	Politics			
137	Cyber Risk: Risikomanagement und Versicherbarkeit	Biener, C., Eling, M., Matt, A., Wirfs, J.H.	2015	I-VW HSG Schriftenreihe	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	
138	Components and challenges of integrated cyber risk management	Kosub, T.	2015	ZVersWiss	Academia	Management	Qualitative	Risk Management (broad sense)	
139	Hype and heavy tails—a closer look at data breaches	Edwards, B., Hofmeyr, S., Forrest, S.	2015	Working Paper	Academia	Finance, Insurance, RM	Empirical	Risk Assessment	Data Breach, Risk Modelling
140	Cyber-risk management	Refsdal, A., Solhaug, B., Stølen, K	2015	Springer International Publishing	Academia	Finance, Insurance, RM	Qualitative	Risk Management (broad sense)	
141	Cybersecurity assessment tool	Federal Financial Institutions Examination Council (FFIEC)	2015	online	Industry	Management	Qualitative	Risk Identification	
142	Insurance banana skins	Centre for the Study of Financial Innovation (CSFI) & PwC	2015	online	Industry	Finance, Insurance, RM	Data collection	Risk Identification	Survey
143	Managing cyber risks in an interconnected world—key findings from the global state of information security® survey 2015	PwC	2015	online	Industry	Finance, Insurance, RM	Data collection	Risk Assessment	Survey

144	2015 data breach investigations report	Verizon	2015	online	Industry	Finance, Insurance, RM	Data collection	Risk Assessment	Survey
145	2015 cost of data breach study—global analysis	Ponemon Institute	2015	online	Industry	Finance, Insurance, RM	Data collection	Risk Assessment	Survey
146	Network and information security directive: co-legislators agree on the first EU-wide legislation on cyber-security	European Commission	2015	online	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation
147	New data protection standards to ensure smooth police cooperation in the EU	European Parliament	2015	online	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation
148	Cyber essentials scheme: assurance framework	Department for Business, Innovation & Skills and Cabinet Office	2015	online	Industry	Law	Qualitative	Risk Management (Mitigation, Insurance)	Regulation
149	Principles for effective cybersecurity: insurance regulatory guidance	National Association of Insurance Commissioners (NAIC)	2015	online	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation
150	Project2020: scenarios for the future of cybercrime	International Cyber Security Protection Alliance (ICSPA)	2015	online	Industry	Trend studies	Qualitative	Risk Identification	
151	Digital security risk management for economic and social prosperity	OECD	2015	online	Industry	Economics	Qualitative	Risk Management (broad sense)	
152	Cyber-security risks in the supply chain	UK National Computer Emergency Response Team	2015	online	Industry	Management	Qualitative	Risk Management (broad sense)	Critical Infrastructure

153	Partnering for cyber resilience—towards the quantification of cyber threats	World Economic Forum (WEF)	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Assessment	Risk Modelling
154	A quick guide to cyber risk	Lloyd's	2015	online	Industry	Management	Qualitative	Risk Management (Mitigation, Insurance)	Cyber Insurance
155	Cyber core data requirements	Lloyd's	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Identification	Risk Taxonomy
156	Market bulletin: cyber-attack: managing catastrophe-risk and exposures	Lloyd's	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Monitoring	
157	The Internet of things is already here, but who bears the risks? A model to explain coverage disputes in a world of interconnected, autonomous devices	Haas, A., Haas, M., Weinert, M.	2015	Working paper	Academia	Finance, Insurance, RM	Theoretical	Risk Management (Mitigation, Insurance)	Externalities, IT Quality, Risk Modelling
158	Drive-bys, spear-phishing and Trojans—the changing face of cyber security	Wüest, C.	2015	Swiss Re Centre of Global Dialogue	Industry	Finance, Insurance, RM	Qualitative	Risk Identification	
159	Has 'big data' become 'too big'?	AXA	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Identification	New Technologies
160	Cyber risk: thread and opportunity	Hartwig, R., Wilkinson, C.	2015	Insurance Information Institute	Industry	Finance, Insurance, RM	Data collection	Risk Identification	Data Breach
161	Cyber war: the next threat to national security and what to do about it?	Clarke, R. A., Knake, R. K.	2015	Strategic Analysis	Industry	Politics	Qualitative	Risk Identification	Cyber War

162	Unique in the shopping mall: on the reidentifiability of credit card metadata	De Montjoye, Y. A., Radaelli, L., Singh, V. K.	2015	Science	Academia	IT	Empirical	Risk Identification	
163	Technology: bitcoin	Lloyd's	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Assessment	New Technologies
164	Risk nexus: overcome by cyber risks? Economic benefits and costs of alternate cyber futures	Zürich	2015	online	Industry	Trend studies	Qualitative	Risk Assessment	
165	Risk nexus: global cyber governance: preparing for new business risks	Zürich	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (broad sense)	New Technologies
166	2015 cyber security and data privacy survey: how prepared are you?	Cusick, D.	2015	White paper	Industry	Finance, Insurance, RM	Empirical	Risk Management (Mitigation, Insurance)	Survey, Cyber Insurance
167	IBM 2015 Cyber Security Intelligence index	IBM	2015	online	Industry	IT	Empirical	Risk Assessment	Cyber Attacks, Data Collection
168	The Internet organised crime threat assessment	EUROPOL	2015	online	Industry	Politics	Qualitative	Risk Management (broad sense)	Cybercrime
169	Cyber risk handbook 2015	Marsh & McLennan	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (broad sense)	
170	Information security and cyber liability risk management	Advisen & Zürich	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Cyber Insurance, Survey

171	OCIE's 2015 cybersecurity examination initiative	Office of Compliance Inspections and Examinations	2015	online	Industry	Politics	Qualitative	Risk Management (Mitigation, Insurance)	
172	The cyber insurance multi-year plan	PwC	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (broad sense)	Cyber Insurance
173	Cross sector—global: cyber risk of growing importance to credit analysis	Moody's	2015	online	Academia	Management	Qualitative	Risk Assessment	Rating
174	Cyber risk and corporate credit	Standard & Poor's	2015	online	Industry	Management	Qualitative	Risk Assessment	Rating
175	Topics risk solutions: reputations under attack	Munich Re	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Reputation, Insurability, Cyber Insurance
176	S&P: US-Versicherer haben Cyber-sparte im Griff	Herbert Frommes Versicherungsmonitor	2015	online	Industry	Finance, Insurance, RM	Qualitative	Risk Assessment	Rating, Underwriting Cyber Risk, Cyber In-
177	VdS Quick-Audit für Cyber-Security: Verfahren	VdS Schadenverhütung GmbH	2015	online	Industry	IT	Qualitative	Risk Management (Mitigation, Insurance)	Operational Cyber Risk, Self-protection,
178	VdS 3473en—cyber security for small and medium enterprises, Requirements	VdS Schadenverhütung GmbH	2015	online	Industry	IT	Qualitative	Risk Management (Mitigation, Insurance)	Operational Cyber Risk, Self-protection, IT Security
179	VdS 5555en—cyber security for small and medium enterprises, Brochure	VdS Schadenverhütung GmbH	2015	online	Industry	IT	Qualitative	Risk Management (Mitigation, Insurance)	Operational Cyber Risk, Self-protection, IT Security

180	Cyber risk: too big to insure? risk transfer options for a mercurial risk class	Eling M., Wirfs, J. H.	2016	Institute of Insurance Economics I.VW-HSG, University of St. Gallen	Academia	Finance, Insurance, RM	Empirical	Risk Management (broad sense)	
181	Issues paper on cyber risk to the insurance sector	IAIS (International Association of Insurance Supervisors)	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Cybercrime, Operational Cyber Risk, Regulation Risk Taxonomy
182	DataLossDB		2016	online	Industry		Data collection	Risk Identification	Data Breach, Data Collection
183	Fact sheet: cybersecurity national action plan	The Withe House	2016	online	Industry	Law	Qualitative	Risk Management (broad sense)	Regulation
184	Cyber insurance exposure data schema V1.0	Cambridge Centre for Risk Studies	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Identification	Risk Taxonomy
185	Cyber exposure data standard and preparer's guide	AIR Worldwide	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Identification	Risk Taxonomy
186	Cyber risks spill over into the physical world	Zürich	2016	online	Industry	Management	Qualitative	Risk Assessment	Risk Accumulation
187	Recommendations for public-private partnership against cybercrime	World Economic Forum (WEF)	2016	online	Industry	Politics	Qualitative	Risk Management (Mitigation, Insurance)	Regulation
188	The benefits and limits of cyber value-at-risk	Deloitte	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Assessment	

189	Ukraine attack highlights cyber-risk to critical infrastructure	Zürich	2016	online	Industry	Management	Qualitative	Risk Identification	Critical Infrastructure
190	Mitigating the inevitable: how organizations manage data breach exposures	Advisen	2016	online	Industry	Management	Qualitative	Risk Management (Mitigation, Insurance)	Operational Cyber Risk, Data breach
191	Companies still unprepared for mounting cyber risks	Zürich	2016	online	Industry	Management	Qualitative	Risk Management (broad sense)	
192	Allianz risk barometer top business risks 2016	Allianz Global Corporate & Specialties (AGCS)	2016	online	Industry	Management	Qualitative	Risk Identification	
193	Data protection and the cloud meeting growing security needs	SCOR	2016	online	Industry	IT	Qualitative	Risk Management (Mitigation, Insurance)	New Technologies
194	Searching for stability in cyber space	Berkshire Hathaway Specialty Insurance	2016	Risk and Insurance	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	
195	UK: businesses don't believe they are at risk of cybercrime	Aviva	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	
196	Environmental cyber risk	XL Group plc	2016	Online; White paper	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Critical Infrastructure
197	Staying ahead of emerging cyber risks	XL Group plc	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	
198	Technology and cyber risk liability	XL Group plc	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	

199	Cyber claim trend: risks go beyond data breaches	XL Group plc	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	
200	2016 Internet security threat report	Symantec Company	2016	online	Industry	IT	Data collection	Risk Identification	Data Breach, Data Collection, Survey
201	Managing cyber insurance accumulation risk	Risk Management Solutions Inc. & Centre for Risk Studies, University of Cambridge	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Critical Infrastructure, Systemic Risk, Risk Accumulation, Risk Modelling
202	Integrated infrastructure: cyber resiliency in society	Kelly, S., Leverett, E., Oughton, E. J., Copic, J., Thacker, S., et al.	2016	online	Academia	Economics	Data collection	Risk Identification	Critical Infrastructure, Systemic Risk, Risk Accumulation, Risk Modelling
203	IRGC workshop on comparing methods for terrorism risk assessment with methods in cyber security	International Risk Governance Council (IRGC)	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (broad sense)	Cyber Terrorism
204	2016 threats predictions	McAfee Labs & Intel	2016	online	Industry	IT	Qualitative	Risk Management (broad sense)	
205	Data breach digest	Verizon	2016	online	Industry	IT	Qualitative	Risk Identification	Data Collection
206	CIS critical security controls	Center for Internet Security (CIS)	2016	online	Industry	Politics	Qualitative	Risk Management (Mitigation, Insurance)	IT Security, Self-protection

207	2016 data breach investigations report	Verizon	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Assessment	Data Collection
208	Global cyber insurance update: expanding threats amplify underwriting Opportunity, Loss Potential	Fitch Ratings	2016	online	Industry	Management	Qualitative	Risk Assessment	Rating
209	CRO Forum concept paper on a proposed categorisation methodology for cyber risk	CRO Forum	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Identification	Risk Taxonomy
210	Pool Re should 'evolve' to cover cyber attacks and pandemics	Financial Times	2016	online	Industry	Finance, Insurance, RM	Qualitative	Risk Management (Mitigation, Insurance)	Insurability, Cyber Insurance, Underwriting Cyber Risk, Cyber Insurance
211	Cyber and beyond: insurance and risk in a digitally interconnected world	IBM	2016	online	Industry	Finance, Insurance, RM	Data collection	Risk Management (broad sense)	Survey, Cyber Insurance, Data Collection

Appendix D. Definitions of cyber risk

Table D1. Definitions of cyber risk

Source	Definition
Mukhopadhyay et al. (2005, 2013)	Risk involved with malicious electronic events that cause disruption of business and monetary loss
Böhme & Kataria (2006)	Breach or failure of information systems
Cebula & Young (2010)	Operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems
Kshetri (2010)	A cybercrime is defined as a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations.
Ögüt et al. (2011)	Information security risk
The UK Cyber Security Strategy (2011)	Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure, and services.
World Economic Forum (2012)	‘Cyber risks’ are defined as the combination of the probability of an event within the realm of networked information systems and the consequences of this event on assets and reputation.
World Economic Forum (2012)	‘Cyber’ refers to the interdependent network of information technology infrastructures and includes technology ‘tools’ such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
Hua & Bapna (2013)	Cyber terrorism: Attacks implemented by cyber terrorists via information systems to (1) significantly interfere with the political, social or economic functioning of a critically important group or organization of a nation, or (2) induce physical violence and/or create panic.
National Association of Insurance Commissioners (2013)	Defines cyber by providing typical examples: Identity theft, business interruption, damage to the firm’s reputation, disclosure of sensitive information and business interruption
National Institute of	Defines cyber space as ‘a global domain within the information environ-

Standards and Technology (NIST, 2014)	ment consisting of the interdependent network of information systems in infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.’
Tallinn Manual (Schmitt, 2013)	Cyberspace: The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks.
Willis (2013a)	Cyber risk can be defined as the risk connected to activity online, Internet trading, electronic systems, and technological networks, as well as storage of personal data
Swiss Re (2014)	Any risk emanating from the use of electronic data and their transmission. This encompasses physical damage caused by cyber-attacks, loss or corruption of data and its financial consequences, fraud committed by misuse of data, as well as any liability arising from a failure to maintain the availability, integrity, and confidentiality of electronically stored information—be it related to individuals, companies, or governments. In this context, cyber risk insurance addresses the first and third party risks associated with e-business, the Internet, networks and informational assets.
CRO Forum (2014)	Any risks that emanate from the use of electronic data and their transmission, including technology tools such as the Internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments.
Institute of Risk Management (2014)	Any risk of financial loss, disruption, or damage to the reputation of an organization from some sort of failure of its information technology systems.
Refsdal, Solhaug, & Stølen (2015)	Definition consisting of three elements: • A cyber-risk is a risk that is caused by a cyber-threat • A cyber-threat is a threat that exploits a cyberspace • Cyberspace is a collection of interconnected computerized networks, including services, computer systems, embedded processors, and controllers, as well as information in storage or transit.
Lloyd’s (2015b)	Losses relating to damage to, or loss of information from, IT systems and networks.
Lloyd’s (2015a)	Definition of Cyber-Attack: exposures arising from a malicious electronic act which for the purpose of this bulletin we label as ‘cyber-attack’. Cyber-attack is therefore the proximate cause of loss, although the consequences may include property damage, bodily injury, financial loss or

	other forms of damage.
CRO Forum (2016)	Cyber risk [is] defined as the risk of doing business in the cyber environment. The definition of cyber risk covers: • Any risks emanating from the use of electronic data and their transmission, including technology tools such as the Internet and telecommunications networks. • physical damage that can be caused by cyber-attacks. • fraud committed by misuse of data. • any liability arising from data use, storage and transfer, and • the availability, integrity and confidentiality of electronic information be it related to individuals, companies or governments.

Appendix E. Data sources

Table E1. Data sources

Source	Description
Panel A: Aggregated Data	
Cyber Attacks Timeline Master Index (Hackmageddon, 2016)	Collection of information about author, target, type and country of publicly reported cyber-attacks (regularly updated).
Cost of Data Breach Study (Ponemon Institute, 2015b)	Survey among 350 companies in 11 countries about the total costs of data breach and the costs per each breached item (sponsored by IBM; updated yearly).
Global Cost of Cybercrime Study (Ponemon Institute, 2015a)	Survey among 252 companies in several countries about the costs caused by cybercrime (sponsored by HP; updated yearly)
Cyber Claims Study (NetDiligence, 2014)	Survey among major cyber risk insurers on claims payed out (117 in total, most of them for data breaches). Additionally they record the number of breached records per incident, the type of cost covered by the policy (e.g. crisis services, legal defense), the type of data exposed (e.g. personal, health and financial information) and the cause for the data breach (e.g. Hacker, Malware).

eRiskHub (by NetDiligence) ¹⁸	NetDiligence is currently setting up a proprietary database where the anonymized data from all cyber claims studies are accessible.
Internet Security Threat Report, Norton Cybercrime Report (Symantec, 2016)	Recorded data are based on attack sensor placed all over the world. Moreover, the company maintains a database on vulnerabilities.
Net Losses—Estimating the Global Cost of Cybercrime (McAfee, 2015)	Estimates the global loss data based on several data sources (e.g. German Office for the Protection of the Constitution, the Netherlands Organization for Applied Scientific Research (TNO), China's Peoples Public Security University, the European Commission, the Australian Institute of Criminology Research, and estimates by government agencies in other countries and consulting and cyber-security companies around the world.)
ICSA survey (by ICSA Lab)	Survey among 300 companies on the infection rate by malicious codes and the associated costs. (used by Herath & Herath, 2011)
Data Breach Investigations Report (Verizon, 2016)	Data on over 100,000 cyber risk incidents (incl. data breaches) for several countries contributed by security service providers, law enforcement, and government agencies.
Panel B: Raw Data	
Biener, Eling & Wirfs (2015a)	Extract cyber losses from a worldwide data set of publicly reported operational losses (SAS OpRisk Global Data ¹⁹) using a predefined search algorithm.
DataLossDB (by Risk Based Security) ²⁰	Information on data breaches from 1995 until present including number of breached items per incident, involved organizations, data type and more (regularly updated, former open security foundation). Is considered as the most comprehensive source of information about data breach (used by Maillart & Sornette; 2010 and Wheatley et al., 2016)
Chronology of Data Breaches (by privacy rights)	Compiles publicly reported data breaches from 2005 until present collected by a U.S. based non-profit organization. It contains information about type of data breach, involved organizations and the

¹⁸ Retrieved May 5, 2016, from <https://eriskhub.com>

¹⁹ Retrieved May 5, 2016, from https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf

²⁰ Retrieved May 5, 2016, from http://datalossdb.org/primary_sources. Since 2015 the data base is provided by Risk Based Security (RBS). Retrieved May 5, 2016, from <https://www.riskbasedsecurity.com>

clearing house) ²¹	number of breached items per incident. 4,486 entries in total. (used by Edwards et al., 2015)
National Vulnerability Database (by NIST, 2016) ²²	Collects software vulnerabilities for the U.S. (used by Maillart & Sornette, 2010)
Honeynet ²³	Honeypot projects (e.g. Leurre.com) conducted by Honeynet, an international non-profit organization. The honeypot (software or server), simulates a potential target, registers the attacks and thereby measures malicious activity in the Internet (used by Böhme & Kataria, 2006).
Internet Storm Center (ISC, by SANS Institute) ²⁴	Collects daily number of attacks per origin and target country (sensors register the criminal activity at different places.)
Cyber Data set (by Advisen) ²⁵	Proprietary database on Cyber risk related events such as data and system breaches and security violations.

²¹ Retrieved May 5, 2016, from <https://www.privacyrights.org/data-breach>.

²² National Institute of Standards and Technology (NIST). Retrieved May 5, 2016, from https://web.nvd.nist.gov/view/vuln/search-results?query=&search_type=all&cves=on, and <http://www.us-cert.gov/cve.html>

²³ Retrieved May 5, 2016, from <https://www.honeynet.org>

²⁴ Retrieved May 5, 2016, from <https://isc.sans.edu>

²⁵ Retrieved May 5, 2016, from <http://www.advisenltd.com/analytics/advisens-cyber-data> set. Currently there is a growing number of specialised consulting firms that offer insurance companies data on cyber risk via web monitoring techniques.

Essay II

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

Martin Eling & Werner Schnell

Abstract

Cyber risk is becoming more significant both in underwriting and operational risk of insurance companies. We first describe the characteristics of cyber risk and then analyze the current regulatory models with respect to cyber risk. We make recommendations for the assessment of cyber risk both in underwriting and operational risk. Our results indicate that regulatory models do not adequately reflect the potential risk exposure. Especially for small portfolios, which are predominant in practice today, diversification does not work, and risk is underestimated. Regulatory models need to take the heavy tails and dependence structure observed in cyber risks into account.

Keywords

Risk management, accumulation risk, cyber insurance, cyber risk, insurability

Status

This paper has been published 2019 in *North American Actuarial Journal* (online) and was presented at *2016 American Risk and Insurance Association (ARIA) Conference*, *2016 German Finance Association (DFA) Conference*, *2017 Insurance Risk and Finance Research Conference (IRFC)*, and *2018 PIF Seminar*, University of St.Gallen.

Acknowledgments

The authors are grateful for feedback and comments from Kwangmin Jung, Christian Kubitz, Pingyi Lou, Joan Schmit, Shaun Shuxun Wang, Steven Weissbart, Jan Wirfs, and the participants of the *2016 ARIA conference*, the *2016 DGF conference*, the *2017 Insurance Research Seminar*, I.VW, University of St.Gallen and the *2017 IRFC* at NTU Singapore.

1 Introduction

As the global economy becomes increasingly dependent on IT systems and digital networks, cyber risk has become a great threat. Global annual losses caused by cybercrime have been estimated as high as US\$445 billion (McAfee, 2014). According to the World Economic Forum (WEF, 2014) there is a 10% probability of a critical information infrastructure breakdown within the next 10 years that might cost about US\$250 billion. In response, insurance companies have started to develop policies to protect against those emerging risks. While the percentage of cyber losses covered by insurance today is still low, the premium spend for cyber risk insurance is expected to grow strongly over the next years.¹

Cyber risk can affect an insurance company in two ways. First, since an insurance company relies critically on its IT infrastructure, it is vulnerable to cyber risk. This exposure is treated by regulatory frameworks as part of the operational risk category (operational cyber risk). Second, writing cyber risk policies seems to be an attractive business opportunity for insurance companies in an often quite saturated market (underwriting cyber risk). These two risk exposures are treated separately in regulatory frameworks, which is why we analyze them separately in this paper.

A sound understanding of cyber risk when developing regulatory frameworks is of utmost importance since insurers rely on IT and networks and increasingly underwrite cyber policies. While new insurance regulations and research have been concentrated on classical underwriting activities and on operational risk in general, cyber risk has not yet been the focus of much regulatory discussions.² A major challenge for the development of adequate regulatory models for cyber risk has been the limited understanding of its

¹ See NAIC (2016b), Betterley (2015), Swiss Re (2015), Advisen (2015), and Marsh (2016). The premium volume for the year 2015 is US\$3.5 billion globally, with US\$3 billion from the US only. The market is expected to grow to US\$18 billion until the year 2025 (see Swiss Re, 2015). KMPG (2017) estimated that cyber risk insurance will become the biggest non-life insurance business line within the next 20 years.

² Only recently regulators in the US and UK recognize the increasing importance of cyber risk. For example, the NAIC has designed the cybersecurity and identity theft coverage supplement which was first filed in 2016 with the 2015 annual statements (see NAIC, 2016b). The UK regulator is developing a qualitative cyber risk assessment in the context of the own risk and solvency assessment (see Prudential Regulation Authority, 2016).

statistical properties due to the lack of data. Recently, however, new research contributes to better understand cyber risk.³ For example, Biener, Eling, and Wirfs (2015) and Eling and Wirfs (2016) analyze the properties of cyber risk and distinguish operational from cyber risk. Since this research shows that cyber risk is different from other types of risk such as operational risk, there might also be a need for regulators to calibrate models differently.

We contribute to this emerging new stream of research by analyzing how regulatory capital regimes treat cyber risk and comparing it with the results of recent empirical studies on cyber risk. In order to compare the empirical properties with the regulatory frameworks, we transform incident data from Biener et al. (2015) and Eling and Wirfs (2016) to company-specific data. The goal of the paper is to analyze whether regulations take cyber risk sufficiently into account and, if not, how it might be done in the future. The three regulatory capital models we consider are the most recent and most often discussed in academic literature: Solvency II (SII), US Risk-Based Capital (RBC) Standards, and Swiss Solvency Test (SST).⁴ Our findings indicate that the characteristics of cyber risk are not reflected appropriately in the regulatory capital models.

The remainder of the paper is organized as follows. In the Section “Cyber Risk: Definition and Properties” we provide an overview on the relevant research done on cyber risk and its characteristics. Subsequently, the Section “Data and Methodology” analyzes our data on cyber risk and develops the model used to evaluate SII, RBC, and SST in the Section “Operational Cyber Risk” and “Underwriting Cyber Risk”. Finally, we conclude by discussing the results and suggesting potential recommendations for improving regulatory models.

³ Probably due to the lack of data, most research about cyber risk does not focus directly on the monetary loss. Instead, proxy variables are used such as number of records breached (Maillart & Sornette, 2010; Edwards, Hofmeyr, & Forrest, 2016), number of attacks (Böhme & Kataria, 2006), or number of system failures (Mukhopadhyay, Chatterjee, Saha, Mahanti, & Sadhukan, 2013).

⁴ See Eling, Schmeiser, and Schmit (2007), Holzmüller (2009) and Braun, Schmeiser, and Schreiber (2015). The intention of the paper is to analyze the regulatory treatment of policies written on cyber insurance (affirmative covers) and operational risk within the insurance firm. On top of these two aspects there is the problem of silent cyber risk covers in existing policies (non-affirmative covers) which are discussed in the conclusion of the paper but are not the main focus of this analysis.

2 Cyber risk: definition and properties

We define cyber risk as “operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems” (Cebula & Young, 2010). When analyzing cyber risk from the perspective of an insurance company, it is necessary to distinguish operational from underwriting cyber risk. While operational cyber risk is the threat to the insurer’s own IT infrastructure, underwriting risk originates from cyber policies. As an insurer’s exposure to cyber risk (operational) might be different from its clients’ exposure (underwriting), the two types of risk might differ, for example depending on the business processes and the IT infrastructure.

Operational cyber risk might be influenced by the insurer’s business model,⁵ IT infrastructure, employees’ education and other cyber risk management policies. IT security measures, such as firewalls and antivirus software, mitigate risk exposure. As operational risk depends on the insurer’s characteristics and its risk management, it is largely a company-specific (idiosyncratic) risk. Therefore, when using cyber risk data (such as the SAS OpRisk database we consider later) to calibrate operational risk models, company specifics need to be taken into account.

In contrast, the underwriting cyber risk consists of a pool of single exposures. Since cyber risk insurance is a new topic, the policy pools on the insurer’s balance sheet are rather small⁶ and as a consequence the diversification potential is limited. In the case of suboptimal diversification, as we discuss below, capital requirements might need to be adjusted. Moreover, the occurrence of asymmetric information (i.e., adverse selection and moral hazard), forces insurance companies to set rather low cover limits and high deductibles (Biener et al., 2015). This has to be taken into account when inferring from cyber risk data. Again the specific characteristics of an insurer’s underwriting portfolio

⁵ For example, health insurers might have a much larger volume of transactions with the customer compared to property & casualty and life insurers.

⁶ For example, Wirfs (2016) considers portfolios of 50 policies and Eling and Wirfs (2016) vary the portfolio size from 50 to 500 based on expert judgement. An additional clue is given by the report on the cybersecurity insurance coverage supplement published by National Association of Insurance Commissioners (NAIC, 2016d; Insurance Information Institute, 2017). This report shows that the median portfolio size for standalone cyber policies is around 50.

need to be accounted for when using cyber risk data for calibrating a loss model.

Insurance losses are frequently modelled by the lognormal distribution especially in regulatory frameworks (e.g., Bundesamt für Privatversicherungen, 2006, for SST; EC, 2010, for SII). However, empirical analyses question lognormality of the loss distribution of cyber risk. It has been found that the lognormal distribution underestimates the probability mass in the tails and thus underestimates risk measures such as value at risk (VaR) or tail value at risk (TVaR). For example, Eling and Wirfs (2016) investigate the statistical properties of cyber risk based on the SAS OpRisk database. Losses from cyber risks show relatively high skewness and kurtosis compared to losses in the property and liability domain. For the tail distribution, Eling and Wirfs (2016) estimate a Pareto index⁷ around 0.63 depending on the region, industry, and time.⁸ This result is confirmed by Maillart and Sornette (2010) as well as Wheatley, Maillart, and Sornette (2016) who estimate a Pareto index of 0.7 and 0.37 to 0.57 respectively.⁹ Thus, the preliminary literature suggests that extremely heavy tailed distributions govern cyber risk.¹⁰

Another important aspect, especially when aggregating a portfolio, is the dependency between cyber risks. The interconnectedness by physical and social networks can be expected to cause cyber risks to be strongly related (see Baer & Parkinson, 2007; Haas & Hofmann, 2014). Moreover, the use of the same technologies and software exacerbates the problem since one bug can be exploited on all systems hosting the same software. The correlation might be especially high in the case of extreme events, such as a breakdown of global communication (Bashan, Berezin, Buldyrev & Havlin, 2013;

⁷ For a formal definition of the Pareto index α see, e.g., Neslehová, Embrechts, and Chavez-Demoulin (2006).

⁸ Wirfs and Eling (2016) also find that cyber risk is slightly less heavy tailed than non-cyber operational risk (Pareto index of 0.61). In fact, Pareto indexes lower than 1 are a reliable finding for operational risks in empirical analyses (see, e.g., Neslehová, Embrechts, & Chavez-Demoulin, 2006). Note that the shape parameter ξ for the generalized Pareto distribution is here always converted to the Pareto index α by $\alpha = 1/\xi$.

⁹ Wheatley et al. (2016) find that the Pareto index decreased from 0.57 in 2007 to 0.37 in 2015 indicating that cyber risk has become more extremely distributed. However, a similar analysis conducted by Eling and Wirfs (2016) is indecisive about this issue.

¹⁰ A distribution is heavy tailed (infinite second and higher moments) if the Pareto index is $\alpha < 2$ and extremely heavy tailed (infinite first and higher moments) if $\alpha < 1$ (see Ibragimov & Prokhorov, 2016).

Böhme & Kataria, 2006). Therefore, an adequate risk model should consider tail correlation between the risks. Moreover, since we aim to derive models that are supposed to predict cyber losses in the future, we must be careful when extrapolating from the past. The fast-changing technological environment might alter the stochastic laws of cyber risk over time. As IT permeates every aspect of life and we become more reliant on it (see, e.g., internet of things), the interconnection and vulnerability could intensify.

From a regulatory point of view, cyber risk characterized by heavy tails and strong, possible nonlinear, dependency can lead to the following challenges. First, regulatory risk measures based on infinite first or second moments are not well defined. For example, if the first moment does not exist then neither the TVaR nor the volatility exist. Second, standard regulatory models implicitly incorporate some risk reduction expected from portfolio diversification. As diversification works less well due to cyber risk characteristics, the standard models might be too optimistic about the risk reduction attained from diversification and underestimate the risk. The cyber risk properties might also reduce insurers' incentive to hold diversified cyber portfolios due to the potential non-diversification trap (Ibragimov & Walden, 2007; Ibragimov, Jaffee, & Walden, 2008). Finally, the regulator must consider the link between operational and underwriting cyber risk. The same attack might simultaneously affect the underwriting portfolio and the insurers' own IT infrastructure, an aspect that is typically neglected in regulatory models.

3 Data and methodology

The data we use to test the regulatory capital models are cyber loss incidents extracted from the SAS OpRisk database (Eling & Wirfs, 2016). The data set contains 1,579 cyber risk losses between 1995 and 2014.¹¹ For detailed description, we refer to Biener et al. (2015) and Eling and Wirfs (2016). The descriptive statistics presented in Table 1 show extreme values (see maximum value) and high dispersion (see standard deviation).

To compare the empirical properties of cyber risk with the regulatory capital frameworks, the SAS OpRisk data with cyber loss incidences needs to be transformed to company-

¹¹ In the Appendix we conduct the same analysis as in the main text for two different data sets. In Appendix C we consider a subset of the SAS OpRisk data used in the main text (used in Biener et al., 2015). Appendix D presents the analyses for a frequently considered data breach data set (e.g., Maillart & Sornette, 2010; Edwards et al., 2016) provided by the Privacy Rights Clearinghouse (PRC, 2016). Both data sets lead to the same qualitative conclusions as those presented in the main text.

specific data. Estimating the loss distribution from an incidence database without the unbundling of frequency and severity would lead to the marginal distribution given that an incidence has happened. This would neglect all periods and companies where there have been no incidences. Risk measures based on such a conditional distribution would be higher than the analogue measure for the unconditional case. The transformation can be done by the widely applied loss distribution approach (LDA, see, e.g., Hess, 2011). In the following, we first analyze cyber risk from an operational risk view. The risk exposure X is modelled as a stochastic sum, where the severities are denoted by Z_i and the frequency by N :

$$X = \sum_{i=1}^N Z_i. \quad (1)$$

Assuming that the severities are iid $Z_i \sim Z \forall i$ and independent of N , the expectation and variance X can be derived by applying the Wald's and Blackwell-Girshick's equations (see, e.g., Wang, 1998):

$$E(X) = E(N) \cdot E(Z), \quad (2)$$

$$Var(X) = Var(N) \cdot E(Z)^2 + E(N) \cdot Var(Z). \quad (3)$$

The estimated expectations and variances according to Equations (2) and (3) are reported in the lower part of Table 1. The expectation for the expected frequency $E(N) = 0.074$ can be estimated by the total number of losses (1,579) divided by the number of companies in our data set (1123) and the number of years recorded (19) (see Hess, 2011).¹² In order to derive the risk measures used by regulators, we need to derive the whole distribution of the risk exposure X that can be expressed as:

$$F_X(x) = \sum_{n=0}^{\infty} P_n F_Z^{n*}(x), \quad (4)$$

where P_n denotes the frequency distribution and F_Z^{n*} is the n times convolution of the severity distribution. We evaluate Equation (4) numerically with the Panjer (1981) re-

¹² This frequency might be too high, because it represents the frequency contingent on a company having a cyber loss event within the observed 19 years. Like in many other empirical studies, we cannot observe the full sample including all companies that never had a cyber loss event. As an alternative approach to overcome this problem we estimate the frequency for the sample of all companies listed in the S&P 500. We found 130 events for those 500 companies over 10 years leading to a frequency value of 2.60%. In Appendix H we show that our findings also hold for this alternative value for the frequency parameter.

cursion and present resulting risk measures in Table 1. Assumptions about both frequency and severity distributions are required to attain the distribution of X . With respect to the frequency, we rely on parametric models frequently used in literature such as the Poisson and negative binomial distribution (Wang, 1998; Moscadelli, 2004).¹³ For the severity, we use both parametric and nonparametric models. We first fit a nonparametric model to the data. Because nonparametric models are flexible, they have the advantage of fitting the sample well. We define the empirical density function as a histogram with bin size h :

$$F_Z(x)' = \frac{1}{nh} \sum_{i=1}^n I\left(\frac{x_i - x}{h} \leq 0.5\right), \quad (5)$$

where I indicates whether an observation is in a certain bin. The disadvantage of this approach is that it is prone to overfitting the sample. Since the extreme tail of the distribution is not regularly populated, the nonparametric estimation approach might suffer from some instability. An instable tail of the estimated distribution is critical because we are particularly interested in analyzing the upper quantiles. To mitigate these deficiencies, we also use parametric models to describe the cyber risk severities. A model frequently used by actuaries and regulators is the lognormal distribution; empirically it was also shown that the lognormal distribution describes data breach data well (Edwards et al., 2016). However, for our data set (which is broader than data breaches only) Table 1 shows excess skewness and kurtosis also for the log-transformed data; tests for normality (Jarque-Bera, Kolmogorov-Smirnov, Anderson-Darling) are rejected at high confidence levels.

¹³ We start with the Poisson and later also consider the negative binomial distribution, which Eling and Wirfs (2016) find to be the best fit for describing the loss frequency of cyber risks.

Table 1. Cyber risk statistics and parameters (sample size n : 1,579)

	Mean	Std	Min	$\text{VaR}_{0.995}$	$\text{TVaR}_{0.99}$	Max	Skew	Kurt
Z	43.9	429.9	0.1	1,247.5	2,558.2	145,891	27.1	877.4
$\ln(Z)$	0.8	2.1	-2.3	7.1	7.4	9.6	0.8 (209.6)	3.4 (221.5)
N	0.07	0.27						
X	3.2	116.4	0	71.4	301.1	14'594.5	99.6	11,803.1

Note: Std: standard deviation, $\text{VaR}_{0.995}$: value at risk at 99.5% confidence level (as applied in SII), $\text{TVaR}_{0.99}$: tail value at risk at 99% confidence level (as applied in SST), Z : Severity, N : Frequency, and X : Loss Distribution Approach (LDA). All numbers, besides n , are reported in million US\$ and the numbers in parentheses show the test statistics for the null hypothesis that the kurtosis and skewness are identical to the respective statistics of the normal distribution. All numbers are reported in million US\$.

This result is illustrated by the QQ plot in Figure 1 where the empirical quantiles are plotted against the fitted lognormal distribution. The upper empirical quantiles are larger than the theoretical analogous and therefore severe losses are more likely to occur than predicted by the lognormal distribution. The lognormal distribution thus underestimates extreme losses and an appropriate model for cyber risk would have to account for heavy tails. We emphasize this result, because the lognormal distribution is widely used in actuarial practice and by regulators.

Here the choice of the tail distribution is especially critical since regulatory model's risk measures such as value at risk (VaR) and tail value at risk (TVaR) concentrate on the tail. Therefore, we consider the cyber severities' tail behavior in more detail. A frequently used distribution for heavy tails is the Pareto distribution. It is, for example, used by the SST for modeling the extreme values. Moreover, the Pareto distribution has useful theoretical properties as it is the limiting tail distribution for many distributions if the threshold is sufficiently high (see Pickands–Balkema–de Haan theorem; Scarrott & MacDonald, 2012). The statistic frequently used for evaluating the adequacy of a Pareto distribution to describe the data is the expected exceedance: the average of all losses above a moving threshold value v .

Figure 1. QQ plot: empirical vs. lognormal

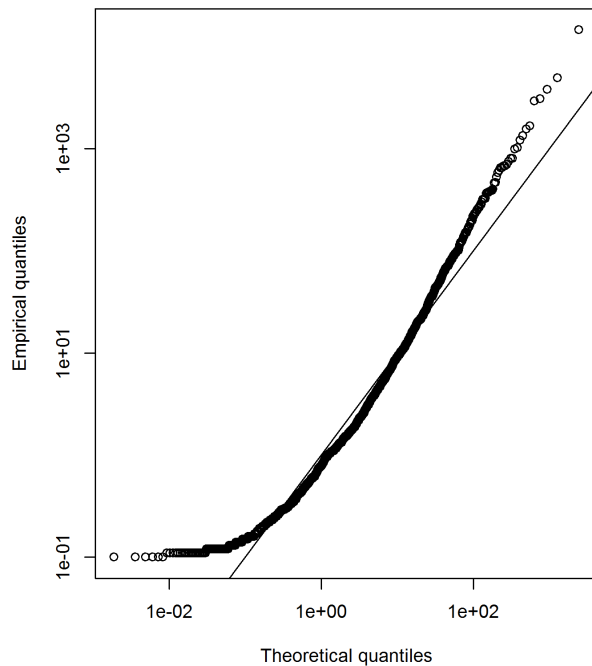
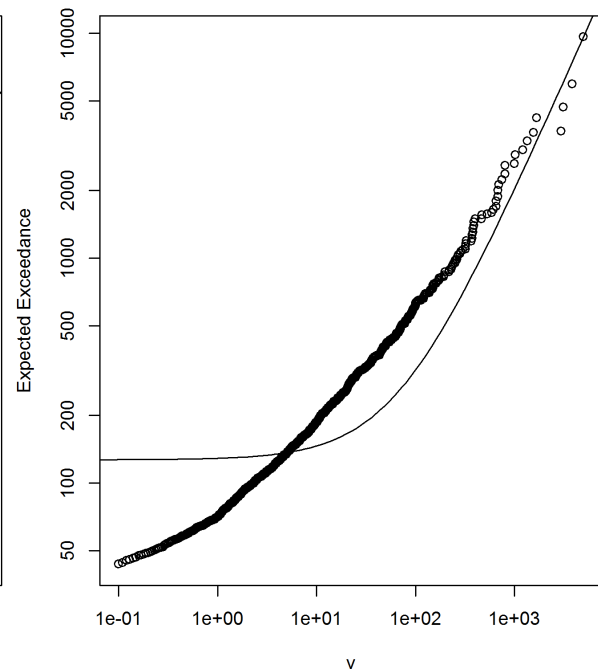


Figure 2. Expected exceedance



Note: The graph on the left plots the lognormal vs. empirical quantile; the solid line shows where the points lie if the lognormal describes the data perfectly. In the graph on the right, the points mark the conditional expectations as a function of the threshold; the solid line is the regression. All numbers are reported in million US\$.

Figure 2 shows that the expected cyber losses are linearly increasing in v . As this is a distinct property of the Pareto distribution, we conclude that it might be a reasonable model for the tails of cyber losses (see, e.g., McNeil, Embrechts & Frey, 2015). Therefore, we consider an extreme mixture model that combines two distributions - a body and a tail. The tail and the body are then spliced together at a threshold that needs to be estimated. Eling and Wirfs (2016) suggest a lognormally distributed body and a Pareto distributed tail. They also show that the optimal threshold is at US\$2 million, corresponding to a 57%-quantile.¹⁴

If we assume that our data is to some extent representative for the insurance industry, X might be interpreted as an estimate for an insurance company's operational risk exposure.

¹⁴ The authors use the bootstrap goodness-of-fit test suggested by Villaseñor-Alva and González-Estrada (2009) to find the optimal threshold. Note that if the threshold is higher, fewer observations are available for the estimation. As a result, the variance of the estimated parameters increases while the Pickands–Balkema–de Haan theorem ensures that the model's bias decreases (see Scarrott & MacDonald, 2012). The situation is reversed if the threshold is set lower. Therefore, choosing the optimal threshold is a tradeoff between the model's bias and variance.

An insurer is then expected to suffer on average a loss due to cyber risk of US\$6.6 million per year at a quite substantial uncertainty as the risk measures in Table 1 show. However, X might also represent the underwriting risk for a single cyber insurance policy in the extreme case where the insurer signs only one contract and there is no cover limit. In practice, however, insurance companies set up portfolios of different cyber risks and state a cover limit in its policies. We thus define the truncated iid risks as $Z_l = \min\{Z, l\}$, where l denotes the cover limit and Equation (1) becomes:

$$X_{l,j} = \sum_{i=1}^N \min\{Z_i, l\}, \quad (6)$$

with $X_{l,j}$ describing the distribution for a single truncated risk. A portfolio consisting of n cyber policies could then be described by:

$$X_{uw} = \sum_{j=1}^n X_{l,j}. \quad (7)$$

Acknowledging that insurers hold portfolios of several risks allows us to account for diversification effects. Our baseline scenario assumes that the individual risks are independent so that there are substantial benefits from diversification. The portfolio's expected frequency would then be:

$$E(N_{uw}) = n \cdot E(N). \quad (8)$$

As an example, Table 2 reports statistics for a cyber risk portfolio with a cover limit of US\$50 million and a size of 50 policies.¹⁵

Table 2. Cyber risk insurance portfolio statistics and parameters

		Mean	Std	VaR _{0.995}	TVaR _{0.99}
Severity (truncated)	Z	8.6	15.0	50.0	50.0
LDA (truncated)	X	0.63	4.7	49.9	44.2
Portfolio (50 policies)	X_{uw}	160.3	822.9	4,030.8	3,990.5
Portfolio (50 policies, truncated)	X_{uw}	31.7	33.2	153.2	159.2

Note: Std: standard deviation, VaR_{0.995}: value at risk, TVaR_{0.99}: tail value at risk. All numbers are reported in million US\$ and the sample size is 1,579.

However, as discussed above, there is likely to be some correlation in the occurrence of

¹⁵ Biener et al. (2015b) show that US\$50 million is a typical deductible used in many cyber insurance policies. Moreover, as discussed above, 50 policies is a typical size for cyber insurance portfolios.

cyber incidents. In the model used here dependency would cause the frequency distribution to be heavier tailed. Since the Poisson distribution has only one parameter, expectation and dispersion cannot be controlled separately. However, a distribution frequently used that provides more degree of freedom is the negative binomial (NB) distribution (see, e.g., Edwards et al., 2016; Eling & Wirfs, 2016). The NB distribution is especially useful since it can be considered as a Poisson model extended by parameter risk.¹⁶ Following Wang (1998), the portfolio frequency N_{uw} is assumed to be governed by a NB distribution with an expectation according to Equation (8) and a variance of:

$$Var(N_{uw}) = \sum_{i=1}^n Var(N_i) + \sum_{\forall i,j \mid i \neq j} Var(N_i) \cdot \rho(N_j, N_i), \quad (9)$$

where N_i is the frequency of each risk in the underwriting portfolio of size n . Assuming equally distributed frequencies $N_i \sim N \forall i$ and identical pairwise correlations $(N_j, N_i) = \rho \forall i, j \mid i \neq j$, Equation (9) simplifies to:

$$Var(N_{uw}) = n \cdot Var(N)(1 + \rho(n - 1)). \quad (10)$$

This equation incorporates pairwise correlations between each risk's frequencies by adjusting the variance of the overall portfolio frequency. Note that considering only the correlation is a simplification since the dependencies might be also nonlinear. Moreover, we assume only that the portfolio frequency is NB distributed and not each risk's frequency. By calibrating the NB distribution with the parameter from Equation (8) and (10), we derive numerically the portfolio's distribution for different pairwise ρ .

To account for potential nonlinear dependencies, we extend our analysis by combining the marginal distributions above with a Clayton copula. This yields a multivariate distribution for the whole portfolio that captures tail dependencies. The Clayton copula is then calibrated with a dependency parameter that corresponds to a correlation $\rho = 0.2$. We motivate this choice by the upper limit of the range reported in Böhme and Kataria (2006). Finally, to derive the portfolio distribution, the portfolio's components are aggregated according to Equation (7). However, in contrast to the approach above, we do not rely on a numerical procedure (Panjer recursion) but use simulations instead.

¹⁶ Parameter risk describes the deviation of our estimated parameters from their true unknown values. The estimated parameter is drawn from a sampling distribution. Combining a Poisson distribution with a $gamma(\alpha, \beta)$ sampling distribution would yield the NB distribution (Wang, 1998).

Finally, evaluating the cumulative distribution function F of the aggregated cyber risk at the capital required by the regulator rc yields the survival probability p_s :

$$p_s = f(F_n^l(rc)), \text{ where } rc = m(n, v, s). \quad (11)$$

F_n^l depends on the portfolio size n and the cover limit l . The functions f and m in turn depend on the regulatory models analyzed. f describes the regulatory risk measure and m the model itself, that is how insurers calculate the required capital. In the case of SII and RBC we are concerned about the VaR and we would have $p_s = F_n^l(rc)$ and for SST we refer to the definition the tail value at risk. The regulatory model $m(\cdot)$ in turn can describe a factor-based approach as it is the case for SII and RBC or, as for SST, it specifies distributions and their parameters. It also depends on n and additionally on some volume measure v and factors s . How m exactly looks like for each framework is described below in more detail.

As Equation (11) shows we evaluate the cyber risk portfolio based on the survival probability. This contrasts to the frequently used approaches that model decision maker's behavior by utility theory (see, e.g., De Giorgi, 2005). However, our analysis is not supposed to fully describe optimal portfolio decisions. Instead we focus on the risk management perspective that might describe the viewpoint of a company's risk management department or the regulator. Moreover, the survival probability resulting from evaluating F_n^l is a nonlinear but, importantly, a positive monotonic mapping into the interval $[0,1]$. While our results are not one to one comparable with Ibragimov et al. (2007, 2008, 2009, 2016), we still can draw qualitatively similar conclusions about the non-diversification trap. It would also go beyond the scope of this paper to model every aspect of the three regulatory models. Thus, we work with simplified versions and in our description focus on the most important aspects. Relaxing these simplifications would massively increase the complexity but would yield qualitatively the same conclusions. We also note that SII and the SST allow for company specific internal models, but we restrict ourselves here to the standard equation, which is the option of choice for the majority of insurers.

4 Operational cyber risk

4.1. Solvency II

Operational cyber risk is not treated as a distinct risk category in SII but instead needs to be considered as a part of the more generic operational risk category. SII defines operational risk as: “[...] risk of loss arising from inadequate or failed internal processes, or from personnel and systems, or from external events. Operational risk should include legal risks, and exclude risks arising from strategic decisions, as well as reputation risks” (EC, 2010). This definition comprises a substantial part of possible cyber risks, but it excludes reputational risk.¹⁷ SII requires that operational risk is assessed qualitatively (by specifying processes to identify, analyze and report operational risks; Pillars II and III of SII) as well as quantitatively (Pillar I of SII). Concerning the quantitative assessment, the capital requirement for operational risk scr_{op} is defined as (EIOPA, 2014):

$$scr_{op} = \min\{0.3 \cdot bscr, bc\}, \quad (12)$$

where $bscr$ stands for the basic solvency capital requirement and bc for the base charge. The first part of the minimum function resembles a factor approach applied on a volume measure $bscr$. $bscr$ is the aggregated capital for different risk categories such as market, underwriting and credit risk. SII defines the total solvency capital scr as the sum of scr_{op} and $bscr$ or equivalently:

$$bscr = scr - scr_{op}. \quad (13)$$

Since no information is available about each insurer’s scr , we approximate it by combining the data we have on equity capital and an average SII ratio sr taken from EIOPA (2017):

$$scr \approx \frac{\text{equity}}{sr}. \quad (14)$$

The most recent SII ratio (Q3 2016) is reported to be 2.11, where 50% of observations fall into a range between 1.5 and 2.97 (EIOPA, 2017). Thus, we consider a solvency ratio of 2.11 as the baseline scenario. The second part of Equation (12) follows a similar factor approach and is defined as:¹⁸

¹⁷ EIOPA (2014) justifies neglecting reputational risk by the lack of historical data on that risk category.

¹⁸ Here we derive the risk factor for the premiums as $s_p = v_p(a_p \cdot s_p^l + (1 - a_p)s_p^{nl})$, where s_p^l is the

$$bc = \max(s_p \cdot v_p, s_r \cdot v_r), \quad (15)$$

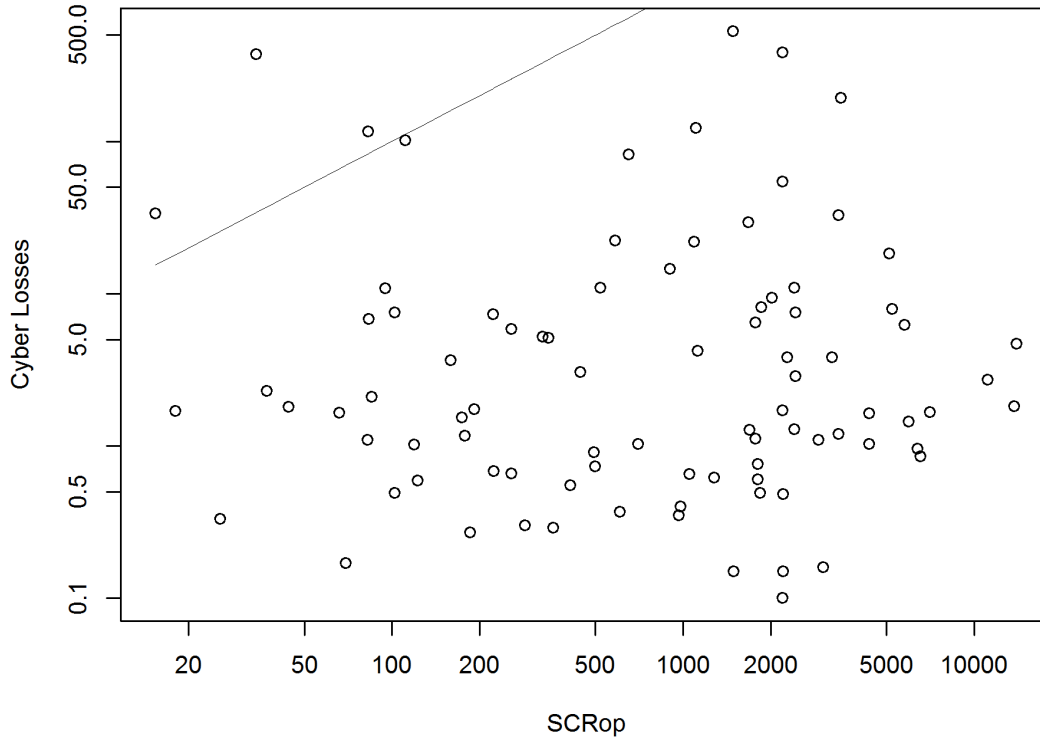
where the volume measures v_p and v_r stand for amount of premiums and reserves respectively. Since our data set does not provided information on this two numbers, we approximate them with the information available that is:

$$v_p \approx \text{Revenue}, v_r \approx \text{Assets} - \text{Equity}. \quad (16)$$

We thus assume that the revenues only contain premiums (i.e. no fee business) and that the reserves are approximated by the difference between assets and equity (e.g. no additional loans on the insurer's balance sheet). When Equation (13)-(16) are insert into (12) this yields an equation where scr_{op} appears simultaneously on the left and on the right side in the first part of the maximum function. We solve it by applying a numerical algorithm (since the function is strictly monotonic a unique solution must exist) and find estimates of scr_{op} for each insurer in our data set. Our data set records 88 complete cyber losses from insurance companies. Figure 3 shows the scatter plot of the realized cyber losses z versus scr_{op} for these 88 cases.

given factor for life premium risk and s_p^{nl} the risk factor for non-life premiums. When assuming that the premiums in our dataset stem equally from life and non-life business, i.e. $a_p = 0.5$ (see Statista, 2017c), we can derive $s_p = 0.035$. In a similar way we find that the reserve risk factor is $s_r = 0.017$.

Figure 3. Operational cyber risk



Note: The solid line shows the situation for $z = scr_{op}$. Numbers are reported in million US\$.

The points above the 45 degrees line show cyber incidents where the losses exceed the estimated scr_{op} . Counting these points and dividing it by the total number of observations would yield the frequency of defaults due to cyber losses, which is 3.41% (3 out of 88). Since this is the frequency given a cyber loss occurred, it is not suited for evaluating the regulatory model. Instead we must calculate the unconditional probability that the random loss Z exceeds the capital that is given by Bayes' theorem as:

$$P(Z > scr_{op}) = P(Z > scr_{op} | Z > 0) \cdot P(Z > 0). \quad (17)$$

As above the frequency of cyber losses per company and year is set to 0.074. Thus, we calculate a default probability due to cyber operational risk of $0.0341 \cdot 0.074 = 0.25\%$. This lower than the 0.5% the regulator aims for. Since the sample of 88 insurers is relatively small, we also conduct the same analysis for the extended sample containing all financial institutions. In this extended sample cyber risk losses exceed operational risk capital with a frequency of 6.8% (78 out of 1,143 cases) so that the unconditional default probability is 0.5%. This value is significantly above the value for the smaller insurance sample. This result suggests that a significant part of the operational risk capital is needed to cover cyber risks. However, scr_{op} is supposed to cover all kinds of operational

risks (not only cyber risks¹⁹) and different types of risk might even accumulate. Moreover, SII neglects the potential connection between operational and underwriting cyber risk. We conclude that the current regime for operational capital under SII might be insufficient in face of the emerging cyber risk exposure.

4.2. US risk-based capital standards

In contrast to SII, operational risk in the US is addressed with a qualitative approach only; the RBC model does not include charges for operational risk. However, the National Association of Insurance Commissioners (NAIC, 2016a) is planning to append an additional term for operational risks to the existing RBC equation. Moreover, insurance companies are required to report cyber risks in an own risk assessment report (ORSA). In this report insurers are required to assess their own operational risks that are substantial enough to interfere with its ability to meet policyholders' obligations. The NAIC is also drafting a law that requires licensed insurers to comply with some minimum data security standards (NAIC, 2016b). It sets requirements for investigating data breaches and notifying the consumers and supervisor.

4.3. Swiss solvency test

Similar to the RBC, the SST does not consider operational risk quantitatively, but qualitatively in the Swiss quality assessment (insurance supervisory ordinance AVO, art. 96-98). The ordinance requires insurers to self-assess and report their operational risk exposures to the supervisor and to collect data on losses suffered from operational risks incidents. Based on this report, supervision can be intensified if some operational risks reported could threaten the insurer's solvability.

5 Underwriting cyber risk

How do regulatory capital models treat cyber risk that originates from the policies an insurance company has written? While SII and the US RBC standards build on a volume and factor approach, the SST employs a stochastic model. Each model allows for com-

¹⁹ For example, in the SAS OpRisk dataset we use here, 1,579 cyber losses are documented, but also 24,962 other operational loss events, for which scr_{op} would also be needed.

pany-specific adjustments. We assume that the insurer retains all liabilities since a reinsurance market for cyber insurance contracts either does not exist or is just emerging (see Biener et al., 2015).²⁰

5.1. Solvency II

The SII standard equation describes the total capital as a composition of capital requirements for several risk categories i . Let $\mathbf{scr}$ be a vector of the capital requirement for each risk category $\mathbf{scr}_i$. Then the aggregated capital is defined by the square root equation (EC, 2014, article 114):

$$\mathbf{scr} = \sqrt{\mathbf{scr}^T \mathbf{P} \mathbf{scr}}, \quad (18)$$

where $\mathbf{P}$ is the correlation matrix between different risk categories. As Equation (18) shows SII only accounts for linear dependencies between different risk categories. In the case of cyber risks, where we might expect nonlinear dependencies, this might lead to too optimistic expectation about the merits of diversification. Drilling Equation (18) further down, $\mathbf{scr}_i$ is defined as (see EC, 2014, article 115):²¹

$$\mathbf{scr}_i = 3 \cdot s_i \cdot v_i, \quad (19)$$

where s_i is the coefficient of variation (volatility divided by the expectation) and v_i is a volume measure based on written premiums or reserves. Applying this approach to cyber risk can be problematic since it does not account for the exact distribution observed. Moreover, the coefficient of variation (and thus volatility) is not a useful risk measure when the distribution is asymmetric; for extreme heavy tails it is not even defined.

Since we do not have information for each risk category, we first aggregate the volume measures and coefficients of variation separately. For this purpose, the volume measures of each risk category are defined as a fraction of the aggregate volume measure v :

²⁰ The regulatory capital models allow for discounts when risks are ceded to a reinsurance company. However, the discounts on capital requirements are partially compensated by the counterparty risk of the reinsurance company. Future research thus has to analyze the potential benefits of reinsurance for managing cyber risks.

²¹ Until the quantitative impact study QIS5 the required capital was defined as $\mathbf{scr} = \text{VaR}_{0.995}(Z) - v$. It assumes a lognormal distribution (EC, 2010) and the capital requirement can be interpreted as the unexpected risk exceeding the expected loss. Equation (19) does not make an explicit distribution assumption but approximates the old one.

$$v_i = \mathbf{w} \cdot \mathbf{v}, \quad (20)$$

where the weights sum up to $\mathbf{1}^T \cdot \mathbf{w} = 1$. According to the proof in Appendix E aggregating scr_i and s_i with the square root equation is equivalent. This means that instead of calculating scr for each risk category first and then aggregating them, we can aggregate weighted s_i first and then apply it on the aggregated volume measure. Appendix E shows that combining Equations (18), (19), and (20) yields:

$$scr = 3 \cdot s \cdot v, \quad (21)$$

where s is the aggregated coefficient of variation. In our empirical analysis, we relate the volume measure to the expected loss. Let X be the random variable describing the losses of the cyber portfolio. We assume that the volume measure equals the expected loss $E(X)$ divided by the loss ratio:²²

$$v \approx b^{-1} \cdot E(X). \quad (22)$$

We choose $b = 0.6$ for the baseline scenario motivated by the average loss ratio for US property & casualty insurers for the years 2009-2015 (Statista, 2017b).²³ Applying (22) to (21) yields:

$$scr = 3 \cdot s \cdot b^{-1} \cdot E(X), \quad (23)$$

s is derived bottom up in three stages as illustrated in Appendix E and for each step the result from Appendix E is applied. First, coefficients of variation for premium s_p and reserve s_r risk as specified by EC (2014, annex II) are aggregated to the coefficient s_{pr}^{sg} per each segment. The correlation between premium and reserve risk is 0.5 (EC, 2014, article 117). We additionally assume that half of the expected losses are coming from reserve risk $w_r = 0.5$ and the other half is coming from premium risk.²⁴

Second, the coefficients s_{pr}^{sg} over all segments sg are again aggregated to attain s_{pr} . However, as the tables do not contain factors specific for cyber risk, the obligations must be allocated according to their true nature of risk, even if unbundling into several LoBs

²² We thus focus on written premiums and neglect the reserves. The premiums are calculated as $b^{-1} \cdot E(X)$.

²³ In Appendix G we show results for different choices of b ; as the loss ratio increases the survival probability decreases.

²⁴ With this we implicitly assume a constant premium volume and linear claims settlement.

is required (EC, 2014, article 55). Relevant segments for cyber risk are “general liability”, “legal expenses” and “miscellaneous financial losses” (see EC, 2014, annex I) and their correlation is 0.5 (see EC, 2014, annex IV). Additionally, we assume that the exposure is equally distributed between the different segments $w_i = w_j \forall i, j$.

Table 3. Aggregation of risk factors

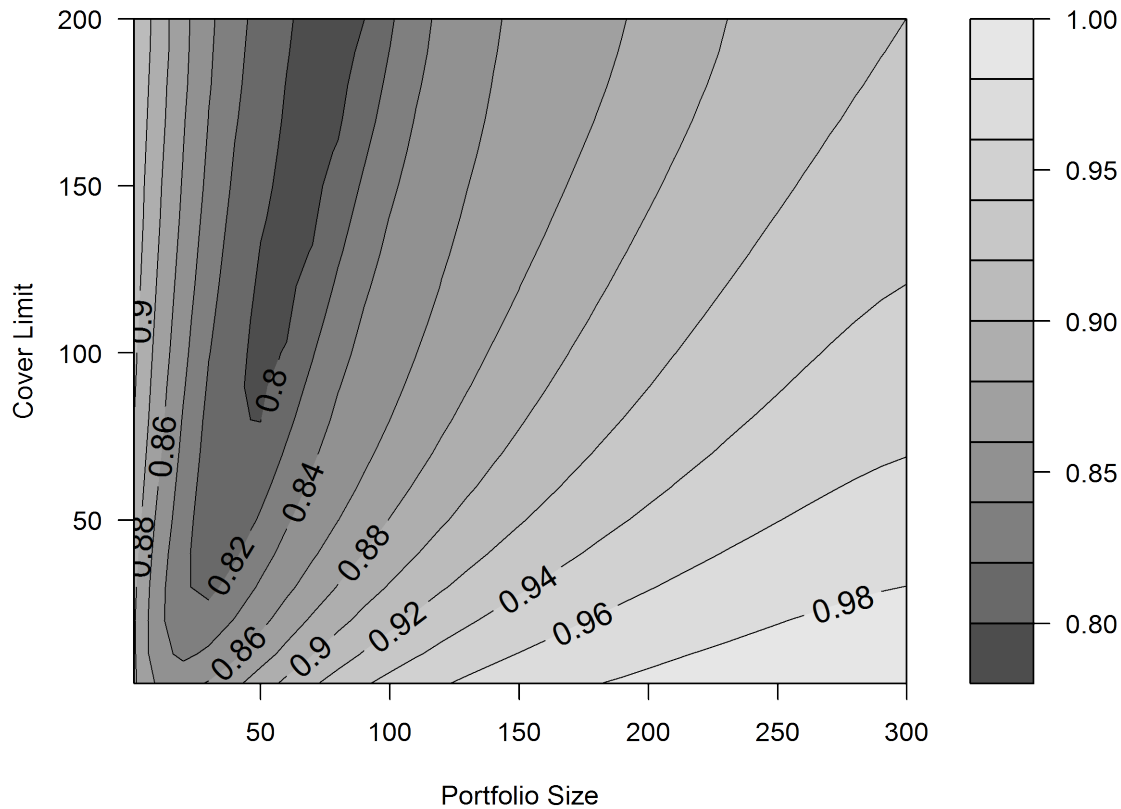
LoBs	w	s_p	s_r	s_{pr}^{sg}
General liability	1/3	0.14	0.11	0.11
Legal expenses	1/3	0.07	0.12	0.08
Miscellaneous financial losses	1/3	0.13	0.20	0.14
s_{pr}	1			0.09
s_{cat}	0.5			0.18
s				0.14

Third, s_{pr} is complemented with catastrophic risk s_{cat} and aggregated to the overall variation coefficient s . The correlation between catastrophic and normal risk is set to $p = 0.25$ (EC, 2014, article 114). Catastrophic risk s_{cat} in turn is composed of several sources of catastrophic risks that are aggregated according to Equation (18). Again there is no specific category for cyber risk. However, from the categories SII specifies, we find “liability risk” and “other cat risk” suitable for our analysis. The risk factor for this two categories is set by SII to 1 and 0.4 (EC, 2014, annex XI and XII). Table 3 shows the aggregation of all risk factors using the specified numerical values. Note that for the final determination of s the s_{pr} (s_{cat}) is weighted with 1 (0.5), because the volume measure for s_{pr} is the sum of premiums and reserves, while the volume measure for s_{cat} are the premiums only; premiums, but not reserves, are thus exposed to catastrophic losses. According to Equation (23) the derived aggregated risk factor s can now be used to calculate the s_{cr} for different portfolio sizes and cover limits. This s_{cr} is then compared with the cumulative distribution functions derived from the empirical data in order to calculate the probability that the estimated loss (for a given cover limit and portfolio size) is smaller than the sum of premiums and s_{cr} according to SII (see Equation 11).²⁵

²⁵ To clarify the actual calculations, we again consider the example of a cover limit of 50 and a portfolio

Figure 4 shows the resulting survival probability for different cover limits and portfolio sizes.

Figure 4. SII survival probability contours



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the sum of premiums and capital required by the regulator.

SII aims at reaching a survival probability of 99.5% (EC, 2010). Figure 4 shows that the survival probability falls short of that goal, especially for small portfolios (as is the case in practice today) and high cover limits. One explanation might be that the factor approach presented in Equation (19) was meant to approximate the 99.5% quantile of the lognormal distribution (EC, 2010). In the worst case, the default probability for a pure cyber risk insurer would be as high as 20%. It is important to emphasize that this is the *ceteris paribus* effect of a pure cyber insurance portfolio, which means that in practice

size of 50 (see Table 2). Then $E(X) = 31.7$ and $b = 0.6$ and thus $v = 31.7/0.6 = 52.8$ and $scr = 52.8 \cdot 0.14 \cdot 3 = 22.2$. Evaluating the distribution function in Equation (11) at $rc = (52.8 + 22.2) = 75$ would yield a probability of about 83% that X is smaller than 75.

the insolvency risk of insurers active in many lines of business will be substantially lower. To analyze the results for different model assumptions, we restrict ourselves to the two-dimensional situation. By slicing the contour plot at a cover limit of US\$50 million we keep the cover limit fixed and analyze the effect the portfolio size has on the survival probability (see Figure 5).²⁶

In the top left figure, the confidence interval obtained by means of bootstrapping (sampling from the data set) indicates that the findings are quite stable and might be applicable for an out of sample application.²⁷ The figure on the top right reports the survival probability for the different severity model (PoT and lognormal). The different severity models yield very similar results and thus our results are robust with respect to the model choice.²⁸ In the bottom part of Figure 5 we show results for different dependence structures (in the upper part we assume iid). The figure bottom left shows the survival probability p_s attained for different correlations ρ . When we deviate from the iid assumption the survival probability is substantially lower and even for large portfolios does not converge to SII's goal of 99.5%.²⁹ The result for the Clayton copula (bottom right figure) is close to the case $\rho=1$ (in the bottom left); this intuitively makes sense, because for the critical tail events that cause ruin the correlation is more like 1 as compared to the overall 0.2 which we use as input parameter for the Clayton copula.

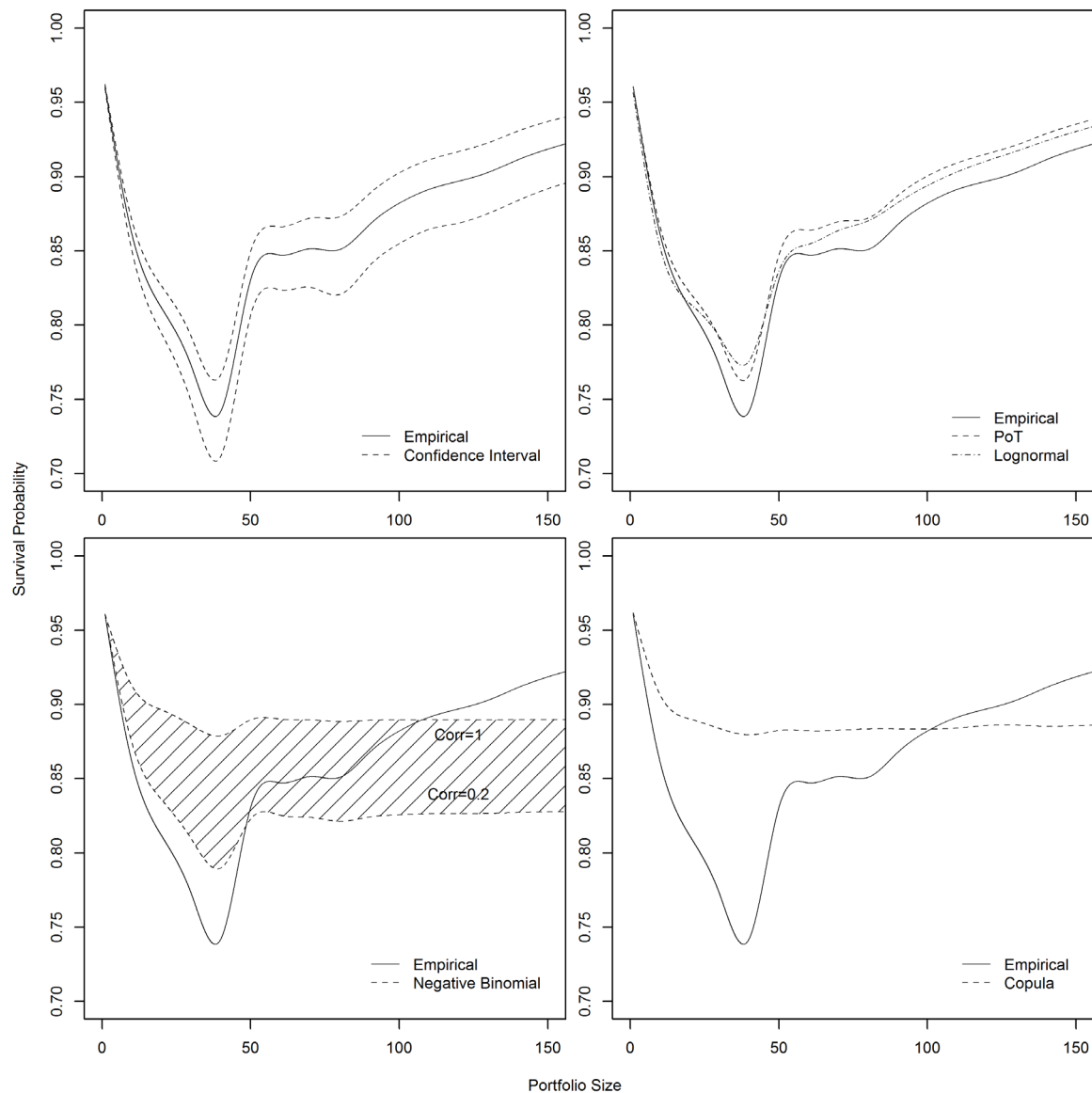
²⁶ In Appendix A we also show the results for a different cover limit of US\$200 instead of US\$50 million.

²⁷ We bootstrap 200 samples from the original data set with replacement and show the 95% confidence interval.

²⁸ Without a cover limit the PoT would lead to a lower survival probability than the lognormal, because of the tail events. With a cover limit the effect of the Pareto distribution in the tail is however reduced so that the two lines more or less correspond to each other.

²⁹ Note that the binomial distribution with a $\rho = 0$ results in the Poisson and binomial survival probability being congruent. Somehow counterintuitive is the observation that the line for a correlation $\rho = 1$ is located above the one for $\rho = 0.1$. However, this difference can be explained by the way the modelling of correlations in the negative binomial distribution changes the density functions. A negative binomial distribution with $\rho = 1$ is heavier tailed than for $\rho = 0.1$. SII evaluated the distribution at a relative low confidence interval so that $p_s(\rho = 1) > p_s(\rho = 0.1)$.

Figure 5. SII survival probability



Note: The top left plot shows the survival probability for combining the Poisson frequency and the empirical severity distribution (with a bootstrapped confidence interval). The top right shows the survival probability when combining the Poisson with parametric severity models. The bottom left figure shows a correlated frequency (negative binomial) paired with the empirical severity distribution. The bottom right shows the result for nonlinear correlations (Clayton copula with dependency parameter corresponding to a correlation of 0.2).

In general, the safety level features an abrupt decrease for small portfolio sizes before it increases again for larger portfolios. We attribute this peculiarity to the heavy tails in the data. It is a similar phenomenon to the non-diversification trap analyzed by Ibragimov et al. (2008). They show that combining heavy tails with limited liability can cause the

portfolio value to decrease with increasing portfolio size before it increases again.³⁰

5.2. US risk-based capital standards

In the US, an insurer that underwrites cyber policies has to hold capital for that business according to the RBC standards defined by the NAIC. The representation of the model here follows Sharara, Hardy, and Saunders (2010). Similar to SII, the calculation of the RBC follows a factor-based approach. While the model in principle also accounts for catastrophic risk, at the moment only the categories earthquake and hurricanes are considered (Seeley, 2012 and NAIC, 2016c). Thus, the model does not account for man-made catastrophic risk that would be of high relevance for cyber risk. The simplified minimum underwriting capital requirement is defined as (NAIC, 2009):

$$rbc = \sqrt{rbc_p^2 + rbc_r^2}, \quad (24)$$

The aggregation of capital for premium risk rbc_p and reserve risk rbc_r is done assuming a correlation of zero. Similar to SII, the capital requirements are derived as some volume measure v multiplied by a risk factor s . The risk factor RBC uses is a stressed loss and expense ratio. The volume measure is composed of premium and reserves. We again use Equation (22) and the same loss ratio. In the following, diversification and adjustment for investment income are neglected. For the premium risk, the required capital is then calculated as:

$$rbc_p = v_p \cdot \max\{(s_p + s_e - 1), 0\} \text{ and } s_p = 0.5 \cdot (c + 1) \cdot s_p^{NAIC}, \quad (25)$$

where v_p is the insurer's current year's net written premium, s_e is the expense ratio, and s_p is the loss ratio risk factor. The second part of the equation enables the insurer to adjust for company-specific exposure by choosing c accordingly. However, since we are

³⁰ We refer to Appendix B for a more detailed comparison with Ibragimov et al. (2008). We extend the finding of Ibragimov et al. (2008), who provide evidence for the non-diversification trap arising under extremely heavy tailed distributions, in two ways. First it is applicable to cyber risk as it indeed is characterized by very heavy tails. Second, we extend the non-diversification trap to the specific perspective taken by the risk management department or regulator. Since these actors only care about the survival or default probability, we show that it might be optimal for them to stick with a small undiversified portfolio since the transition to the optimally diversified portfolio is too risky.

interested in analyzing the overall adequacy of the model for cyber risk, we set the company-specific variables to industry averages. Therefore, let c be equal to 1 and the expense ratio for the US is chosen to be $s_e = 0.275$ (Statista, 2017a). The loss ratio factor s_p^{NAIC} is specified by NAIC. While there is no specific risk factor for cyber policies, the one for “other liabilities” seems to be suitable and the most recent value has been set to 1.027 (NAIC, 2017). The capital for reserve risk is defined as:

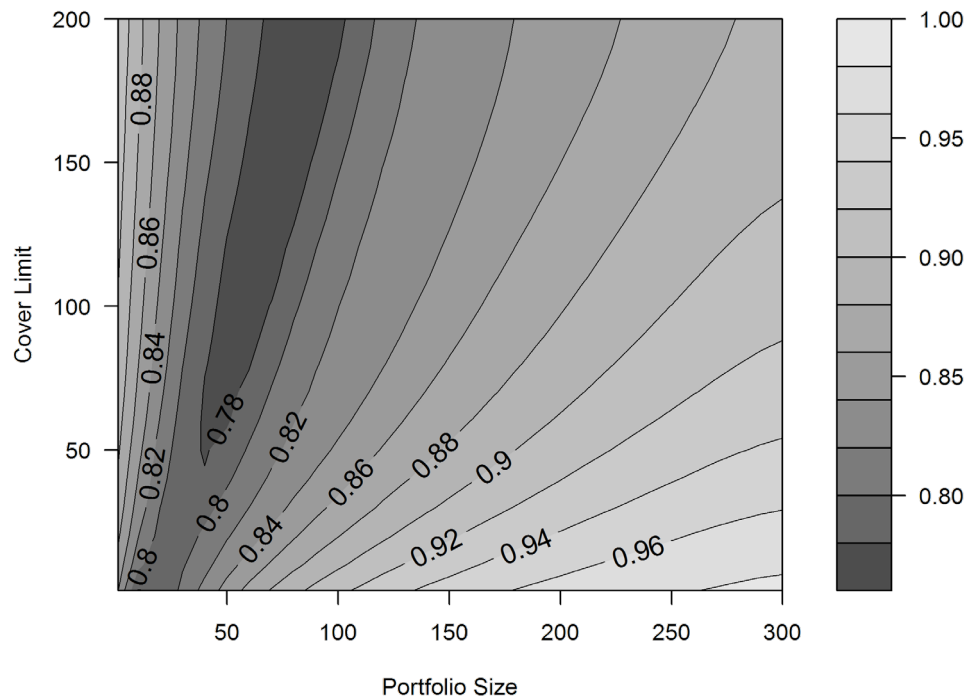
$$rbc_r = v_r \cdot s_r \text{ and } s_r = 0.5 \cdot (d + 1) \cdot s_r^{NAIC}, \quad (26)$$

where v_r corresponds to the reserves and s_r the combined ratio risk factor. Again the company-specific factor d is set to 1 and NAIC’s most recent number for s_r^{NAIC} is 0.531 (NAIC, 2017). Then, rbc_r and rbc_p are aggregated according to Equation (24) and by applying the derivation in Appendix E. Again, we assume equally distributions between premium and reserve risk $w_p = w_r = 0.5$. Thus, the overall risk factor for underwriting cyber risk is

$$\sqrt{(0.5 \cdot (1.027 + 0.275 - 1))^2 + (0.5 \cdot 0.531)^2} = 0.31.$$

Finally, the RBC is calculated for different combinations of portfolio sizes and cover limits and used as quantiles to evaluate the security levels reached based on the available data. While the RBC model does not explicitly aim for any particular safety level, it has been shown that the safety level achieved corresponds to an 87.5%-VaR level (American Academy of Actuaries, 2007). Figure 6 shows the set of portfolio sizes and cover limits with an isotonic survival probability.

Figure 6. RBC survival probability contours

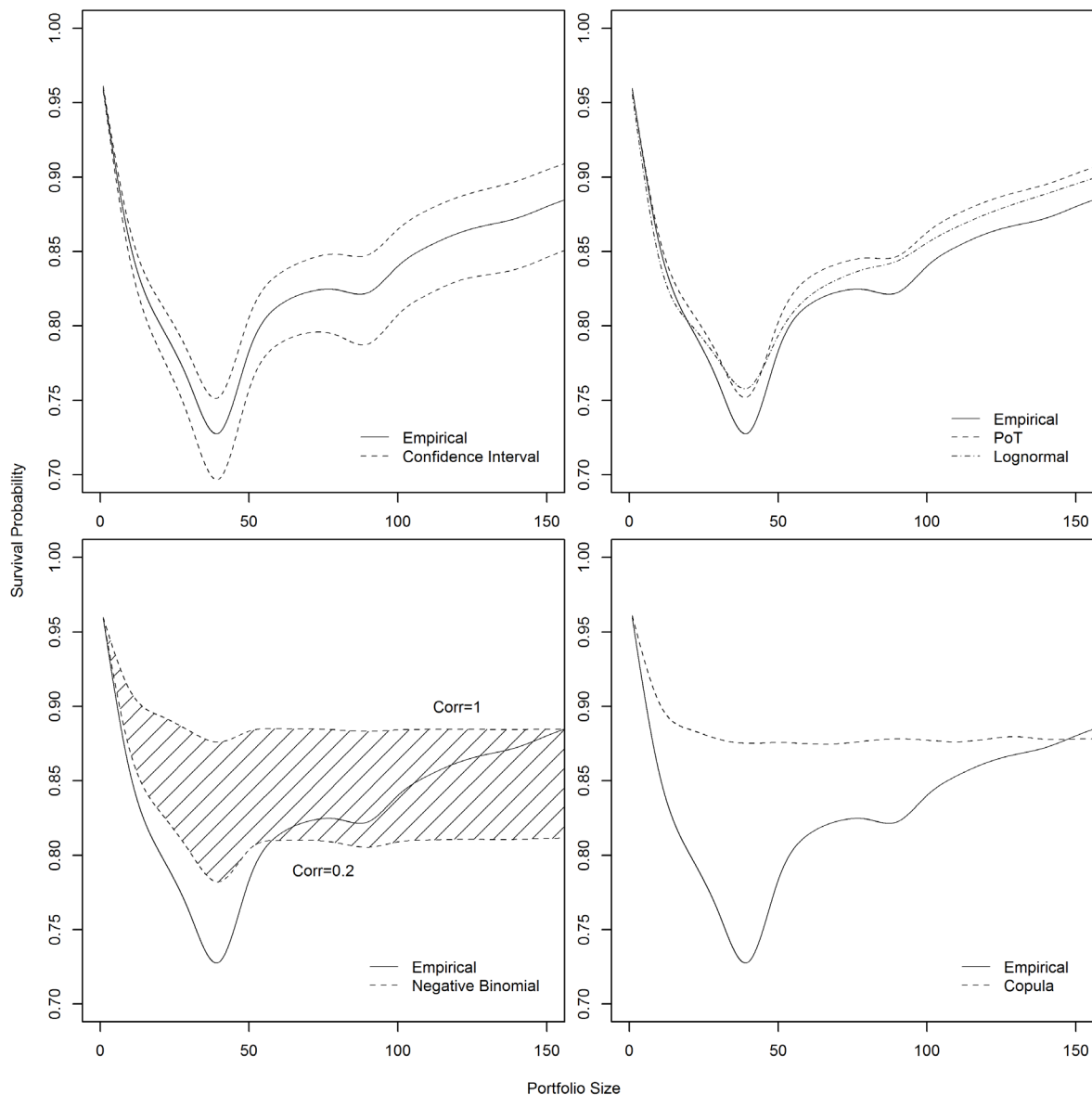


Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Similar to SII, RBC reaches safety levels of 99% only for very large portfolios. However, RBC generally performs even worse than SII as it takes even more risk to reach a certain survival probability. In the worst case, the default probability is as high as 22%. This finding is again related to the non-diversification trap described above.

To analyze the results for different model assumptions, we again slice the contour plot at a cover limit of US\$50 million and analyze the survival probability in Figure 7.

Figure 7. RBC survival probability



Note: The top left plot shows the survival probability for combining the Poisson frequency and the empirical severity distribution (with a bootstrapped confidence interval). The top right shows the survival probability when combining the Poisson with parametric severity models. The bottom left figure shows a correlated frequency (negative binomial) paired with the empirical severity distribution. The bottom right shows the result for nonlinear correlations (Clayton copula with dependency parameter corresponding to a correlation of 0.2).

In the top left figure, the confidence interval obtained by means of bootstrapping indicates that the findings are again quite stable. Also, the findings for the other three plots shown in Figure 7 come to the same conclusions as those for the SII model, but as indicated on an even lower level in terms of survival probability. The figure bottom left

shows the survival probability p_s attained for different correlations ρ . As for SII the survival probability for $\rho = 1$ is above the one for $\rho = 0.1$ and the same explanation applies in the context here. The RBC results thus show that the security level the regulator aims for is often missed if an insurer writes cyber policies. It needs to be evaluated whether this low safety level under the RBC model needs to be raised to ensure stability in the insurance industry. From a dynamic point of view, the RBC model demands additional capital for business with excessive premium grow ($>10\%$ per year; Sharara et al., 2010). This might be especially relevant for cyber risk as the market is growing.

5.3. Swiss solvency test

For the SST the required capital, called RTK, is derived by calculating the tail value at risk (TVaR) of the loss distribution X and subtracting the expected loss (Bundesamt für Privatversicherungen, 2006). In the following, market, credit risk, discounting and the market value margin are neglected; only the ceteris paribus effect of underwriting cyber risk X is of interest:

$$rtk = TVaR_{0.99}(X) - E(X). \quad (27)$$

Generally, the TVaR shows better statistical properties than the value at risk as it is a coherent and therefore sub-additive (see McNeil et al., 2015). Moreover, it is more sensitive to the tail behavior of a distribution than, for example, volatility. As with SII, the total loss is subdivided into several LoBs and (sub-) modules and for the aggregation the same equations are applicable. In terms of random variables, the total loss is defined as:

$$X = X_{pr} + Z_{ex}, \text{ where } X_{pr} = (Z_p + Z_r). \quad (28)$$

The first and last terms subdivide the losses in normal and extreme events Z_{ex} . SST defines the normal losses as those below a threshold of CHF1 or 5 million, respectively. The choice of the exact threshold is at the discretion the insurer; we use a threshold of US\$5 million (and present the alternative threshold of US\$1 million in the Appendix F).³¹ With this threshold, our sample contains about 70% normal and 30% extreme losses.

³¹ As a simplification, we assume a nominal parity exchange rate between US\$ and CHF. Appendix F shows that the threshold to US\$1 million yields a lower survival probability and the survival probability the regulator aims for would not be achieved for the whole size-cover limit space analyze here. Additionally, for increasing portfolio sizes the survival level does not converge to the regulator's target.

Compared to the empirical findings of Eling and Wirfs (2016) that the optimal threshold should be set to US\$2 million corresponding to a 57%-quantile this is too high. On the other side, this threshold is rather low for the Pareto distribution to be a good approximation of the tail distribution (see Pickands-Balkema-de Haan theorem; McNeil et al., 2015).

Turning to the normal losses, the reserve risk Z_r and the premium risk Z_p are assumed by the regulator to be together lognormally distributed and the aggregation is done by adding up the lognormal parameters. Random and parameter risk for each LoB, premium risk, and reserve risk have to be aggregated.³² As in SII there is no specific category for cyber risk but they need to be allocated according to their risk nature. Table 4 shows the risk factors we consider as relevant to derive the aggregated parameters. The total variation coefficient for premium risk s_p is the two steps aggregation of first the variation coefficients for parameter s_{pa} and random risk s_r and second over all LoBs by the square root equation. Note as the factors for the reserve risk s_r have to be calibrated according to internal data, we discard them here. The mean and standard deviation are estimated from the normal losses observed in our data set. Then the distribution of the normal losses is assumed to be:

$$X_{pr} \sim LN(E(X_{pr}), \sigma_{pz}), \text{ where } \sigma_{pz} = s_{pz} \cdot E(X_{pr}). \quad (29)$$

Finally, the extreme events Z_{ex} are described by a Poisson compounded ordinary Pareto distribution (CPois).³³ The Pareto indexes α given by SST depend on the LoB and are reported in Table 4. In the following, a simple average of the different LoB's Pareto indexes is used to test the SST model. As we have already derived estimates for the parameters of the generalized Pareto distribution in the previous section, the estimated ordinary Pareto distribution would have a Pareto index of 0.63 (see Eling & Wirfs, 2016). That means the occurrence of severe losses is underestimated by SST. Moreover, the mean cannot be calculated. While this would suggest that the capital requirement for cyber risk under the standard approach does not ensure the ruin probability aimed for, it is important to remark that most parameters used above could be adapted to cyber risk

³² Since the premium and reserve risk have a similar risk structure and SST assumes no correlation between the two, the same risk factors are used.

³³ The framework allows for an alternative aggregation procedure that cannot be applied in this context.

specifics. The SST regulator allows to calibrate the location and dispersion of the distribution differently.

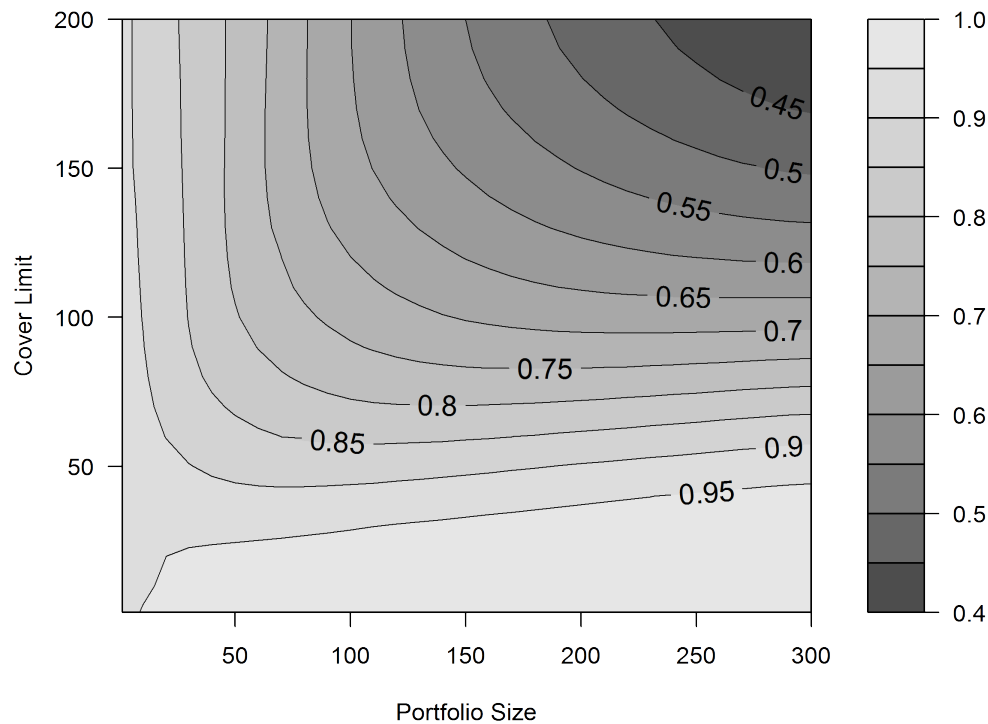
Table 4. SST parameters

LoB	w	Normal		Extreme
		s_{pa}	s_z	α
Liability	1/4	3.5%	11%	2
Financial losses	1/4	5%	5%	0.75
Legal costs	1/4	5%	5%	1.5
Others	1/4	4.5%	5%	1.5
Aggregate	1			1.43

The Pareto index can thus be chosen accordingly. However, a drawback of the CPois is that it requires risks to be independent. This is not generally true for cyber risk and for extreme events. The SST assumes extreme events to be independent and proposes a Panjer recursion to aggregate them. Moreover, the excess and normal losses are again assumed to be independent and are convoluted. Since the loss data from SAS is incident based, again a Panjer recursion is used to Poisson compound the empirical loss severities to derive the total loss on a cyber policy pool.

Figure 8 shows the survival probability for different combinations of portfolio sizes and cover limits. Our analysis shows that for small portfolio sizes and high cover limits the capital requirements are too low to ensure a TVaR at the 99% level. For the range of limits and sizes analyzed here, we can conclude that in the best case the insurer-only underwriting cyber risk would default once in ten years. However, compared to the other regulatory models, we see that the SST performs better in the sense that the survival probabilities are higher, at least for cover limits below US\$100 million. This is due to the more flexible modelling approach for the tails. Using a Pareto distribution for extreme values makes it possible to account better for the extreme values observed in cyber risks.

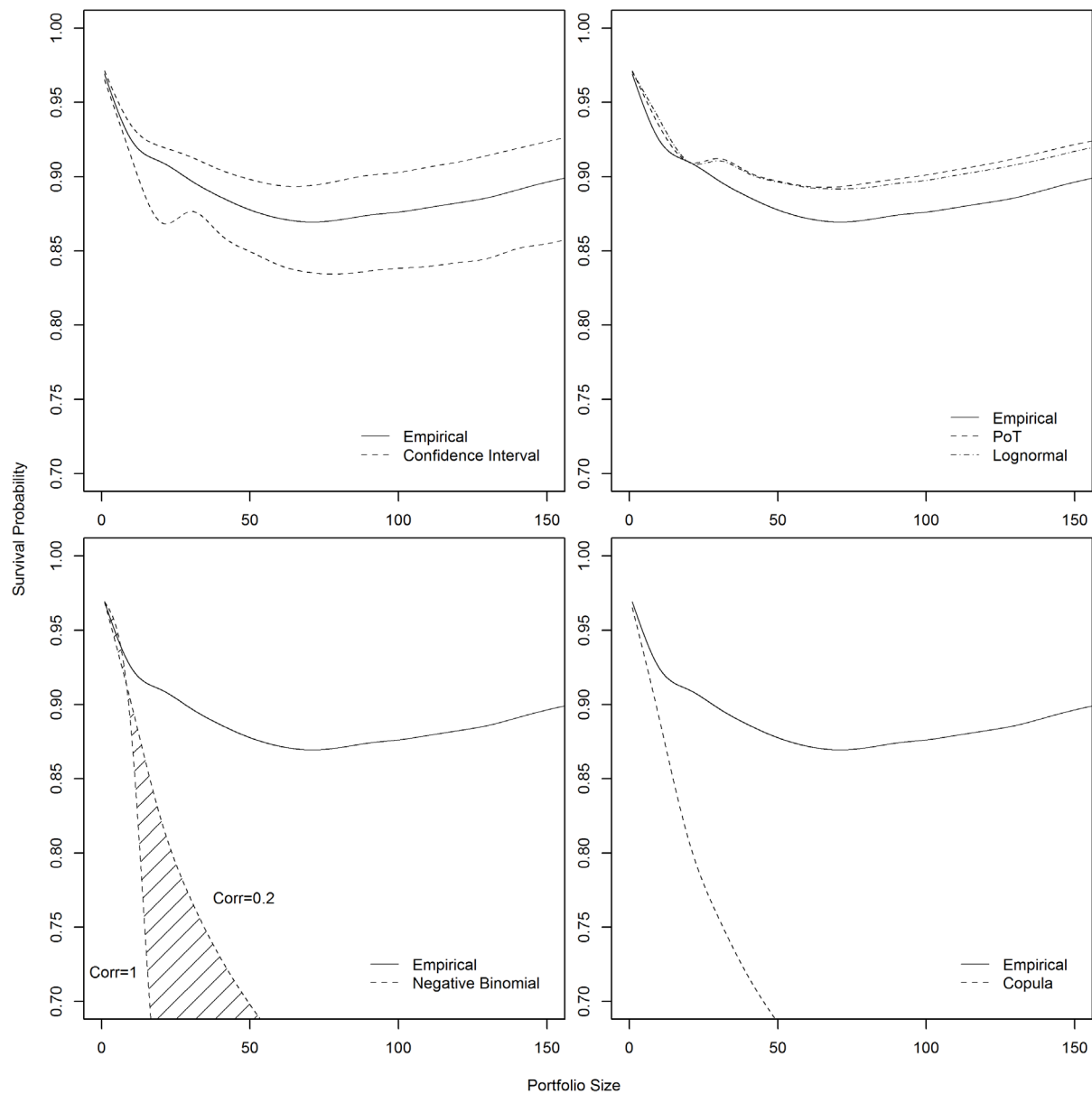
Figure 8. SST survival probability contour



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Figure 9 shows the contour plot for the survival probability at a cover limit of US\$50 million, again coming to identical conclusions as SII and US RBC; in this case, however, on higher levels of survival probability indicating that the SST model better achieves the regulatory goals. But still in the uncorrelated case the necessary portfolio size is between 50 and 100 to reach the desired safety level of 99%. As written in the introduction, that will not be the case for many insurance companies which start to develop their cyber insurance portfolio. Furthermore, if we deviate from the iid assumption the survival probability is substantially lower. At the end of the day it remains an empirical question what the dependence structure looks like and to date there is no answer, because there is no empirical research. But many people believe that cyber risks are not uncorrelated so that also the modelling results in the lower part of Figure 9 might be relevant and are thus of serious concern. It is also important to note here that for the case of non-linear dependence the survival probability never reaches the desired safety level of 99%, also when the portfolios are growing.

Figure 9. SST survival probability



Note: The top left plot shows the survival probability for combining the Poisson frequency and the empirical severity distribution (with a bootstrapped confidence interval). The top right shows the survival probability when combining the Poisson with parametric severity models. The bottom left figure shows a correlated frequency (negative binomial) paired with the empirical severity distribution. The bottom right shows the result for nonlinear correlations (Clayton copula with dependency parameter corresponding to a correlation of 0.2).

6 Conclusions

Our analysis shows that cyber risk is underestimated by all three regulatory capital models, especially for small portfolios sizes and high cover limits. Assuming a positive linear correlation or nonlinear dependencies between cyber risks further reduces the insurer's

survival probabilities. Extensive robustness checks show that the results are quite stable. For example, using different models for severity and frequency or alternative data sets for cyber risk does not qualitatively change our findings. This is an important result, because there is still substantial uncertainty around the empirical properties of cyber risk. Existing regulatory models thus have numerous shortcomings when applied to cyber risk. First, all models account for cyber risk only in a “one fits it all” approach since none of them uses specific cyber risk categories or factors. Using more specific risk factors and correlations calibrated with cyber risk data, would improve the models’ performance and ensure the safety level the regulator aims for. The heavy tails would call for replacing the lognormal distribution used by SII and SST by a power law distribution (e.g., Pareto distribution). Moreover, underwriting cyber risk models should pay close attention to the dependence structure characterizing cyber risks. A major part of cyber threats distributes over the internet and therefore the correlation might be higher than for other underwriting risk. In addition, extreme scenarios suggest that cyber risk could accumulate and become catastrophic (Kelly et al., 2016). While insurers can geographically diversify other cat risk, cyber risk propagated by the internet does not know any boundary so that geographical diversification might not work.

With respect to current regulatory models and new cyber insurance policies, the “one fits it all” approach might disturb risk-mitigating behavior and might not reward sound risk management. In certain cases, especially for operational cyber risk, the capital requirement for cyber risks should be increased to maintain the soundness of the insurance industry. Sound risk models will become even more important as the industry will make heavier use of new technologies (block chain, cloud computing, etc.) and cyber policies will make up a bigger share of an insurer’s underwriting portfolio. Moreover, governmental or private initiatives directed at enhancing the availability and quality of data about cyber risk will be crucial to build more sophisticated risk models.

We want to emphasize that the results of this paper should not be interpreted as an argument to massively increase capital requirements for cyber risk, especially in underwriting. Increasing capital requirements for cyber risk underwriting might hinder the development of the cyber insurance market. Our results illustrate that small cyber insurance portfolios might be problematic, but they also show that a sufficiently large portfolio can help to overcome the non-diversification trap. How the regulator should proceed might thus also depend on the development of the cyber insurance market in the supervised

region. In Europe or Asia where the market is in its infancy, the regulator should promote market development to support insurance companies in setting up sufficiently large portfolios and generating experiences on this new type of insurance exposure. The US insurance market is more developed so that specific capital requirements for cyber risk might be more relevant. Moreover, our results emphasize the importance to closely track the operational cyber risk within from the operations of the insurance companies. Here we might also see the need for more capital in the future.

We also recognize the current limitations of the cyber insurance market and the lack of data that limits the scope of the analyses presented here. Still, however, researchers and practitioners have highlighted that cyber risks seem to be heavy tailed and not independent (see, e.g., Maillart & Sornette, 2016; Eling & Wirfs, 2016; Böhme & Kataria, 2006). While the data does not allow us to determine the “correct” risk model, policymakers, regulators, and insurance managers should be aware of these properties. Our results thus also emphasize the need to consider the practice of cyber risk management both in the operational risk as well as in the underwriting of insurance companies. An own risk and solvency assessment as envisioned, for example, by the British regulator (see Prudential Regulation Authority, 2016) should also be implemented in other countries to analyze the potential risk exposure as well as the responsibilities and processes in place for their identification, evaluation, and management. Moreover, the “silent covers” (i.e., cyber covers in traditional policies) which are not the focus of this paper might be even more relevant than the cyber policies analyzed here, because they can affect the existing book of policies. Potential silent covers thus also need to be carefully considered within the own risk and solvency assessment.

7 References

- Advisen. (2015). Cyber liability insurance market trends: survey. http://www.partnerre.com/assets/uploads/docs/PartnerRe_Cyber_Liability_Trends_Survey_2015.pdf
- American Academy of Actuaries. (2007). An update to p/c risk-based capital underwriting factors: September 2007 report to the National Association of Insurance Commissioners P/C risk-based capital working group. http://www.actuary.org/files/publications/CPC_Report_on_RBC_Underwriting_Factors_to_NAIC_Property_RBC_Working_Group_092507.pdf

- Baer, W. S., & Parkinson, A. (2007). Cyberinsurance in IT security management. *IEEE Security and Privacy*, 5(3), 50-56.
- Basel Committee on Banking Supervision. (2006). International convergence of capital measurement and capital standards. <http://www.bis.org/publ/bcbs128.pdf>
- Bashan, A., Berezin, Y., Buldyrev, S. V., & Havlin, S. (2013). The extreme vulnerability of interdependent spatially embedded networks. *Nature Physics*, 9(10), 667-672.
- Betterley. (2015). The Betterley report - cyber/privacy insurance market survey 2015. http://betterley.com/samples/EPLI15_nt.pdf
- Biener, C., Eling, M., & Wirfs, J. H. (2015a). Insurability of cyber risk: an empirical analysis. *Geneva Papers*, 40(1), 131-158.
- Biener, C., Eling, M., Matt, A., & Wirfs, J. H. (2015b). Cyber Risk: Risikomanagement und Versicherbarkeit. *Institut für Versicherungswirtschaft der Universität St. Gallen*.
- Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. Fifth Workshop on the Economics of Information Security, University of Cambridge (U.K.). Working Paper.
- Braun, A., Schmeiser, H., & Schreiber, F. (2015). Portfolio optimization under Solvency II: implicit constraints imposed by the market risk standard formula. *Journal of Risk and Insurance*, 84(1), 177-207.
- Bundesamt für Privatversicherungen. (2006). Technisches Dokument zum Swiss Solvency Test. https://www.finma.ch/FinmaArchiv/bpv/download/d/SST_technischesDokument_061002.pdf
- Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks. <http://www.sei.cmu.edu/reports/10tn028.pdf>
- Chavez-Demoulin, V., Embrechts, P., & Hofert, M. (2015). An extreme value approach for modeling operational risk losses depending on covariates. *Journal of Risk and Insurance*, 83(3), 735-776.
- De Giorgi, E. (2005). Reward-risk portfolio selection and stochastic dominance. *Journal of Banking & Finance*, 29(4), 895-926.
- Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: a closer look at

- data breaches. *Journal of Cybersecurity*, 2(1), 3-14.
- Eling, M., & Wirfs, J. H. (2016). Cyber risk is different. Working Paper. <http://www.ivw.unisg.ch/~media/internet/content/dateien/institute-undcenters/ivw/wps/wp160.pdf>
- Eling, M., Schmeiser, H., & Schmit, J. T. (2007). The Solvency II process: overview and critical analysis. *Risk Management and Insurance Review*, 10(1), 69-85.
- Embrechts, P., Nešlehová, J., & Wüthrich, M. V. (2009). Additivity properties for value-at-risk under Archimedean dependence and heavy-tailedness. *Insurance: Mathematics and Economics*, 44(2), 164-169.
- Embrechts, P., McNeil, A. J., & Straumann, D. (2002). Correlation and dependence in risk management: properties and pitfalls. *Risk Management: Value at Risk and Beyond*, 176-223.
- European Commission (EC). (2010). QIS5 technical specifications. https://eiopa.europa.eu/Publications/QIS/QIS5-technical_specifications_20100706.pdf
- European Commission (EC). (2014). Commission delegated regulation (EU): supplementing directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II). *Official Journal of the European Union*.
- European Insurance and Occupational Pensions Authority (EIOPA). (2014). The underlying assumptions in the standard equation for the solvency capital requirement calculation. https://eiopa.europa.eu/Publications/Standards/EIOPA-14-322_Underlying_Assumptions.pdf
- European Insurance and Occupational Pensions Authority (EIOPA). (2017). EIOPA statistics - accompanying note. https://eiopa.europa.eu/Publications/Insurance%20Statistics/SQ_Accompanying%20note.pdf
- Haas, A., & Hofmann, A. (2014). Risiken aus Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. *ZVersWiss*, 103(4), 377-407.
- Hess, C. (2011). The impact of the financial crisis on operational risk in the financial services industry: empirical evidence. *Journal of Operational Risk*, 6(1), 23-35.

- Holzmüller, I. (2009). The United States RBC standards, Solvency II and the swiss solvency test: a comparative assessment. *Geneva Papers on Risk and Insurance-Issues and Practice*, 34(1), 56-77.
- Ibragimov, R. (2009). Portfolio diversification and value at risk under thick-tailedness. *Quantitative Finance*, 9(5), 565-580.
- Ibragimov, R., Jaffee, D., & Walden, J. (2008). Nondiversification traps in catastrophe insurance markets. *Review of Financials Studies*, 22(3), 959-993.
- Ibragimov, R., & Prokhorov, A. (2016). Heavy tails and copulas: limits of diversification revisited. *Economics Letters*, 149, 102-107.
- Ibragimov, R., & Walden, J. (2007). The limits of diversification when losses may be large. *Journal of Banking and Finance*, 31(8), 2551-2569.
- Insurance Information Institute. (2017). Cybersecurity and identity theft coverage: the state of the industry. <http://www.iii.org/article/cybersecurity-and-identity-theft-coverage-the-state-of-the-industry>
- Jacobs, J. (2014). Analyzing Ponemon cost of data breach. <http://datadrivensecurity.info/blog/posts/2014/Dec/ponemon>
- Kelly, S., Leverett, E., Oughton, E. J., Copic, J., Thacker, S., Pant, R., Pryor, L., Kassara, G., Evan, T., Ruffle, S. J., Tuveson, M., Coburn, A. W., Ralph, D., & Hall, J. W. (2016). Integrated infrastructure: cyber resiliency in society, mapping the consequences of an interconnected digital economy. Centre for Risk Studies, University of Cambridge.
- KPMG. (2017). Insurance Thinking Ahead: Neues Denken, neues Handeln – Versicherungen im Zeitalter von Digitalisierung und Cyber.
- National Association of Insurance Commissioners (NAIC). (2009). Risk-based capital, forecasting and instructions 2009: property/casualty. http://codes.ohio.gov/pdf/oh/admin/2016/3901-3-15_ph_em_ne_app1_20091228_1156.pdf
- National Association of Insurance Commissioners (NAIC). (2017). Property and casualty risk-based capital newsletter, 21.1. http://www.naic.org/documents/cmte_e_prbc_newsltr_1708.pdf

- National Association of Insurance Commissioners (NAIC). (2016a). Operational risk. http://www.naic.org/cipr_topics/topic_op_risk.htm.
- National Association of Insurance Commissioners (NAIC). (2016b). Cyber Risk. http://www.naic.org/cipr_topics/topic_cyber_risk.htm
- National Association of Insurance Commissioners (NAIC). (2016c). Catastrophe risk (E) subgroup. http://www.naic.org/cmte_e_cat_risk_sg.htm
- National Association of Insurance Commissioners (NAIC). (2016d). Report on the cybersecurity insurance coverage supplement. http://www.naic.org/documents/committees_ex_cybersecurity_tf_report_cyber_supplement.pdf
- Neslehová, J., Embrechts, P., & Chavez-Demoulin, V. (2006). Infinite mean models and the LDA for operational risk. *Journal of Operational Risk*, 1(1), 3-25.
- Maillart, T., & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *European Physical Journal B*, 75(3), 357-364.
- Marsh. (2016). Continental European cyber risk survey: 2016 report. <https://www.marsh.com/de/de/insights/research-briefings/continental-european-cyber-risk-survey-2016-report.html>
- McAfee. (2014). Net losses: estimating the global cost of cybercrime. <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cyber-crime2.pdf>
- McNeil, A. J., Embrechts, P., & Frey, R. (2015). Quantitative risk management: concepts, techniques and tools. Princeton University Press.
- Moscadelli, M. (2004). The modelling of operational risk: experience with the analysis of the data collected by the Basel committee. Technical Report 517. Banca d'Italia.
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukan, S. K. (2013). Cyber-risk decision models: to insure it or not?. *Decision Support Systems*, 56(1), 11-26.
- Panjer, H. H. (1981). Recursive evaluation of a family of compound distributions. *Astin Bulletin*, 12(1), 22-26.

- Ponemon Institute. (2015). 2015 cost of cyber crime study: global. http://informationsecurity.report/Resources/Whitepapers/5fe1dd7e-b46d-49f6-833a-d192cecb29e3_2015-cost-cyber-crime-study-global-pdf-10-w-2093.pdf
- Privacy Rights Clearinghouse (PRC). (2016). Data breaches. <https://www.privacyrights.org/data-breaches>
- Prudential Regulation Authority (PRA). (2016). Cyber insurance underwriting risk. Consultation Paper CP39/16.
- Scarrott, C., & MacDonald, A. (2012). A review of extreme value threshold estimation and uncertainty quantification. *Statistical Journal*, 10(1), 33-60.
- Seeley, A. (2012). Implementation of a catastrophe risk charge in p&c risk-based capital. http://www.casact.org/education/infocus/2012/handouts/Per_1271_handout_647_0.pdf
- Sharara, I., Hardy, M., & Saunders, D. (2010). Regulatory capital standards for property and casualty insurers under the US, Canadian and proposed Solvency II (standard) formulas. <https://www.soa.org/Files/Research/research-2010-08-regulatory-cap.pdf>
- Statista. (2017a). Underwriting expense ratio of property/casualty insurance in the United States from 2009 to 2015 (in billion U.S. dollars). <http://www.statista.com/statistics/437137/underwriting-expense-ratio-pc-insurance-usa>
- Statista. (2017b). Loss ratio of property/casualty insurance in the United States from 2009 to 2015. <https://www.statista.com/statistics/437126/loss-ratio-pc-insurance-usa>
- Statista. (2017c). Life and non-life insurance direct premiums written globally from 2013 to 2015 (in trillion U.S. dollars). <https://www.statista.com/statistics/217278/world-life-and-nonlife-insurance-premiums-written>
- Swiss Re. (2015). Investors' day – Rüschiikon, December 8, 2015. http://media.swissre.com/documents/id2015_full_slide_package.pdf
- Villaseñor-Alva, J. A., González-Estrada, E. (2009). A bootstrap goodness of fit test for the generalized Pareto distribution. *Computational Statistics and Data Analysis*, 53(11), 3835-3841.

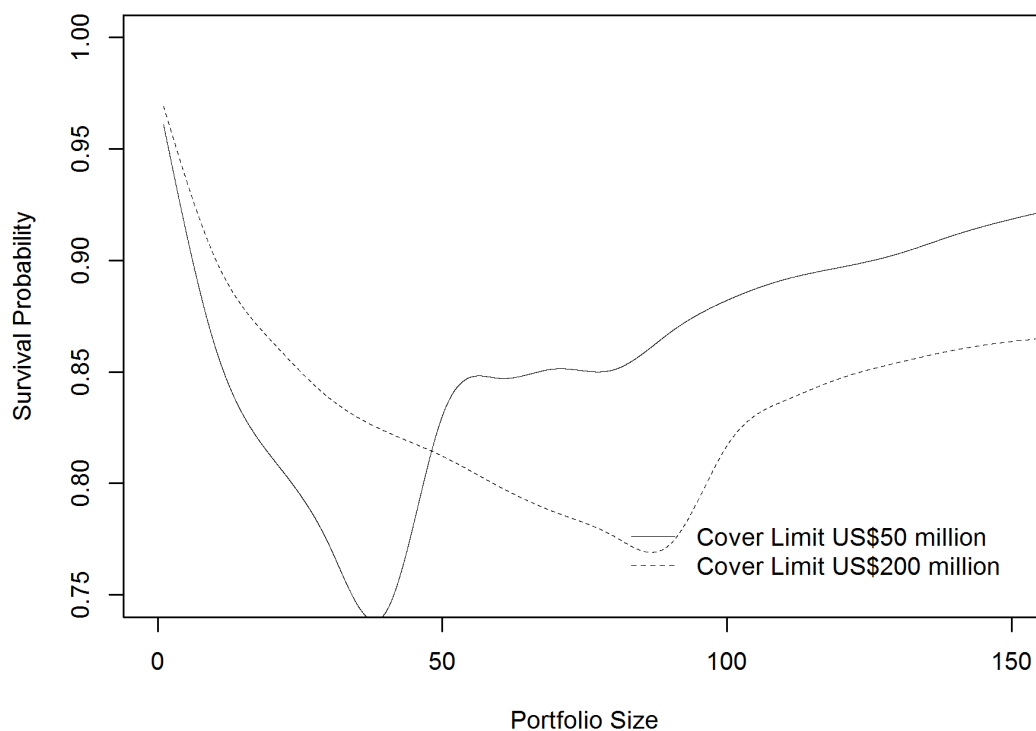
- Wang, S. (1998). Aggregation of correlated risk portfolios: models and algorithms. *Proceedings of the Casualty Actuarial Society*, 85(163), 848-939.
- Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *European Physical Journal B*, 89(1), 7.
- Wirfs, J. H. (2016). How to organize cyber risk transfer? Working Paper. <https://www.alexandria.unisg.ch/248635/>
- World Economic Forum (WEF). (2014). Global risks 2014: ninth edition. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

8 Appendices

Appendix A. Comparison of different cover limits

We compared the result obtained by combining Poisson frequency with the empirical severity distribution. We slice the contour plots from the main text at US\$50 and at 200 million and then compare them. For SII, Figure A1 shows the survival probability as a function of the portfolio size.

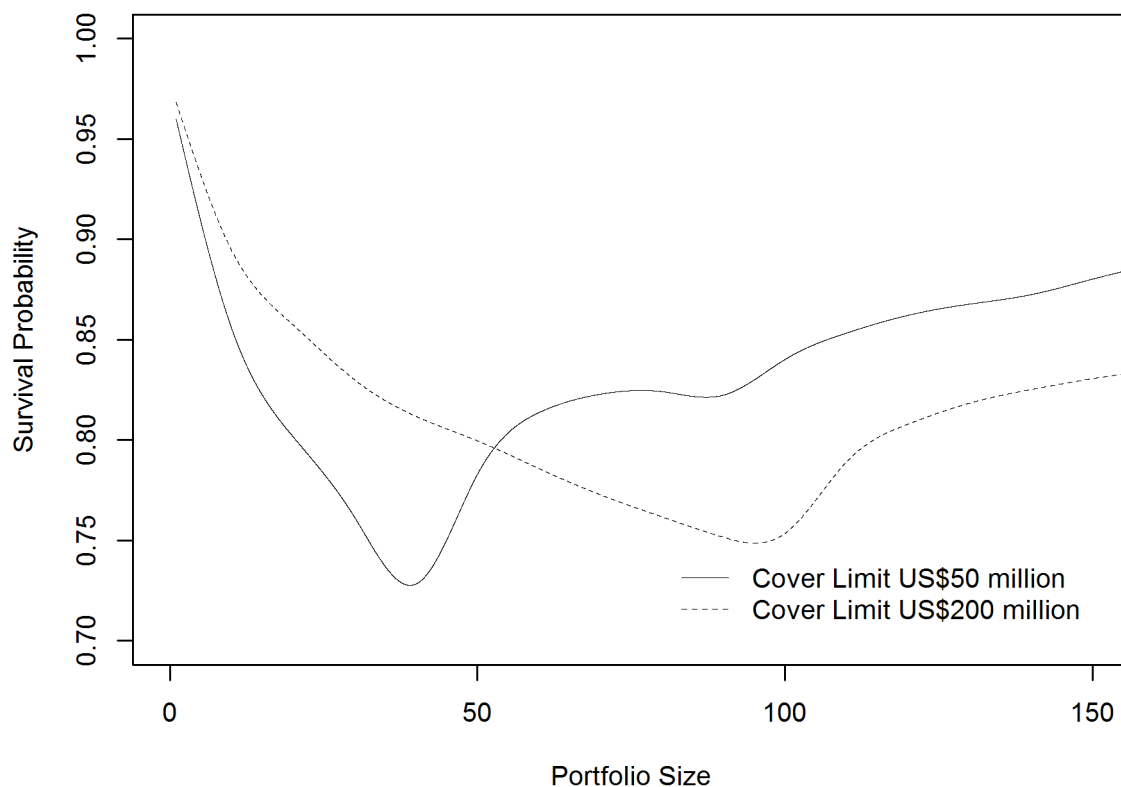
Figure A1. SII survival probability (different cover limits)



Note: Both curves show the survival probabilities attained by combining a Poisson distribution for the frequency with the empirical distribution for the severity. The space between the grid points is interpolated by cubic splines.

Our finding that SII does not ensure a sufficiently high default probability for small cyber portfolios is confirmed. Moreover, the plot shows that as the portfolio grows diversification does not work well at first since the survival probability is decreasing. Only after a certain critical portfolio size is attained the security level increases again. These findings are similar for the RBC model as shown in Figure A2.

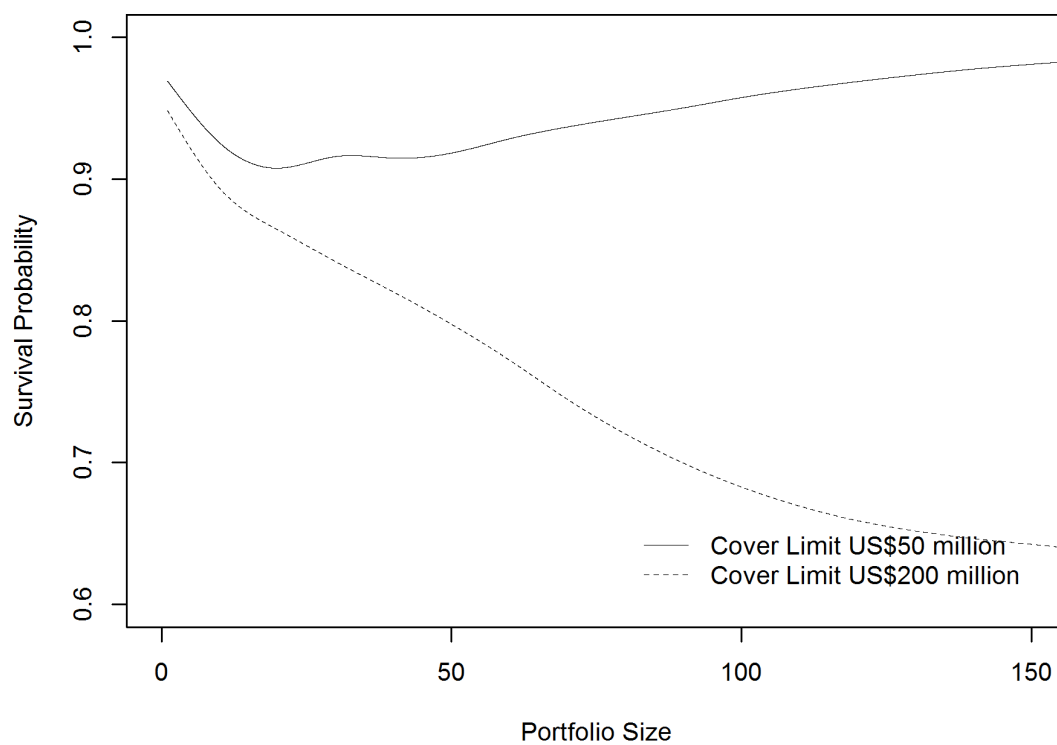
Figure A2. RBC survival probability (different cover limits)



Note: Both curves show the survival probabilities attained by combining a Poisson distribution for the frequency with the empirical distribution for the severity. The space between the grid points is interpolated by cubic splines.

In comparison to SII the plot shows that the RBC security level reached is low over the whole range of portfolio sizes and is far away from the levels regulators usually aim for. Even with a portfolio size of 150 the attained security level does not reach the level for just one risk. The result for SII and RBC both confirm and extend the findings of Ibragimov et al. (2008) for the security level as a special case of value function. The cover limits combined with heavy tailed severity cause the “value of the portfolio” to decrease and then increase as the portfolio size increases. As a consequence, if risk management takes the underwriting decision, the company would eventually be stocked in a non-diversification trap. The situation is a bit different in the case of SST, as shown in Figure A3.

Figure A3. SST survival probability (different cover limits)

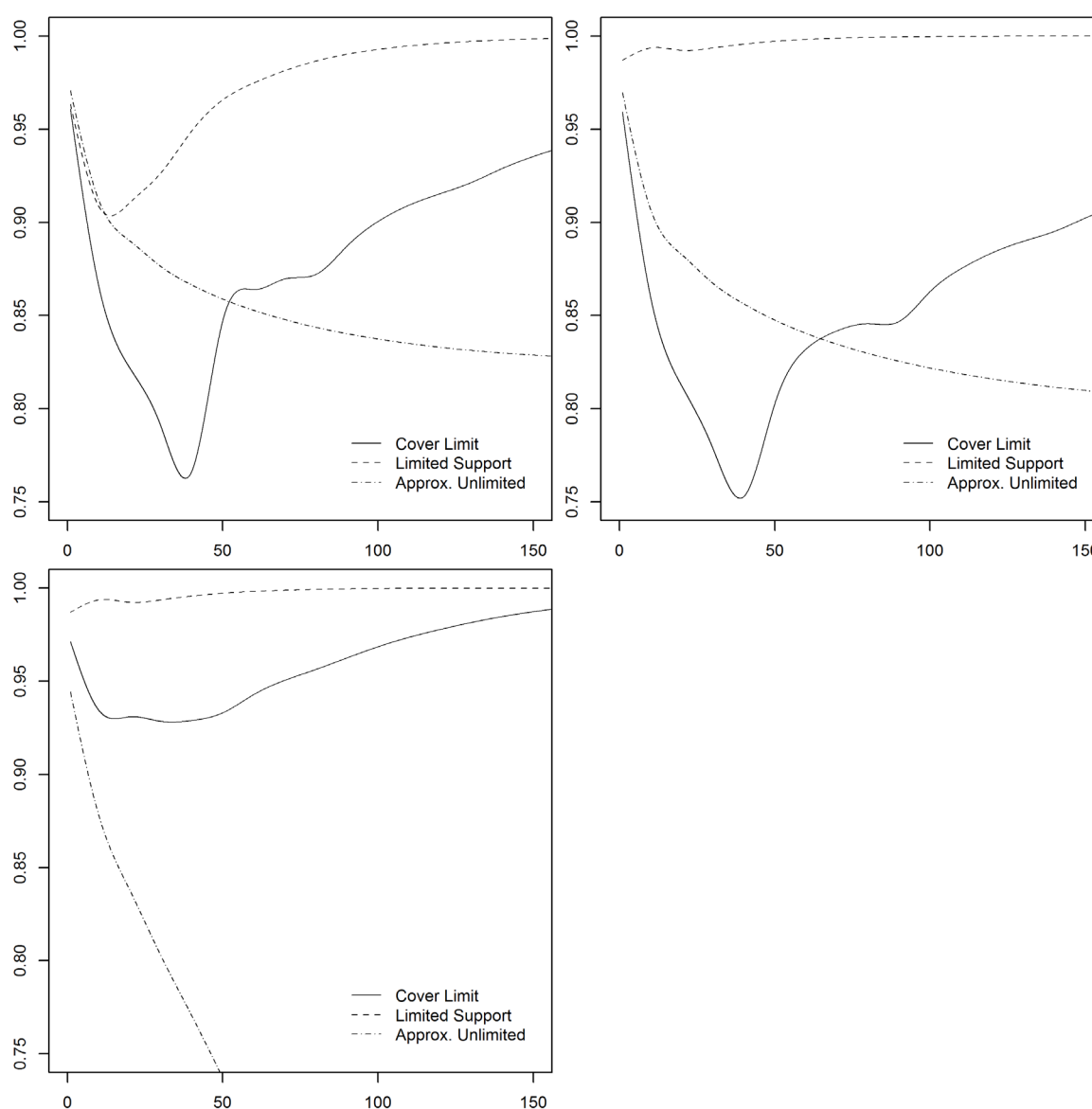


Note: Both curves show the survival probabilities attained by combining a Poisson distribution for the frequency with the empirical distribution for the severity. The space between the grid points is interpolated by cubic splines.

Appendix B. Cover limit vs. limited support

In order to provide further insights, here we compare our results with the findings of Ibragimov et al. (2007). For that we use three modelling assumptions for each regulatory model. First, we plot the survival probability curve for a cover limit of US\$50 million (cover limit) as shown in the main text.

Figure B1. Cover limit vs. limited support



Note: All curves show the survival probabilities attained by combining a Poisson distribution for the frequency with the empirical distribution for the severity. The line “Cover Limit” compresses the tails down to the cover limit, “limited liability” slices at the cover limit, and “approx. unlimited” approximates the case of unlimited support of the distribution. The plot top left shows the results for SII, top right for RBC, and bottom left for SST.

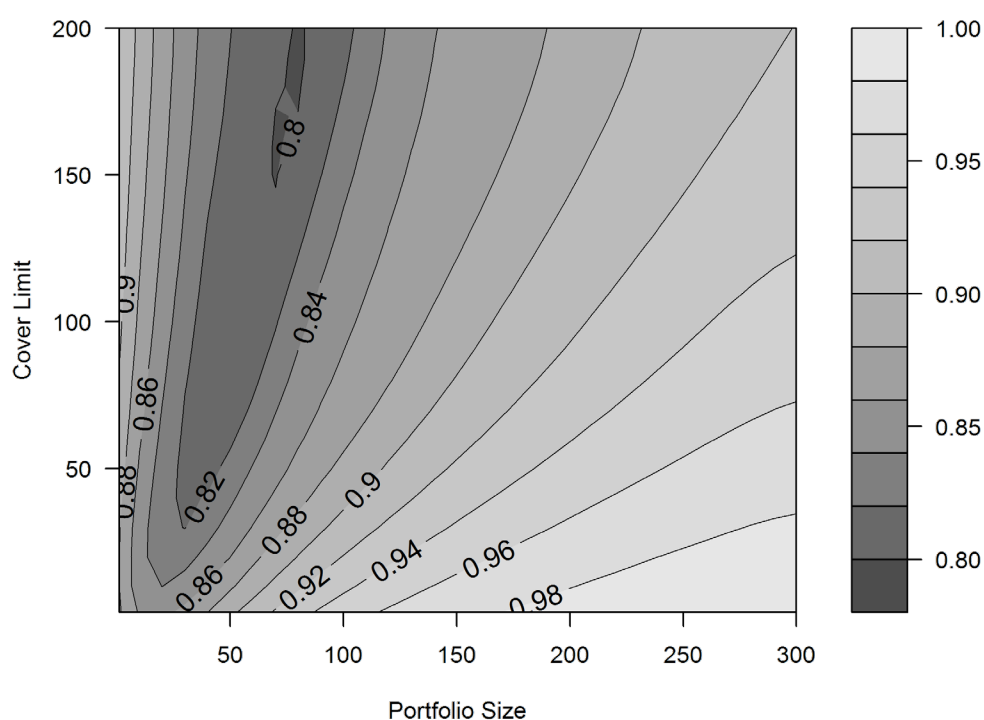
A cover limit means that the insurer is covering the loss only up to the limit, even if it was higher. In this case the probability mass above the limit is squeezed down to the threshold. Imaginably this builds up two peaks at the distribution's extremes: one close to zero and one at the limit. Moreover, the resulting distribution is discontinuous.

In comparison, Ibragimov et al. (2008) use distributions with limited liability or support. Limited liability would be quite similar to cover limits and it can be considered for example as the shareholders' option like exposure on an aggregate firm level. For limited support the tail is not compressed down, but the distribution is sliced instead at the threshold. This leads to a monotonic decreasing distribution function. Our last approach sets the threshold high and is supposed to approximate the results for a heavy tail distribution without any limits in support (approx. unlimited). Figure B1 shows the results for the different tail assumptions. We see that replacing the case of limited support with cover limit leads to a more extreme plunge in the survival probability for small sizes portfolios and a slower recovery as the portfolio size increases. Finally, we see that using a heavy tailed distribution without any limits would flatten out the u-shaped survival curve to the point where it monotonically decreases (e.g., RBC).

Appendix C. Robustness test with reduced data set

The same analysis as in the main text is conducted for a smaller SAS data set taken from Biener et al. (2015). This data set can be considered as a subset of the data used in the main text as it records only a total number of 994 losses between 1995 and 2010. Figure C1 shows the survival probability contours for the SII model. The finding is almost identical to the one for the extended data set. For small portfolio sizes the survival probability falls short of the 99.5% value the regulator aims for.

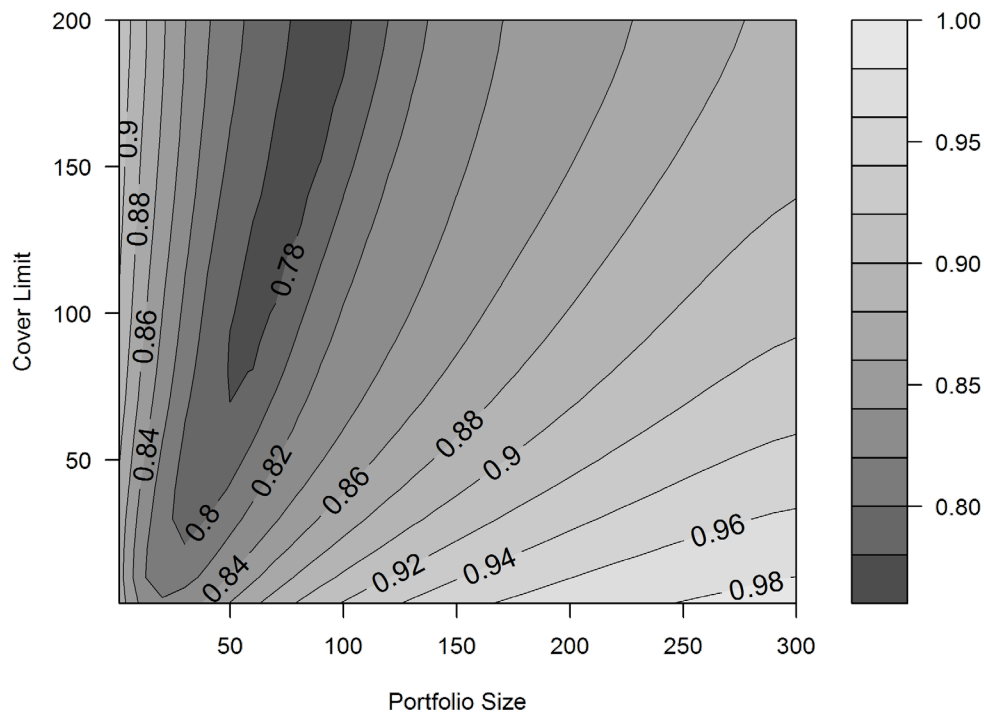
Figure C1. SII survival probability contours



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Figure C2 shows the survival probability contours for the RBC model. The finding is almost identical to the one for the extended data set. Compared to SII, the survival probability for the RBC model is everywhere on the size-cover limit space lower than the SII model. For small portfolio sizes, the survival probability can drop as low as about 78%. This is much lower than what the regulator usually aims for.

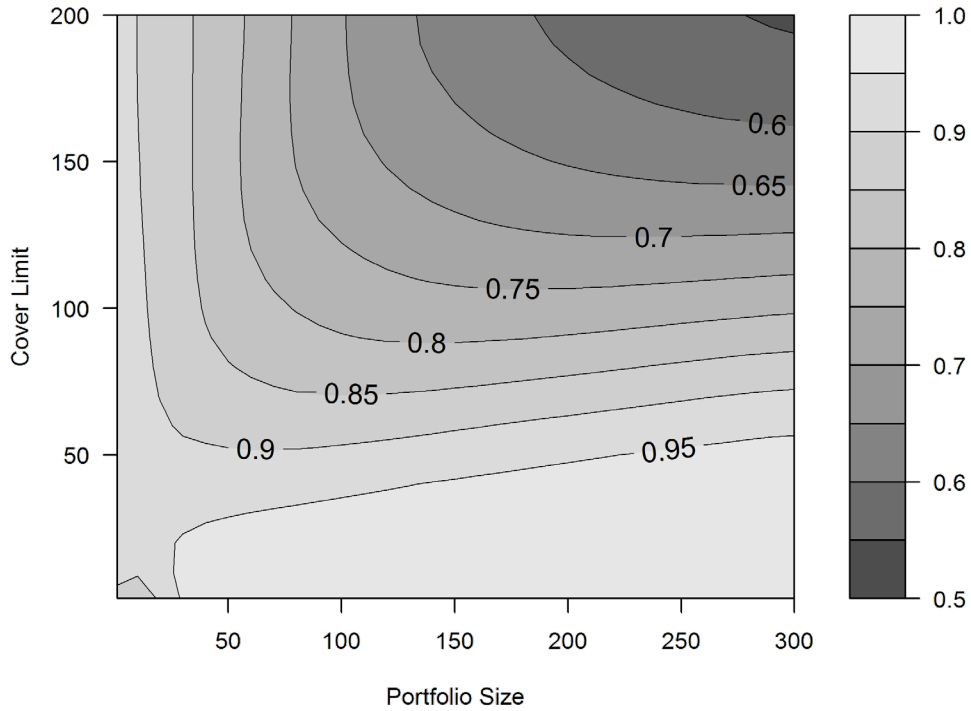
Figure C2. RBC survival probability contours



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Figure C3 shows the survival probability contours for the SST model. The finding is almost identical to the one for the extended data set in the main text. For low cover limits, SST achieves the highest survival probability compared to all three regulatory models analyzes here. However, as the cover limit is expanded the security level drops to as low as 50%. This is much lower than the 99% the regulator aims for.

Figure C3. SST survival probability contours



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Since the results for the reduce SAS data sets is almost identical to the extended SAS data set in the main text we can conclude that our results are stable with respect to the choice of the time period.

Appendix D. Robustness test with PRC data set

As an additional robustness test we conducted the same analysis with another frequently used data set on data breaches (e.g., Maillart & Sornette, 2010; Edwards et al., 2016) provided by the Privacy Rights Clearinghouse (PRC, 2016). It contains data breaches that occurred between 2005 and 2015 in the United States. We follow Edwards et al. (2016) and delete all observations with zero breached records and attain a sample of 2,266 observations. The database documents the number of records breached per incident and not the financial losses. To derive an estimate for the financial losses Z we multiply each record R with an estimate of the average costs per data breach (see, e.g., Ponemon Institute, 2015; Jacobs, 2014):

$$\ln(Z) = 7.68 + 0.76 \cdot \ln(R). \quad (\text{D1})$$

We note that since the data set only tracks breaches, it might not be representative for cyber risk generally as it does not contain all possible types of cyber incidences. Table D1 shows summary statistics analogous to Table 1 for the alternative data set.

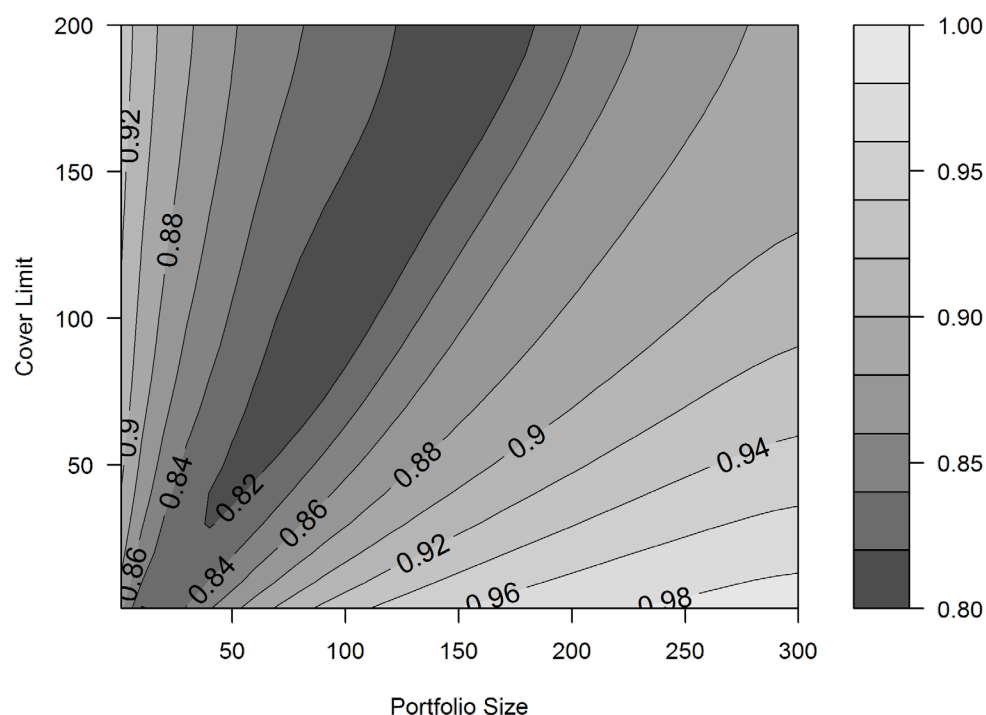
Table D1. Cyber risk parameters (in million US\$)

		n	Mean	Std	VaR _{0.995}	TVaR _{0.99}
Severity (per incident)	Z	2,266	16.3	126.6	574.3	966.5
Frequency (per year)	N		0.07	0.27		
LDA (per company)	X		1.2	34.7	23.7	112.0
Severity (truncated)	Z_t	2,266	5.2	11.2	50.0	50.0
LDA (truncated)	X_t		0.39	3.35	23.8	29.4

Note: n: sample size, Std: standard deviation, VaR_{0.995}: value at risk, TVaR_{0.99}: tail value at risk. All numbers, besides n, are reported in million US\$.

Figure D1 shows the survival probability contours for the SII model. The findings are almost identical to those presented in the main body of the paper. For small portfolio sizes, the survival probability falls short of the 99.5% value the regulator aims for; it can drop as low as about 82%.

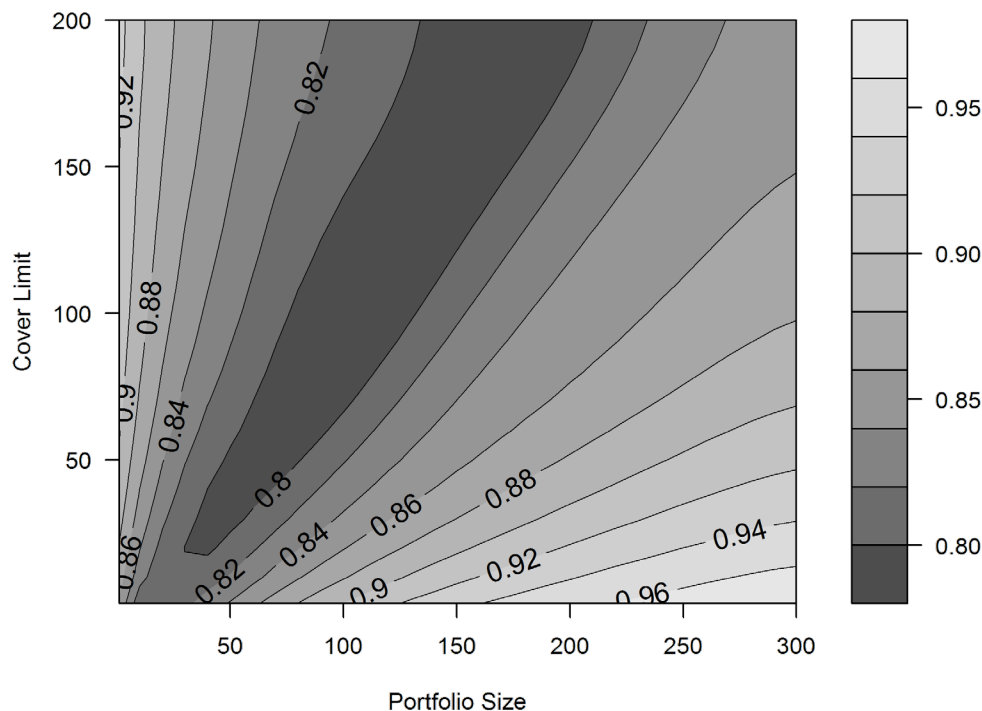
Figure D1. SII survival probability contours



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Figure D2 shows the survival probability contours for the RBC model. The finding is almost identical to the one for the extended data set. Compared to SII, the survival probability for the RBC model is everywhere on the size-cover limit space lower. For small portfolio sizes, the survival probability can drop as low as about 80%. This is much lower than what the regulator usually aims for.

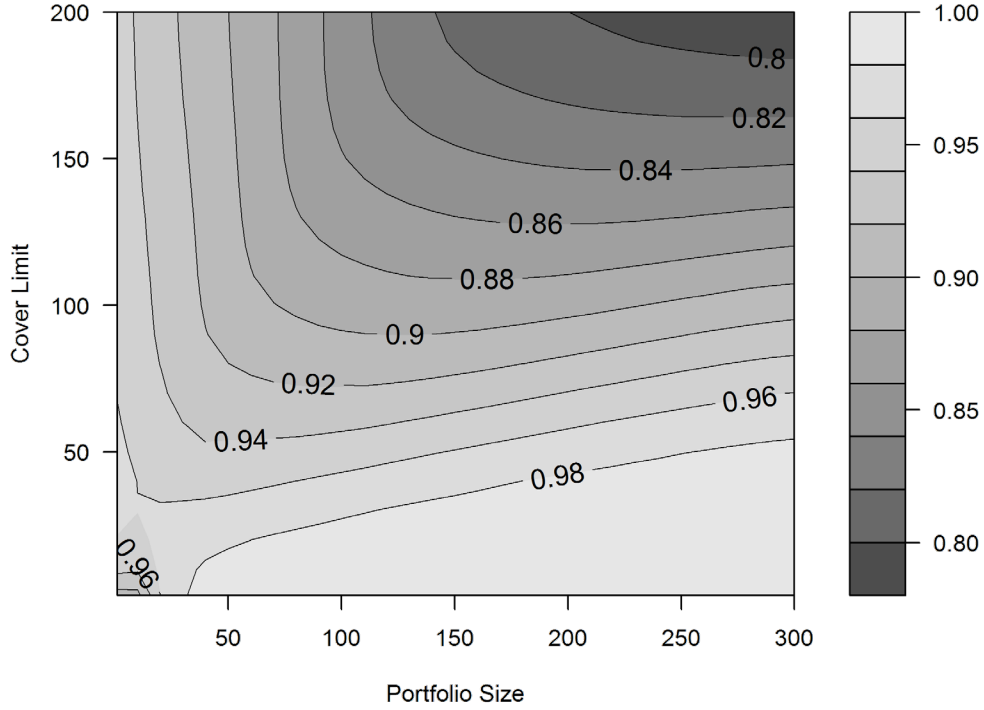
Figure D2. RBC survival probability contours



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Figure D3 shows the survival probability contours for the SST model. The finding is almost identical to the one for the data set in the main text. For low cover limits, SST achieves the highest survival probability compared to the three regulatory models analyzed here. However, as the cover limit is expanded the survival probability drops to as low as 80%. This is much lower than the 99% the regulator aims for.

Figure D3. SST survival probability contours



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Since the results for the PRC and SAS data sets used in the main text are very similar we can conclude that our result is stable with respect to the choice of data.

Appendix E. Derivation of aggregation equation

Proof: Inserting the regulatory model $m(\mathbf{v} \cdot \mathbf{s})$ from Equation (11) into the square root Equation (18) and introducing portfolio weights $\mathbf{w}$ (Equation 20):

$$rc = \sqrt{(m(\mathbf{v} \cdot \mathbf{w} \cdot \mathbf{s}))^T \cdot \mathbf{P} \cdot m(\mathbf{v} \cdot \mathbf{w} \cdot \mathbf{s})},$$

where, $v_i = \mathbf{v} \cdot \mathbf{w}$ is the volume measure per each risk category i . Since $m(\cdot)$ is linear for the models we analyze, we have:

$$= \sqrt{(m(\mathbf{v})^T \cdot (\mathbf{w} \cdot \mathbf{s})^T \mathbf{P} (\mathbf{s} \cdot \mathbf{w}) \cdot m(\mathbf{v}))},$$

$$= \sqrt{(m(v))^2 \cdot (\mathbf{w} \cdot \mathbf{s})^T \mathbf{P} (\mathbf{s} \cdot \mathbf{w})},$$

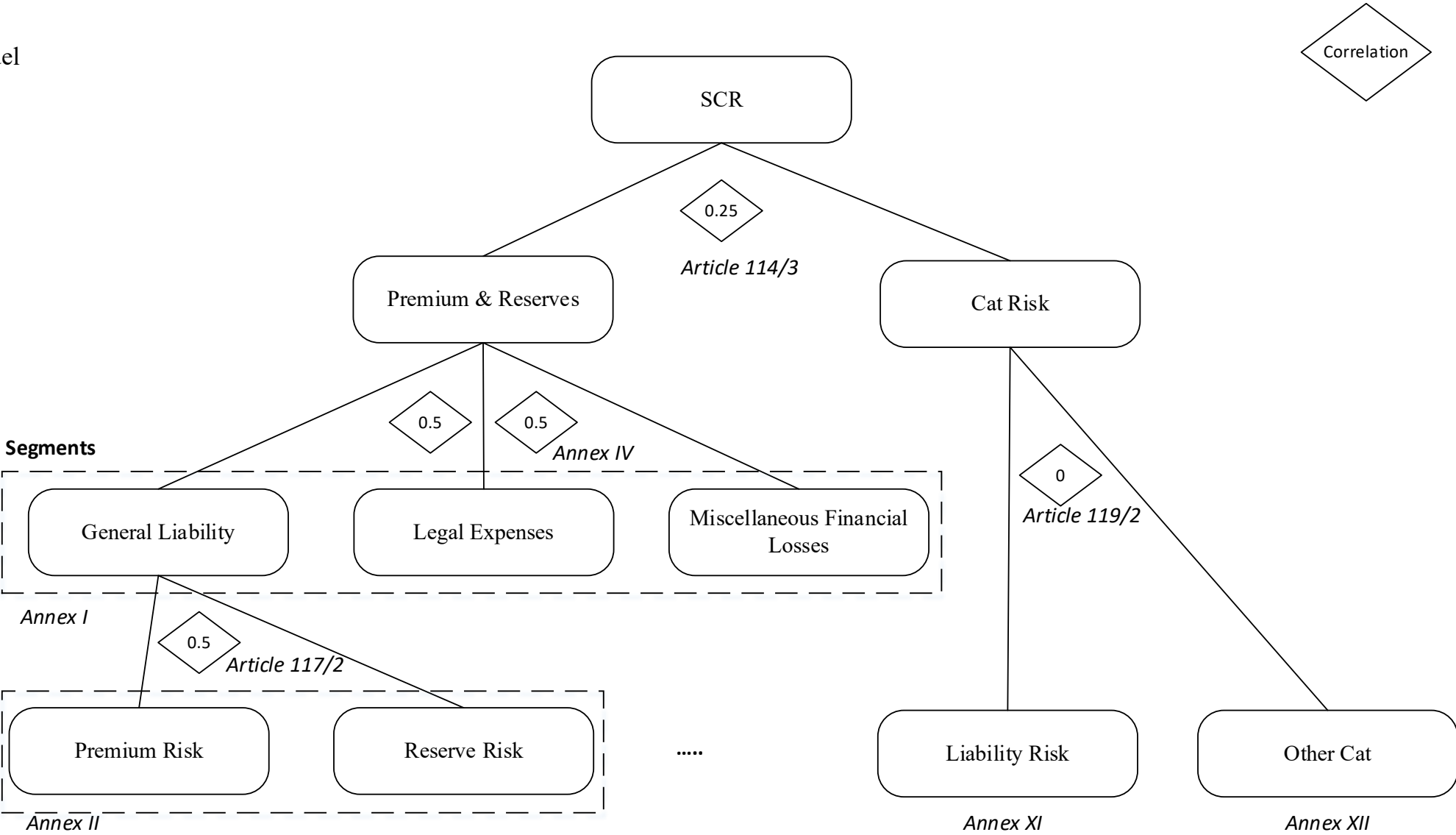
$$= m(v) \cdot \sqrt{(\mathbf{w})^T \cdot \mathbf{s} \cdot \mathbf{P} \cdot \mathbf{s} \cdot \mathbf{w}},$$

$$= m(v) \cdot \sqrt{\mathbf{w}^T \mathbf{\Sigma} \mathbf{w}},$$

$$= m(v) \cdot s, \quad \blacksquare$$

where $\mathbf{P}$ denotes the correlation matrix and $\mathbf{\Sigma}$ is the covariance matrix. Calculating required capital m for each risk categories separately before we aggregate them by the square root equation is thus equivalent to aggregate the risk factors s first before applying them on the aggregated volume measure v . This result applies to all linear regulatory models that build on the square root equation. This is the well-known equation for a portfolio's standard deviation or in our context the standard deviation of the underwriting cyber portfolio. For the SII model we would have $scr = m \cdot s = 3 \cdot s \cdot v$.

Figure E1. SII model

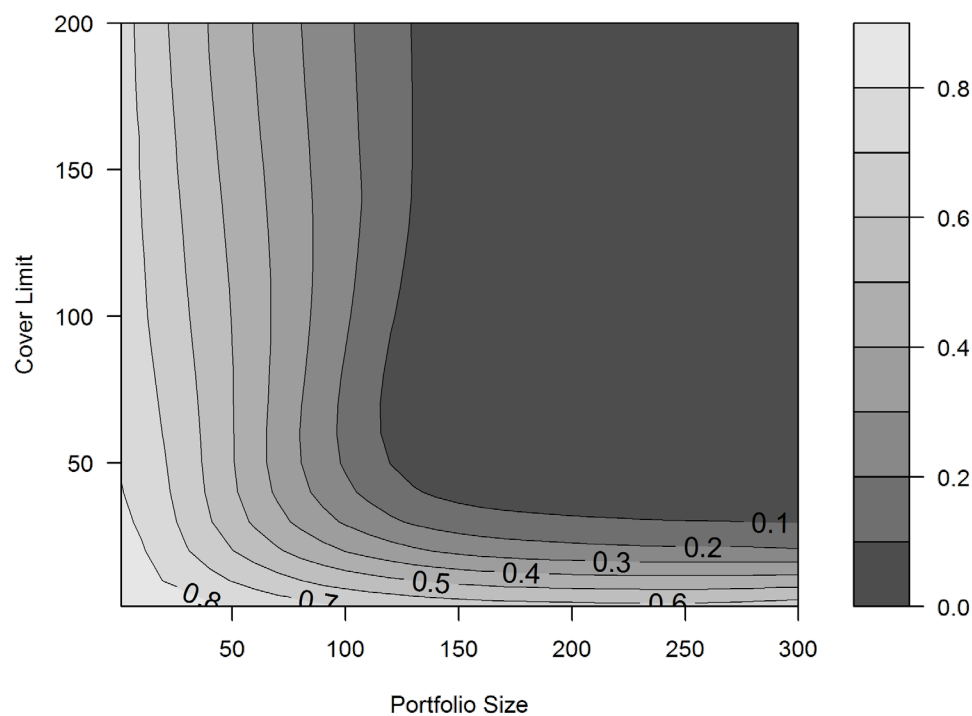


Reference: EC, 2014

Appendix F. SST with US\$1 million threshold for the Pareto distribution

As mentioned in the main text, the SST framework suggests two thresholds for the Pareto distribution that are supposed to model the extreme losses. The insurer can choose to set the threshold at US\$1 or 5 million¹. While in the main text we use the more conservative threshold of US\$5 million, we additionally report here the result for a threshold of US\$1 million. As Figure F1 shows, the survival probability is much lower than for the higher threshold and it never reaches the regulator's target for the whole size-cover limit space. Moreover, the survival probability is not u-shaped, suggesting that there is no benefit of diversification and the fast decaying curve projects that the survival probability will not converge to the regulators' target even for ever-increasing portfolio sizes.

Figure F1. SST survival probability contour (US\$1 million threshold)



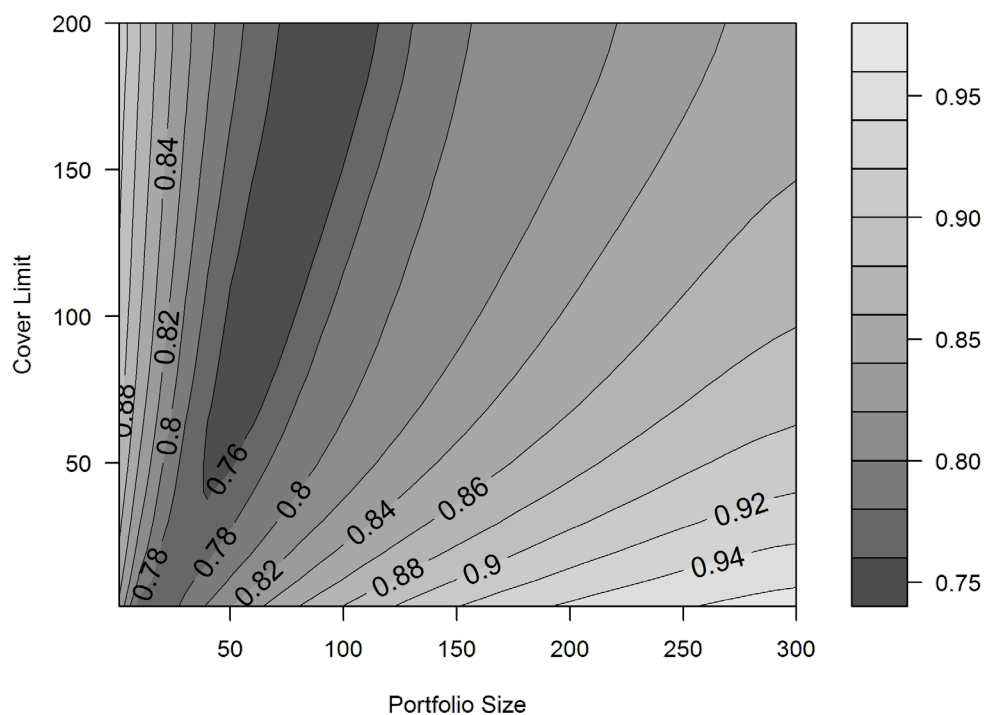
Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

¹ As a simplification we assume a nominal parity exchange rate between US\$ and CHF.

Appendix G. Different loss ratio

Since we need assumption about the loss ratio b for the SII and RBC model, our results are sensitive to the choice of b . Because the SST model builds directly on the expected value as a volume measure instead of premiums and reserves, we do not need robustness checks for the loss ratio for SST. While in the main text we use an average of property and causality loss ratio for the US (Statista, 2017b), here we analyze the effect if the loss ratio would increase to $b=0.8$. Figure G1 shows the contour plot for SII.

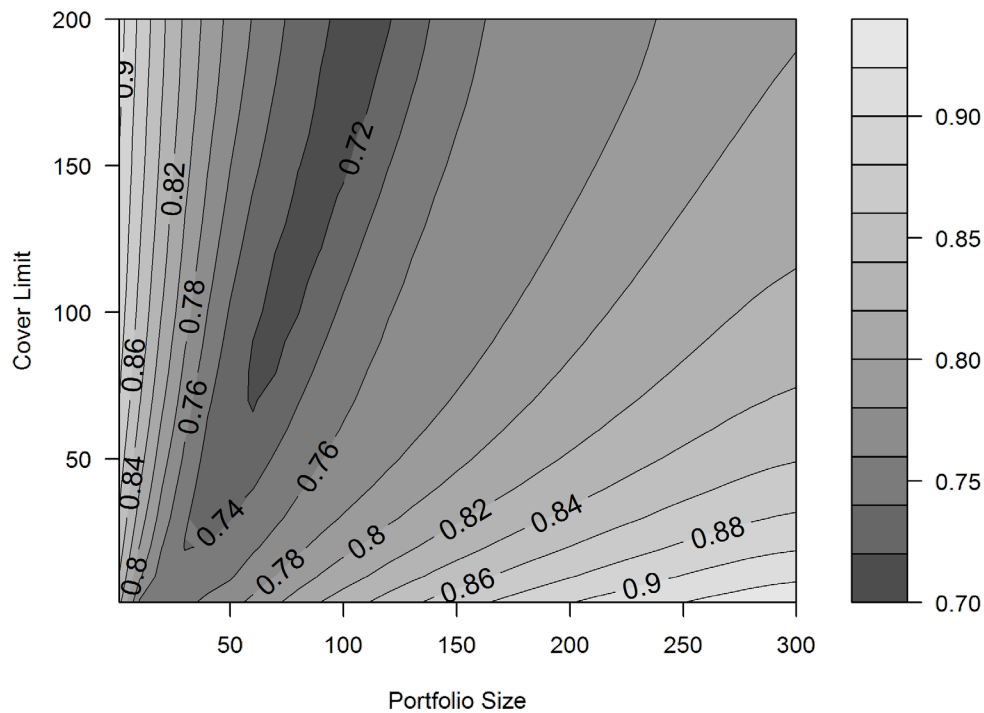
Figure G1. SII survival probability contour (loss ratio 0.8)



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

When comparing SII results for a higher loss ratio to the one in the main text we can see that for every point in the cover limit and portfolio size space the survival probability is lower. Similar results are shown for RBC in Figure G2.

Figure G2. RBC survival probability contour (loss ratio 0.8)



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

The explanation for this finding is as follows. When the loss ratio increases *ceteris paribus* the premium volume decreases. Then a lower premium volume would reduce the required capital since the latter is a positive monotonic function of the premium volume. To summarize premiums do not necessarily serve as a good approximation of the volume measure like the expected value. For example, higher premiums do not necessarily mean higher risk exposure but maybe indicate higher risk loadings when calculating premiums. Moreover, premiums contain a loading for the administration costs. As the uncertainty in costs is different to the variation in claim payments, it is questionable whether treating both similarly is questionable.

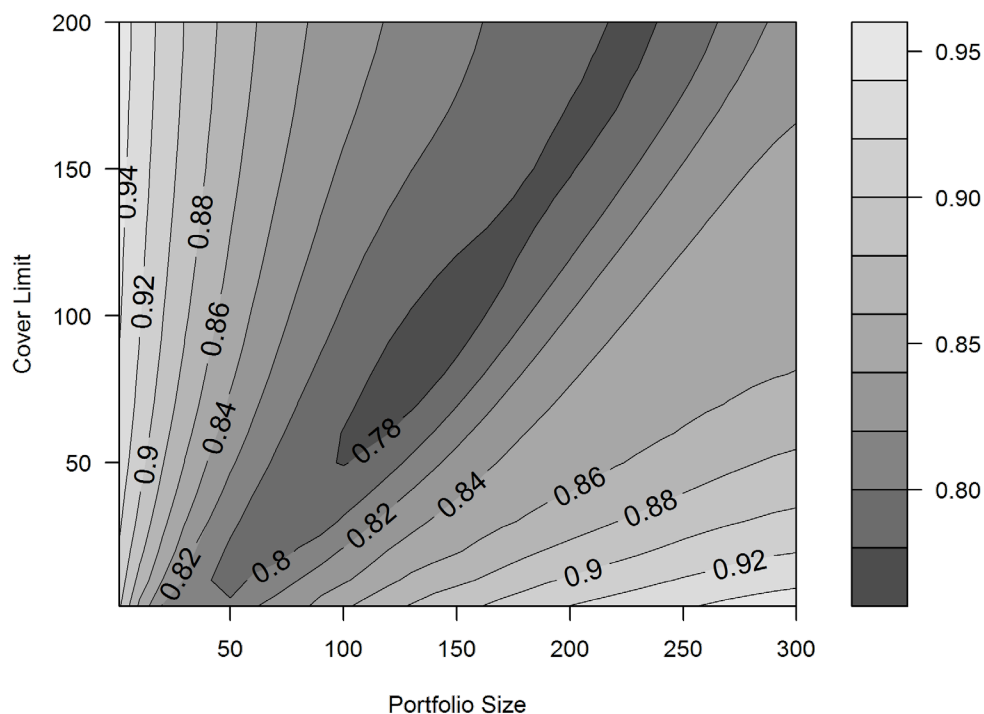
Appendix H. Different frequency parameter

In order to validate the assumption in the main text about the expected frequency, we identify all cyber losses caused companies in the S&P 500 index between 2000 and 2010. Then estimate the frequency of 2.6% as the number of cyber losses 130 divided by the

number of companies 500 and the number of years 10. The frequency is the only parameter we change and the rest is based on the standard assumptions as in the main text. For the operational risk this would mean we set $P(Z > 0) = 2.6\%$ in Equation (17) and thus the unconditional frequency would be $0.0341 \cdot 0.026 = 0.08\%$. This means that the regulatory framework would work assumable well.

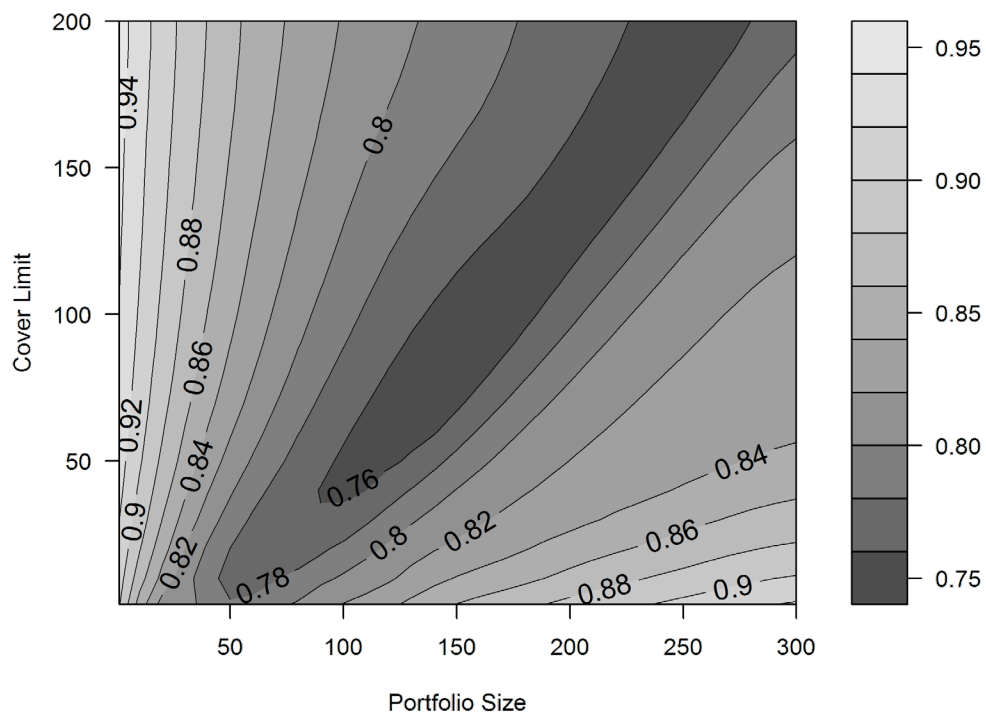
The situation for the underwriting cyber risk looks quite different. As the contour plots below show, a lower frequency actually increases default probability. This might be explained by the convexity of the probability distribution.

Figure H1. SII survival probability contour (frequency 2.6%)



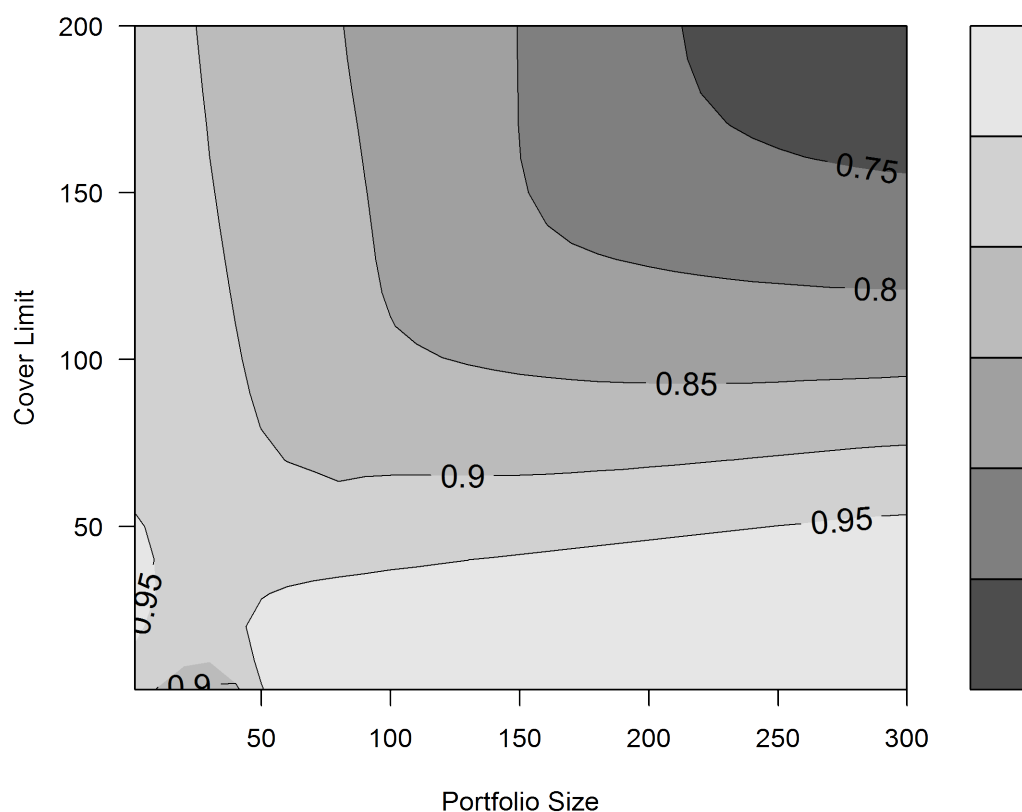
Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Figure H2. RBC survival probability contour (frequency 2.6%)



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Figure H3. SST survival probability contour (frequency 2.6%)



Note: The contours and gray shades mark combinations of portfolio sizes and cover limits (in million US\$) with the same survival probabilities. The survival probability is the probability that the loss based on our model (Poisson for frequency and empirical distribution for severity) is smaller than the capital required by the regulator.

Essay III

Is cyber risk insurable?

Martin Eling & Werner Schnell

Abstract

We use data on cyber losses and model the potential market equilibrium for cyber insurance to document a market failure when portfolios of cyber risk are constructed. This can be explained by the distinct properties of cyber risk, namely heavy tails, strong (tail) dependencies, high costs due to asymmetric information, and modelling risk. Our results help to explain why many insurance companies are reluctant to offer cyber insurance on a broad scale. We also discuss ways to overcome the market failure. Our analyses expand results from catastrophic insurance and have implications for corporate risk management and public policy.

Keywords

Cyber risk, market failure, insurability, extreme value theory, loss distribution approach, risk management, insurance economics

Status

This paper was presented at *2017 European Group of Risk & Insurance Economists (EGRIE) conference*, *2018 American Risk and Insurance Association (ARIA) conference*, *2018 German Insurance Science Association (DVFVW) conference*, *2018 PiF Seminar*, University of St.Gallen, and *2020 World Risk and Insurance Economics Congress (WRIEC)*.

Acknowledgements

We thank Martin Boyer, Dick Butler, Annette Hoffman, Madhusudan Acharyya, Randy Dumm, and Florian Klein for helpful comments and suggestions. Furthermore, we appreciate valuable comments by the participants of the *2018 ARIA conference*, the *2017 EGRIE conference*, the *2018 DVFVW* and the *2020 (WRIE) conference*.

1 Introduction

The transition of society to a global knowledge-based economy, the increasing dependency on the IT sector and the integration of digital technologies into almost any sphere of life expose individuals and organizations to cyber risks. One example of the potential drastic consequences was when the 2017 WannaCry ransomware crippled health care institutions and many other organizations around the world leading to economic losses estimated at US\$8 billion (Parenty & Domet, 2019). The overall economic costs of cybercrime alone are estimated to be at least US\$600 billion per year (Lewis, 2018 p. 4) with significant uncertainty regarding both frequency and severity of such events (Dreyer et al., 2018). Cyber risk is regularly reported as one of the top risks globally for companies according to manager surveys (Centre for the Study of Financial Innovation, 2019; World Economic Forum, 2020). Despite the remarkable importance, costs and uncertainty around cyber incidents, the cyber insurance market is lacking far behind expectations (Swiss Re, 2017), with the majority of companies having no insurance at all (Spiceworks, 2019; Statista, 2019). According to industry reports, the cyber insurance available does not address the needs of clients (Marsh-Microsoft, 2018) and coverage is extremely restricted (the large majority of insured firms have a cover limit below US\$5 million, Spiceworks, 2019). This paper provides an explanation for why the cyber insurance market lacks behind expectations.

To investigate why the market for cyber insurance is underdeveloped, we model demand and supply for cyber risk insurance and compare fair prices from the insurer's perspective with the willingness to pay of the potential client. We calibrate our model with actual cyber loss data and document a market failure in the current market environment. Our model shows that the specific properties of cyber risk can explain the underdevelopment of the cyber insurance market. Cyber risks are characterized by heavy tail marginal distributions (see, e.g., Edwards et al., 2016; Maillart & Sornette, 2010) and (tail) dependence (see, e.g., Herath & Herath, 2011).¹ While for traditional expected utility optimization, risk always decreases and utility increases as a portfolio gets more diversified (if

¹ While the heavy tails of cyber risks are well documented in the empirical literature, there is only little empirical research on the dependence structure. Many experts claim that certain cyber risks are dependent, e.g. because companies are using the same software or because some attacks spread like viruses.

the risks are not perfectly correlated and at least elliptically distributed; Meyer, 1987), research on catastrophic risks has shown that in the presence of heavy tails (Ibragimov et al., 2009) and strong (tail) dependence (Ibragimov & Prokhorov, 2016) it can be optimal not to diversify at all. Even if there is a critical portfolio size where diversification becomes optimal, coordination problems might hinder the development of an insurance market.² On top of these well-known coordination problems, cyber risks are prone to asymmetric information (see, e.g., Baer & Parkinson, 2007) leading to high transaction costs. Moreover, the lack of loss experience and respective data result in parameter and model uncertainty. All these properties might lead to high insurance premiums far beyond the client's willingness to pay. We discuss potential ways for insurers and policy-makers to overcome the market failure. Among these are pooling or reinsurance to address dependence, mandatory insurance or other governmental intervention to overcome the coordination problem, improving data quality to reduce modeling uncertainty, and IT security standards to reduce information asymmetry.

To our knowledge this is the first paper to provide a complete equilibrium model for cyber insurance that based on empirical data investigates the development of the cyber insurance market. Existing papers related to our analysis model only partial aspects on the supply or demand side of cyber insurance. The focus on the supply side has been on pricing and risk management, mainly published in actuarial science journals (see, e.g., Eling & Wirfs 2019; Eling & Schnell 2019; Fahrenwaldt, Weber, & Weske 2018). The demand side literature consists of papers mainly from the information security field analyzing optimal investments in IT security and the tradeoff between IT security and cyber insurance (Aspnes et al., 2006; Bolot & Lelarge, 2009; Shetty et al., 2010).³ Related to our analysis is also the model for catastrophic risk by Ibragimov et al. (2009),

² Ibragimov et al. (2009) distinguish a global market failure where diversification is never optimal no matter how large the portfolio and a local market failure where diversification is only optimal above a critical portfolio size. In the second situation coordination problems between several insureds bundled in an insurance pool make it difficult to reach the critical portfolio size. As Ibragimov et al. (2009) point out a global market failure can be caused by heavy tailed risks (and strong tail dependency); combined with limited liability a local market failure might be observed.

³ Böhme and Schwartz (2010) and Marotta et al. (2017) provide literature reviews on both the supply and demand of cyber insurance. The only highly published paper in finance is Kamiya et al. (2020), who develop and test a model for the impact of cyber-attacks on target firms.

which we adapt and extend to account for cyber risk specific characteristics. For example, while catastrophic risk can geographically be diversified, cyber risk cannot and the spreading behavior of cyber risk is very different (see, e.g., Fahrenwaldt et al., 2018). Thus, we put more scrutiny in developing a realistic dependence model. Additionally our model extends Ibragimov et al. (2009) by explicitly considering asymmetric information, model risk, cover limits, and endogenous premiums, other characteristics that distinguish cyber from catastrophic risk. Ibragimov et al. (2009) focus on the supply side and assume that the premium is exogenously given. However, they point out that a natural extension would be to allow the premium to be determined endogenously by demand and supply. These extensions not only provide us with more specific and reliable results but also enrich the conclusions we can derive.

The remainder of the paper is organized as follows. First, in the Section “Methodology” we derive a model for the cyber insurance market. Then, the Section “Data and Parameter Choice” presents the data and parameters used to calibrate our model, followed by the Section “Results” with the findings and robustness tests. Finally, we conclude by summarizing the results and providing recommendations for how governments and insurers might address the failure of cyber insurance markets.

2 Methodology

To derive an equilibrium of the cyber insurance market, we first model the risk exposure of insurers and clients. We then evaluate both exposures by applying a utility framework and solve for the minimum premium required by the insurer (supply) to underwrite cyber risk and the maximum premium the potential client is willing to pay for insurance (demand). By comparing demand and supply, we identify whether both market sides are willing to participate and thus whether a market exists.

We adapt and extend the catastrophic risk modeling framework presented in Ibragimov et al. (2009) to model the exposure from participating in the cyber insurance market.⁴ While Ibragimov et al. (2009) focus on the supply side (with demand exogenously

⁴ Since in practice catastrophic insurance is often provided by monoline insurers (Ibragimov et al., 2018), our analysis focuses on monoline insurers that underwrite cyber risks only. It is not clear whether premiums would be lower or higher for multiline insurers. While monoline insurer have less economies of scales, adding extreme risks (heavy tailed, correlated risks) to an existing underwriting portfolio might increase the default probability on the existing business (Ibragimov et al., 2018).

given), we model both supply and demand. As in Ibragimov et al. (2009) the insurers have a predefined limited liability (ll); additionally to Ibragimov et al. (2009), and important for the cyber insurance market, is that the cyber policies have a predefined cover limit cl . The insurance market is composed of a certain number of policies n which are shared among multiple insurers s . The insurer's exposure is derived as a stochastic sum of the individual cyber policies (see, e.g., McNeil et al., 2015, p. 472). We assume that the insurer's portfolio consists of identically distributed cyber losses $Z \in [-\infty, 0)$. To account for potential (non-linear) dependence, we use a flexible copula framework that combines different marginal distributions $P_i(Z_i)$ with different dependence structures defined by some copula C . The joint distribution $P(\cdot)$ can then be written as:

$$P(Z_1, \dots, Z_n) = C(P_1(Z_1), \dots, P_n(Z_n)). \quad (1)$$

As baseline scenario we assume iid losses, so the copula simplifies to the n -fold convolution $P(Z_1, \dots, Z_n) = P_1(Z_1)^{n*}$. Additionally, we consider the Gaussian copula that assumes linear dependence (Böhme & Kataria, 2006; Mukhopadhyay et al., 2013) and the Clayton copula that allows for tail dependencies (see, e.g., Herath & Herath, 2011; Ibragimov & Prokhorov, 2016). Applying the cover limit $cl > 0$ to Z yields the (truncated) policy exposure $\hat{Z}$:

$$\hat{Z} = \begin{cases} -cl, & \text{if } Z < -cl \\ Z, & \text{otherwise} \end{cases} \quad (2)$$

$\hat{Z}$ represents the loss given an insured incident. For pricing we need to derive the unconditional exposure that combines this potential loss with the frequency. The loss on a single policy is then the mixture of frequency I and severity $\hat{Z}$, where I is Bernoulli distributed (1 with probability r , 0 with $1 - r$). Since the portfolio frequency is the sum of Bernoulli trials, it is binomial and (for small r and large n) approximatively Poisson distributed. Both the binomial and Poisson distribution are widely used for modeling frequency (see, e.g., Eling & Wirfs, 2019). The unconditional exposure per contract is then:

$$Y = I \cdot \hat{Z}. \quad (3)$$

These unconditional exposures per contract are aggregated in a portfolio, where we consider the case of a single insurer ($s = 1$) as well as an insurance pool ($s > 1$). Insurers face capacity restrictions and the number of risks they can sign are limited so that each

individual insurer might not reach the critical underwriting size required to benefit from diversification. Sharing risk in a pool could help to attain the required diversification. We aggregate the individual risks Y_i for different portfolio sizes and denote the pool exposure per individual insurer as $X_{n,s}$:

$$X_{n,s} = s^{-1} \sum_{i=1}^n Y_i, \quad (4)$$

where n is the total number of risks in the risk pool, $s > 0$ is the number of insurers in the pool, and $m = \frac{n}{s}$ is the number of policies per insurer. We assume limited liability ll that is the maximal amount the single insurer is able to cover before bankruptcy. The (truncated) pool exposure per individual insurer with limited liability $ll > 0$ is:

$$\hat{X}_{n,s} = \begin{cases} -ll, & \text{if } X_{n,s} < -ll \\ X_{n,s}, & \text{otherwise} \end{cases}. \quad (5)$$

The limited liability is the amount of capital available to cover losses.⁵ Following Zan-jani (2002), we define the limited liability as capital k plus premium income:

$$ll_{n,s} = k + m \cdot \pi \approx -VaR_{99.5\%}(X_{n,s}), \quad (6)$$

where π is the premium. The right-hand part follows from that insurers strive for maintaining a certain survival probability, e.g. predefined by regulators (such as $VaR_{99.5\%}$ predefined by Solvency II) or rating agencies (to get a desired rating).

To analyze whether insurer and insuree are willing to participate in the cyber insurance market, we could compare the utility before and after the transaction. Alternatively, we can ask what the premium would need to be for the agents to participate. The focus on premiums has the advantage to be easier to interpret than utility values and it allows to analyze the market equilibrium by letting the supply (the insurer's premium) and demand (the insuree's willingness to pay) interact.

We first specify how premiums from the insurer's perspective are calculated. What the insurer ultimately cares about in the decision whether to underwrite cyber insurance is the profit. To calculate the profit we use a two-period model where the premium is collected, costs accrue upfront and the losses are evaluated immediately thereafter (no time

⁵ Cover limits and limited liability are also technical requirements since with heavy tailed distributions the moments required to calculate the premium would not exist (Ibragimov et al., 2009).

value, only the losses are stochastic). The stochastic profit would then be premium income $m \cdot \pi$ minus losses $\hat{X}$ and transaction costs c (see, e.g., Zanjani, 2002):

$$m \cdot \pi + \hat{X} - c. \quad (7)$$

The transaction costs c for administration and capital expenditure depend on the number of contracts. The insurer evaluates the stochastic profit in Equation (7) by applying a pricing functional H that accounts for risk preferences and beliefs. In a competitive equilibrium the value of the profit should be zero, thus:

$$H_I^{\mathcal{P}}(m \cdot \pi + \hat{X} - c) = 0. \quad (8)$$

The interpretation of $H \in \mathbb{H}$ is that it describes the risk attitudes of the insurer. Modeling and parameter uncertainty emerge from different choices of distribution models $\mathcal{P} \in \mathbb{P}$ and their calibration. Assuming that the pricing functional is scale and translation equivariant (see, e.g. Wang et al., 1997), we can solve for the competitive premium per policy:

$$\pi^*_{n,s} = H_I^{\mathcal{P}}(P_I) = \frac{c - H_I^{\mathcal{P}}(\hat{X}_{n,s})}{m}. \quad (9)$$

In a competitive market the premium is thus determined by the marginal costs of an additional insurance policy. As $\hat{X}$ also considers limited liability the equation accounts for a potential default. The transaction costs c are decomposed into administration costs $c_a \cdot \pi \cdot m$ and friction capital costs $c_k \cdot k$. The administration costs are defined recursively as a loading (with the cost ratio c_a) on the gross premium. We used this definition since data on cost ratios are easily observable and argue that c_a contains an additional loading compared to other insurance risks due to the pronounced asymmetric information that the insurer needs to mitigate by high monitoring efforts. This approach of internalizing asymmetric information in the premium calculation has been used in other settings before (see, e.g., Jean-Baptiste & Santomero, 2000; Subramanian & Wang, 2018). The friction capital costs⁶ are defined as the cost of capital rate c_k times the capital k necessary to obtain a certain solvency level or a desired target rating. Inserting the

⁶ We differentiate between a risk and a frictional capital cost component. While the risk component is already reflected in the risk premium (via the utility function) an additional allowance for taxes and frictional costs is necessary to compensate insurance investors (see, e.g., Ibragimov et al., 2018;

cost function into Equation (9) and combining it with Equation (6) yields:

$$\pi^*_{n,s} = \frac{c_k \cdot ll_{n,s} - H_I^P(\hat{X}_{n,s})}{m(1 - c_a + c_k)}. \quad (10)$$

The administration costs per policy depend on the number of insured risks. The literature does not suggest any specific shape for the cost function of cyber risk. However, for non-life insurance most empirical studies assume a translog function (see, e.g., Bikker & van Leuvensteijn, 2008), which can be written as (see Appendices for derivation):

$$c_a(m) = c_{a,1} \cdot m^\beta. \quad (11)$$

This cost function starts with $c_{a,1}$ for one risk. For $\beta < 0$ it is then monotonically decreasing ($c'_a(m) < 0$) and convex ($c''_a(m) > 0$), describing the frequently assumed and empirically confirmed (see, e.g., Huberman et al., 1983) economies of scales and diminishing returns respectively.

We now compare the competitive premium (Equation 10) with the client's willingness to pay. The insuree evaluates her payoff from the insurance contract and considers also the possibility of default of the insurer. The insurance contract's payoff from the client's perspective is then:

$$P_c = -\left(Y + \frac{D}{m}\right), \quad (12)$$

where $\frac{D}{m}$ is the amount per policy not paid in case of a default. The default option is defined as:

$$D_{n,s} = \begin{cases} -ll, & \text{if } X_{n,s} > -ll \\ X_{n,s}, & \text{otherwise} \end{cases}, \quad (13)$$

with $ll > 0$. The insuree's willingness to pay can be measured by a price functional applied on the insuree's position. Both the portfolio size and the pool structure are private information of the insurers. The insuree, however, knows the range of viable portfolio and pool structures and can infer the default probability based on the public knowledge that the insurer needs to comply with the regulatory capital requirements. Thus, the insuree can calculate $H_c^P(D|n,s)$. But the asymmetric information forces the insuree to evaluate the default option in ignorance of the realized portfolio and pool structures,

$H_c^{\mathcal{P}}(D)$ (independent of n and s). This essentially means the default option is evaluated as an average over all possible portfolio and pool structures. Due to scale equivariance and comonotonic additivity (Wang et al., 1997), we obtain the willingness to pay for one policy:

$$\pi^{WTP}_{n,s} = H_c^{\mathcal{P}}(P_c) = -H_c^{\mathcal{P}}(Y) - \frac{H_c^{\mathcal{P}}(D)}{m}. \quad (14)$$

In order to conclude whether there is a market, we compare π^{WTP} with π^* and calculate:

$$R^{\pi}_{n,s} = \frac{\pi^{WTP}_{n,s}}{\pi^*_{n,s}}. \quad (15)$$

If the premium ratio is $R^{\pi} > 1$, the client's willingness to pay exceeds the competitive premium and participating in the cyber insurance market would be Pareto optimal. In this case the premium can be anywhere in the interval $\{\pi^*, \pi^{WTP}\}$ depending on the market structure and price elasticities.⁷ The premium ratio is determined by differences between insurers and their clients risk aversions, i.e. H_I vs. H_c , the distribution assumptions, i.e. $\mathcal{P}_I$ vs. $\mathcal{P}_c$, the diversification effects on P_I vs. P_c , and the costs c . Diversification affects premiums and willingness to pay differently as shown in Equation (10) and (14). While the insuree also cares about how diversification influences the distribution far out in the tail (i.e. $\hat{X} > ll$), the insurer is concerned about how diversification affects the more "moderate tail" (i.e. $\hat{X} < ll$). The diversification of the insurer does not reduce client's opportunistic risk exposure without insurance (Y), but affects the perceived quality of the insurance product itself (via D). The insurer in turn is only concerned about how diversification affects its exposure below the limited liability (ll). In conclusion, how premiums and willingness to pay relate to each other depends on how diversification affects the outer tail relative to the moderate tale of the portfolio distribution.

We use the expected utility approach to calculate the premium that make both the insurer and insuree at least as well off as not participating in the market, that is the certainty

⁷ Equations (10) and (14) set an upper and lower limit for the premium; a premium outside of this range would not be compatible with supply and demand and there would be no market. If the market deviates from the competitive structure (e.g. oligopoly, monopoly), the insurer would choose prices $\pi' > \pi^*$, which would just change the allocation of the rent between clients and insurers, but not our results.

equivalent⁸. We first do this to get an estimate of the premium consumers are willing to pay and second to evaluate the competitive price from the insurer's perspective. For the insuree and insurer respectively $i \in \{C, I\}$, we obtain:

$$H_i(P_i) = u_i^{-1} \left(-E^{\mathcal{P}} (u_i(P_i)) \right) = u_i^{-1} \left(- \int u_i(p_i) d(\mathcal{P}) \right), \quad (16)$$

where the expectation of the utility u_i is taken with respect to the objective probability $\mathcal{P}(P)$. Recall that $\mathcal{P}(P)$ is derived by applying Equation (1 to 14) to the distribution of each risk in the portfolio. $\mathcal{P}(Z)$ in turn is estimated based on data. Note that the beliefs about $\mathcal{P}(Z)$ potentially differ between agents and modeling and parameter uncertainty is about finding the "correct" $\mathcal{P}$. We thus use different $\mathcal{P}(Z)$ as a robustness check to quantify the modeling uncertainty.

We consider the exponential function for u_i , which has often been used to model decisions in an insurance context (see, e.g., Freifelder, 1979; Golubin, 2016) and it is better suited for heavy tailed risks than other utility function like for example the power utility (Ikefuji et al., 2020); from a technical perspective, the certainty equivalent needs to be translation invariant so that we can solve for the premium (Equation 9). This property only holds for the exponential utility function (Reich, 1984). After inserting the exponential utility in Equation (16) and some transformations, the certainty equivalent (also called the exponential premium principle) simplifies to (Denuit et al., 2006):

$$H_i(P_i) = \begin{cases} \frac{\ln E(e^{a_i P_i})}{a_i}, & \eta_i \neq 0 \\ E(P_i), & \eta_i = 0 \end{cases}, \quad (17)$$

where a_i describes the constant risk aversion (CARA) for the insurer and insuree. We use a concave utility function that describes risk averse agents, $a_i \in (0, \infty)$ (Ibragimov

⁸ There are several alternative approaches for premium calculations. One is the actuarial premium principle which is based on some moments of the loss distribution plus a loading. This approach is supply orientated and assumes that premiums can be set monopolistically (see, e.g., Zweifel & Eisen, 2012, p. 221). Another alternative is the financial approach based on the idea that premiums must obey the principle of non-arbitrage and individuals' risk attitudes are not relevant. However, arbitrage free pricing is not available for insurance risks since they are not traded, their stochastic nature feature jumps and are thus difficult to hedge (Denuit et al., 2006). Thus, our pricing relies on the agent's risk preferences (Denuit et al., 2006) as described by the risk aversion within the classical expected utility framework.

et al., 2009).⁹ In order to generalize and confirm the robustness of our results, we also evaluate the cyber risk exposure with the risk neutral approach and isoelastic utility function (see Appendices). Since there are generally no closed-form expressions for Equation (17) available, we use Monte Carlo simulations to evaluate the portfolio distribution.

3 Data and parameter choice

To calibrate our model, we use two datasets. In the main results presented in the paper cyber incidents are extracted from the SAS OpRisk database which contains 1'579 cyber incidents between 1995 and 2014, with a wide range of different cyber incidents including man-made, technical failure, and external events (e.g. virus, hacking, and denial-of-service attack). For a detailed description of the dataset we refer to Eling and Wirfs (2019). As robustness test, we also analyze a frequently used dataset of data breaches provided by the Privacy Rights Clearinghouse (Kamiya et al., 2020; Maillart & Sornette, 2010; PRC 2019) which is more homogenous, but has the disadvantage that only the number of breach data are reported instead of dollar loss values. The results for the alternative dataset are comparable to the main dataset (see Appendices).

To determine appropriate distribution models for each cyber policy $\mathcal{P}(Z)$, we fit several parametric distribution models frequently used to model insurance losses to the dataset and compare the goodness of fit (see Appendices). Extending Eling and Wirfs (2019), we find that besides the peak over threshold (POT) model (which combines a lognormal body and a generalized Pareto tail), the stable, Levy, and the generalized beta distribution of the second kind (GPB2) fit the data best. In the following we use the Levy distribution as base line model since it is closed under portfolio formation and with two parameters is the most parsimonious one. This reduces the risk of overfitting and we can easily vary parameters to conduct sensitivity analyses. Considering the other distributions yields the same general conclusions as those presented in the main body of the text

⁹ Risk aversion at the firm level can be motivated both theoretically and empirically. In the presence of frictions, such as taxes, costly external financing, principle-agent problems, and financial distress costs, it can be shown that even a risk neutral company might act as if it were risk averse (Berk et al., 2010; Bickel, 2006; Gollier et al., 1997). For insurance, Zanjani (2002) shows that if the clients care about the product quality (default risk) insurers are incentivized to reduce risk and thus behave risk averse. As shown in the supplemental material, our results are not sensitive to risk preferences.

(see Appendices).

To provide a realistic description of the cyber insurance market, we calibrate our model using secondary literature (see Table 1). All parameters are varied in sensitivity tests to show the robustness of the results with respect to the modelling assumptions. For the different distribution models, we estimate Pareto indices α in the range of 0.44 for the stable and 0.69 for the POT (see Appendices). This result confirms that cyber risks are indeed extremely heavy tailed ($\alpha < 1$).¹⁰ To explore the boundaries of insurability, the cover limit is set to the upper limit observed in the market today (US\$100 million; Swiss Re, 2017), while the majority of cyber insurance policies today have a cover limit of not more than US\$5 million (Spiceworks, 2019). For the frequency of cyber losses r , we follow Eling and Schnell (2019) and consider the subsample of companies listed in the S&P 500. Using our dataset, Eling and Schnell (2019) estimate a yearly cyber loss frequency between 2.6% and 7.4% for the S&P 500 companies, so we take the average value of 5%.

Table 1. Parameter choice

Parameter	Notation	Value	Source
Pareto index [Stable, POT]	α	[0.44, 0.69]	Estimated based on the data
Cover limit	cl	US\$100 million	Swiss Re (2017)
Loss frequency	r	5%	Estimated (Eling & Schnell, 2019)
Correlation	ρ	0.18	Böhme & Kataria (2006)
Survival probability	q	99.5%	Solvency II (EC, 2015)
Administration costs	$c_{a,1}, \beta$	0.47, -0.07	Bikker & Gorter (2011)
Frictional capital costs	c_k	2%	Swiss Re (2005)
Risk aversion	a_C, a_I	0.02, 0.02	Geruso (2017)

Estimating the dependencies is difficult because there is only little empirical evidence

¹⁰ Ibragimov et al. (2009, p. 980) use in their earthquake application a Pareto distribution and find a local market failure if the Pareto index α is between 0.76 and 1.46 and a global market failure if $\alpha < 0.76$. In the supplement we also analyze the stability of α and find that the extreme heavy tailedness is a stable trait of cyber risks.

that investigates the dependence between cyber losses. For this reason, different dependency structures will be considered. We use a correlation of 0.18 between cyber losses Z_i and for the nonlinear copula (Clayton) an equivalent calibration.¹¹ For the capital requirements we choose the value at risk Var_q with a survival probability of $q = 99.5\%$ as required by Solvency II (EC, 2015). Note that the effect diversification has on the Var_q depends also on q . For extreme heavy tailed and tail dependent risks, larger q reduce the benefit from diversification with respect to Var_q (see, e.g., Embrechts, Nešlehová, & Wüthrich 2009).

The administration cost function is calibrated according to Bikker and Gorter (2011)'s result for the Dutch non-life insurers. We transform their estimated parameters for the translog regression model, $\ln(c_a) = b + \beta_{TC} \cdot \ln(m)$, according to $c_{a,1} = e^b$ and $\beta = (\beta_{TC} - 1)$.¹² We use an estimate for the frictional capital costs of 2%. The rest of the capital costs are already considered by the risk premium based on risk averse utility. We also compare different cost functions in the Appendices.

The literature is ambiguous on the viable range for the risk aversion, especially for the case of firms considered here, be it either the insurer a_I or their corporate clients a_C . Risk aversion for firms might be smaller than the one for individuals because the shareholders' exposure is limited and they can hold the firm's stock in diversified portfolios. As Equation (15) illustrates we are not only interested in risk aversion as such, but in the ratio of insurer's to client's risk aversion. The difference between the two agents is that insurers additionally need to comply with insurance regulations and the quality of the insurer's product depends on the risk taking (Zanjani, 2002).¹³ This might make the

¹¹ Böhme and Kataria (2006) derive this correlation estimate between firms based on attack data registered by firewalls, but they do not consider loss data.

¹² The later transformation is required since the authors use total costs instead of the cost ratios used here. This function converges towards cost ratios observed in mature markets as the number of risks m increases (e.g. $c_a(10^2) = 0.34$, $(10^3) = 0.29$). Data on the property and casualty industry suggests for mature markets an expense ratio of 28% on average for the US (NAIC, 2017), 30% for Canada (1990-2017; Statista, 2018), and 27% globally (2016; OECD, 2017). A peculiar aspect of cyber insurance is the substantial information asymmetry (Biener et al., 2015) leading to additional costs associated with screening, monitoring, as well as modeling and parameter uncertainty relative to other line of insurance businesses.

¹³ Fines and other regulatory consequence for excess risk taking should make insurers more risk averse especially towards tail events than other firms. Using a higher risk aversion parameter for the total

insurers more risk averse. However, given the lack of empirical evidence on differences in risk aversion, in the main part we assume that insurers have the same degree of risk aversion as their clients ($a_c = a_I = 0.02$; we choose a value in the range of the numbers reported in Geruso, 2017), while in sensitivity tests we also vary these parameters to show the impact of alternative calibrations (see Appendices).

4 Results

We first discuss the client's willingness to pay (Equation 14) and the competitive premium (Equation 10) for iid Levy distributed risks. Figure (1a) shows the result for a single insurer's portfolio with 1 to 200 risks.¹⁴ The price, the insurer charges, starts off much higher than what the potential clients are willing to pay. This is especially due to the necessary cost loading (see Figure 1b).

Because of the distribution and cost structure the premium then first increases before it decreases as the portfolio size increases. This result mirrors the U-shaped utility Ibragimov et al. (2009) document in their analysis. Since the willingness to pay is never above the premium, a market does not exist.¹⁵ Due to the additivity of the expectation the expected loss stays the same for all portfolio sizes. The risk premium is the additional loading required because of the insurer's risk aversion. As the portfolio increases diversification reduces risk and consequently also the risk premium. This is also true for the value at risk (VaR) as a specific risk measure, so that the capital costs (cost of capital rate times the necessary capital based on the VaR) decrease as the portfolio size increases.

distribution can thus be seen as an approximation for higher tail risk aversion.

¹⁴ The cybersecurity insurance coverage supplement (NAIC, 2019) shows that the median portfolio size for standalone cyber policies for US insurers is around 50 (with an increase from 52 in 2015 to 57 in 2017). We are grateful to Xiaoying Xie for providing us with the data.

¹⁵ The kink observed with $n=30$ is because the loss distribution is bounded at the cover limit. For a portfolio size above 580 risks the premium ratio exceeds one (see supplemental material) which is very far from the median portfolio size observed in the cyber insurance market today.

Figure 1a. Premium versus WTP

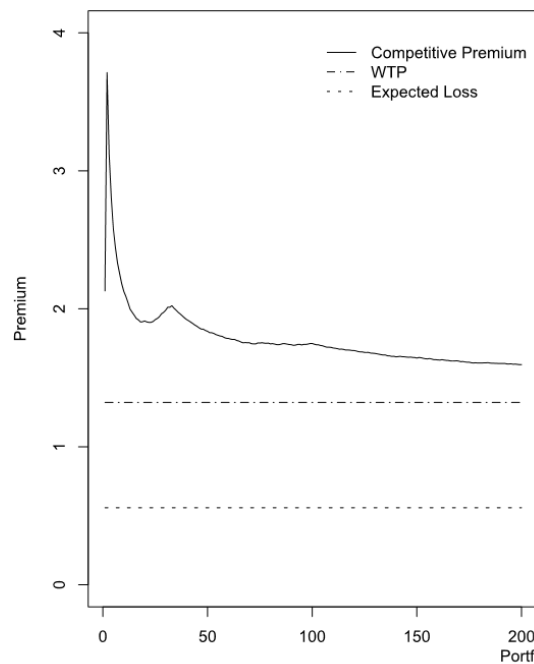
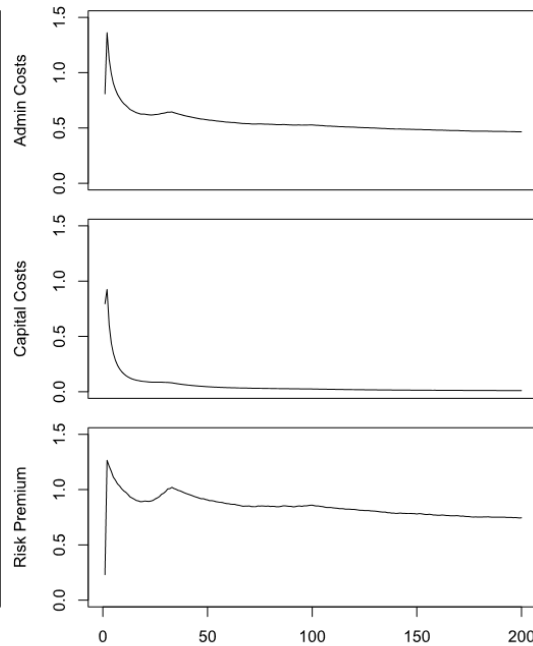


Figure 1b. Premium components

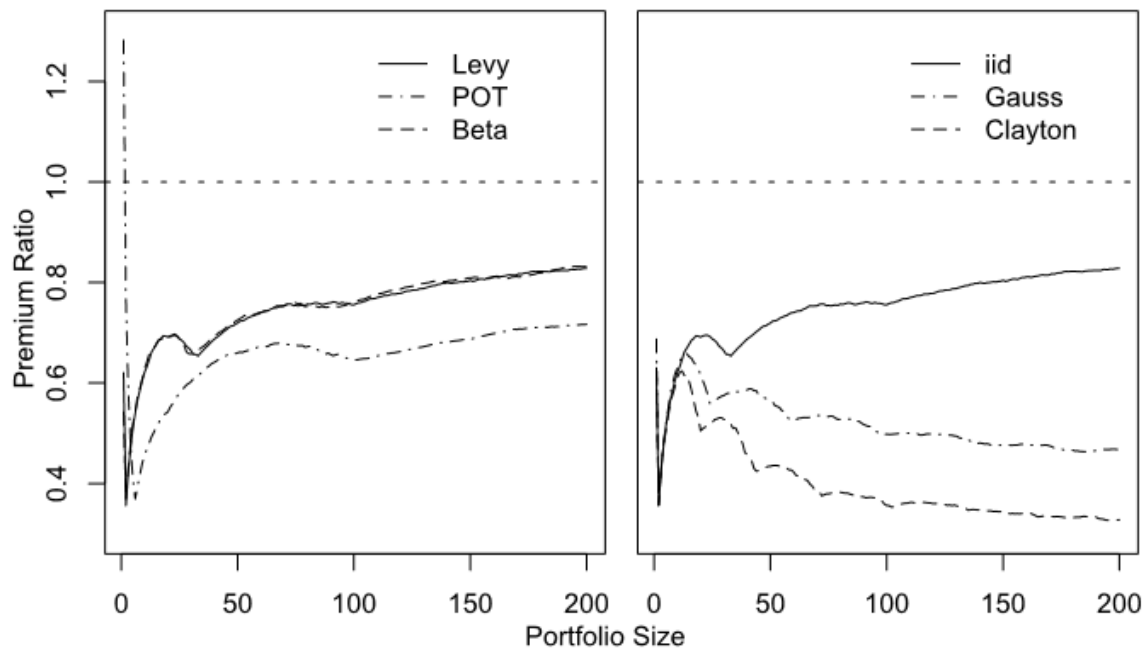


Note: The left side compares the competitive premium and the client's willingness to pay (in million US\$) per policy for iid Levy distributed risks as a function of portfolio size. The right side shows the decomposition of the competitive premium into costs components, where the expected loss must be added to obtain the competitive premium.

Figure 2 shows the premium ratio as defined in Equation (15) for different distributions (left) and dependency assumptions (right, using the Levy as underlying distribution again). Irrespective of the distribution and dependency assumptions a global market failure arises when portfolios of up to 200 policies are considered. Insurability is thus never given, i.e. the premium ratio is always smaller than 1. While the results for the Levy and generalized beta distribution are very similar, the POT approach even leads to a slightly lower premium ratios.¹⁶ The result are relatively similar for different distributions since the cover limit reduces the effect the tail has on our result. Positive dependence between risks and tail dependence as modeled by the Clayton copula further reduce the benefits from diversification. As a result, the gap between the willingness to pay and premium increases. The results indicate that for the parameters considered here strong dependence there is a global market failure, meaning that the market failure cannot be resolved no matter how many risks are pooled.

¹⁶ Results for other distributions (stable, GPD, lognormal) are very similar (see Appendices).

Figure 2. Premium ratio for single insurer

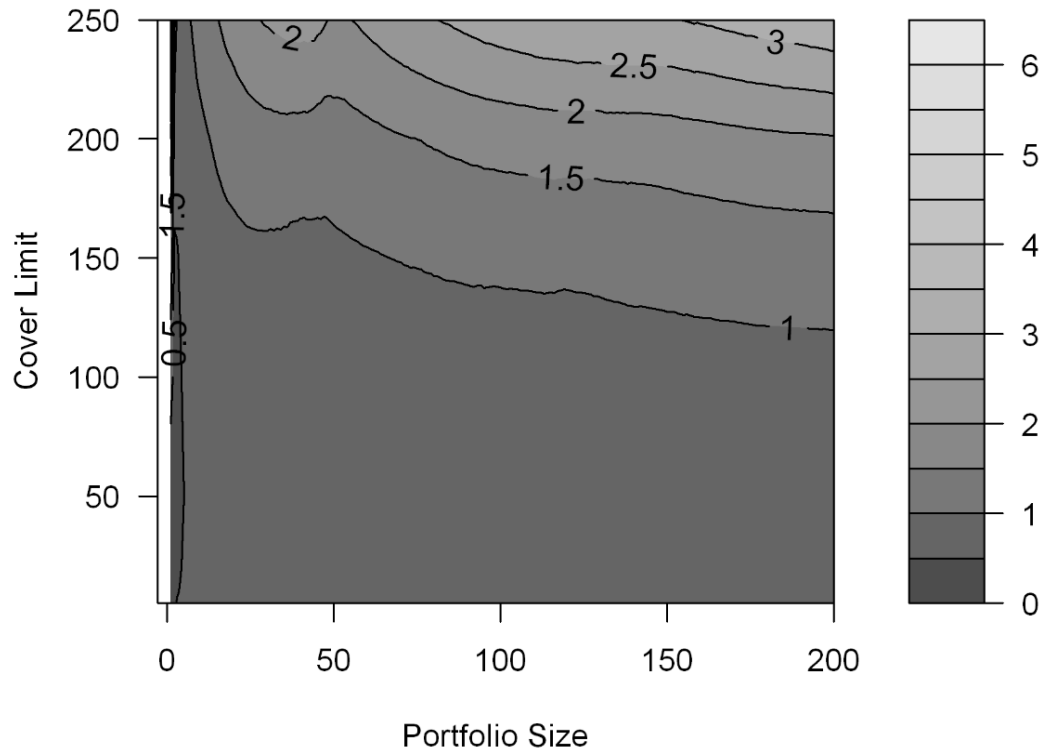


Note: The figure shows the premium ratio for different distribution and dependence assumptions. The figure on the left illustrates the results for iid Levy, Peak Over Threshold (POT) and generalized beta (Beta) distributed risks and the one on the right presents the result for dependent Levy risk (Gauss, Clayton). A premium ratio below one indicates that no market exists.

The only free parameter that the insurer can set in our model is the cover limit. In Figure 3 we let the cover limit vary for different portfolio sizes. Generally, higher cover limits and larger portfolio size can turn the global market failure into a local one (premium ratio above 1). For example, if the cover limit is larger than US\$150 million and the portfolio contains more than 70 policies a market would exist. As the cover limit increases both the willingness to pay and competitive premium increase. The clients' willingness to pay increases since the contract covers potentially higher losses. Similarly, with higher cover limits the insurer expects higher indemnities and thus charges higher prices. However, the willingness to pay and the competitive premium are affected by the cover limit differently. Since the insurer keeps the policies in a portfolio, higher cover limits are less expensive for the insurer than for the client (above the critical portfolio size where diversification works again). By setting the cover limit too low the insurer restricts the scope of service the insuree is willing to pay for. One potential recommendation might thus be that insurers should set cover limits higher. Industry reports confirm that clients indeed started to demand higher cover limits (PartnerRe, 2018). Insurers that reacted by increasing the cover limits might explain the current growth observed in the

cyber insurance market (A.M. Best, 2019).¹⁷

Figure 3. Premium ratio for different cover limits



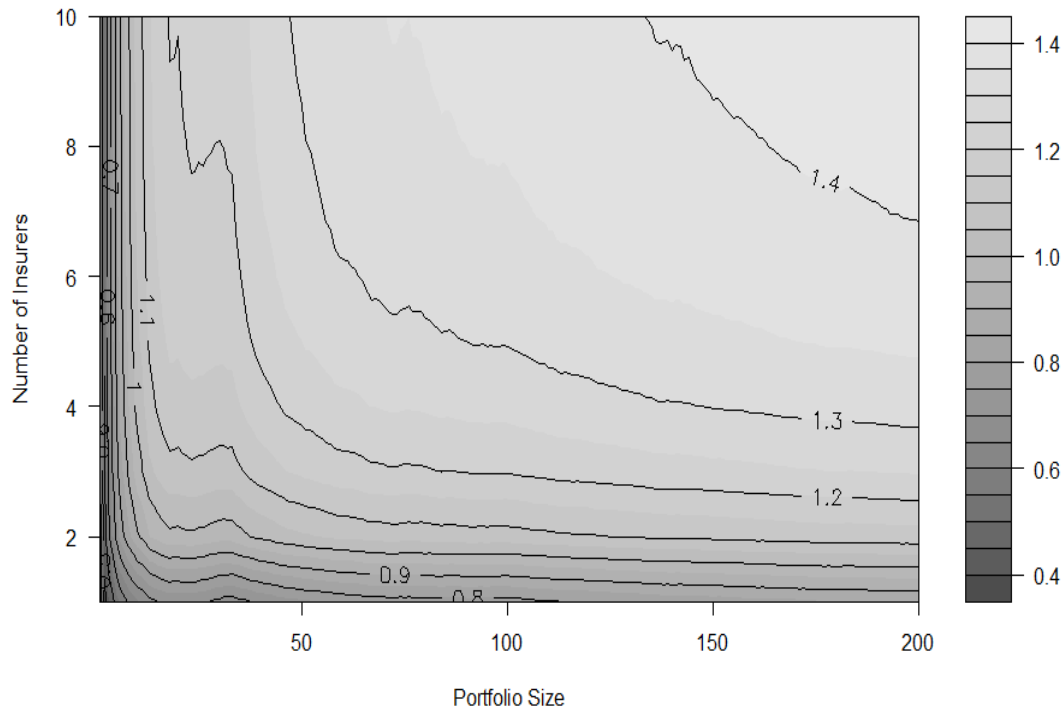
Note: The figure shows the premium ratio contours for the iid Levy model when the cover limit (cl; in million US\$) is varied. A premium ratio below one indicates that no market exists.

We also analyze whether the pooling of cyber policies across several insurers improves insurability. Two main types of risk pool have been discussed and are observed in practice. The main distinction is whether the insurers are jointly liable for the pool losses or not (see, e.g., Reichel & Schmeiser, 2018). If they are jointly liable the solvent insurers would also need to cover any insolvent insurer's share of the pool. Here we use the model of each insurer is only liable for its own share of the pool (Ibragimov et al., 2009). Premium and losses are shared equally between the insurers. This also means that each insurer needs to hold capital and incurs capital and administration costs according to its share of the pool. This pooling regime is very similar to a quota share reinsurance contract, where several insurers share their risk capacity.

¹⁷ We note however that the large majority of insured firms have a cover limit below US\$5 million (Spiceworks, 2019). For a cover limit of US\$5 million, a premium ratio of 1 is never reached, emphasizing again the limitations of today's cyber insurance market (see Appendices).

In Figure 4 we show the premium ratio for the case of several insurers that share their risks in an insurance pool.

Figure 4. Premium ratio for insurance pools



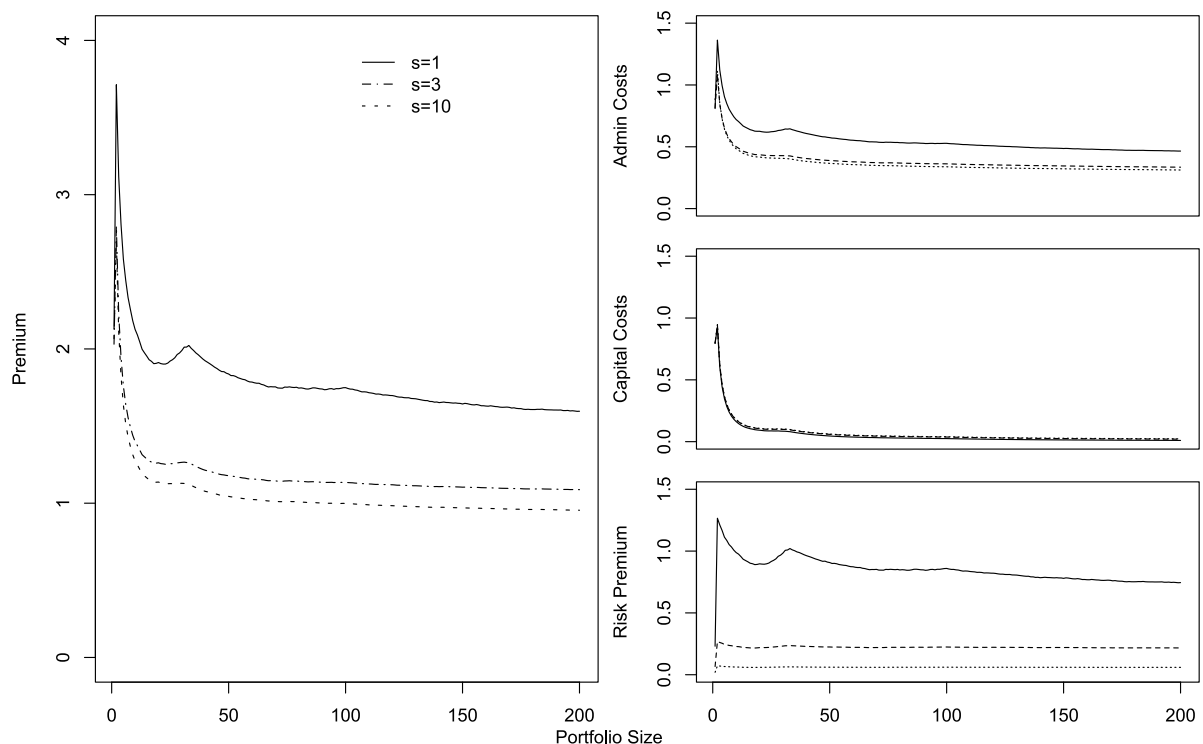
Note: The figure shows the premium ratio contours for different number of insurers s in the pool for iid Levy distributed risks. A premium ratio below one indicates that no market exists.

Pooling again turns the global to a local market failure. For example, for 3 (10) insurers in the pool the critical size where a market would develop is already reached with 11 (8) policies. As shown in Figure 5, this can be explained by lower risk premium and lower administration costs. If we consider the negative of the premium (certainty equivalent) as a special case of a utility function than the risk premium (left figure) can be compared with the findings of Ibragimov et al. (2009). For a fixed number of policies n the risk premium (utility) decreases (increases) $H\left(\frac{x}{s}\right)/m$. This is because as number of insurers in the pool s increases, the losses are scaled according to X/s . Thus, the distribution is less heavy tailed, the variance decreases and the risk premium decreases as well for a risk averse insurer.

Since the administration costs are defined relative to the premium, they accentuate the reduction in the risk premium (see top right figure). This effect is not compensated by the reduction in capital requirement capital cost (see middle right figure) due to addi-

tional diversification stemming from pooling. Our analysis also shows that if the administration and management tasks would be organized at the pool level, the pooling would be even more beneficial due to economies of scales. Diversification would also be beneficial if the administration costs would feature less cost depression. While these arguments would certainly increase the benefits of pooling, they do not necessarily lower the competitive premium enough for a market equilibrium ($WTP < p^*$) to exist.

Figure 5. Premium composition for insurance pools



Note: The figures show the competitive premium per unit of risk and its components (administration costs, capital costs, risk premium, not shown is the expected loss) for different pool sizes s (number of insures). The losses are assumed to be iid Levy distributed.

By comparing different distribution models, we account for potential model risk, but not for the uncertainty inherent in estimating parameters. Parameter uncertainty can emerge because the data we use does not well describe the future or, due to a flawed recording process, does not even describe the past well. Moreover, the asymmetric information an insurer faces can also be understood as uncertainty in the distribution assumptions. Accounting for parameter uncertainty thus can be interpreted as an out of sample test. In principle, most of the parameters used in our models are uncertain. Since our results are sensitive to the assumption about the Pareto index α , we focus on this parameter in the

following.

One widely used way to incorporate parameter uncertainty is the Bayesian approach (see, e.g., Venter & Sahasrabudde, 2015). Instead of using a point estimate, a sampling distribution of α given the observed data is derived. For that we assume that a prior distribution is governing α . Generally, the prior is either based on subjective expert judgment or on uniformed objective arguments. Here we rely on the objective priors. Several objective priors have been suggested (see, e.g., Northrop & Attalides, 2016). A prior that has been suggest due to useful properties (low-informative prior i.e. flat, diffuse, and with high variance) is:

$$f(\alpha) = \left(\frac{1}{\alpha}\right). \quad (18)$$

The prior, when updated according to the likelihood function $L(\mathbf{z}|\alpha)$ over our sample $\mathbf{z}$, is proportional to the posterior distribution $f(\alpha|\mathbf{z})$:

$$f(\alpha|\mathbf{z}) \propto L(\alpha|\mathbf{z}) \cdot f(\alpha), \quad (19)$$

where the likelihood function is the Pareto density. Venter and Sahasrabudde (2015) show that under these assumptions the posterior follows a gamma distribution¹⁸ with shape parameter n (sample size) and mean equal to the maximum likelihood estimate for α .

In order to calculate the premium, we again use simulations. However, instead of continuously drawing from the same distribution, we use a two steps approach. First, the parameter α is drawn from the gamma distribution. Then the losses are drawn from the stable distribution with α from the first step. Thus, each draw is based on a different parameter. We use the stable distribution here because it allows to let the Pareto index vary (which would not be possible for the Levy since its Pareto index is fixed). We then evaluate the premium risk from two different perspectives. The first one is the variation of the premium ratio around our point estimate due to parameter uncertainty. The parameter risk can then be quantified by the mean squared error based on different α :

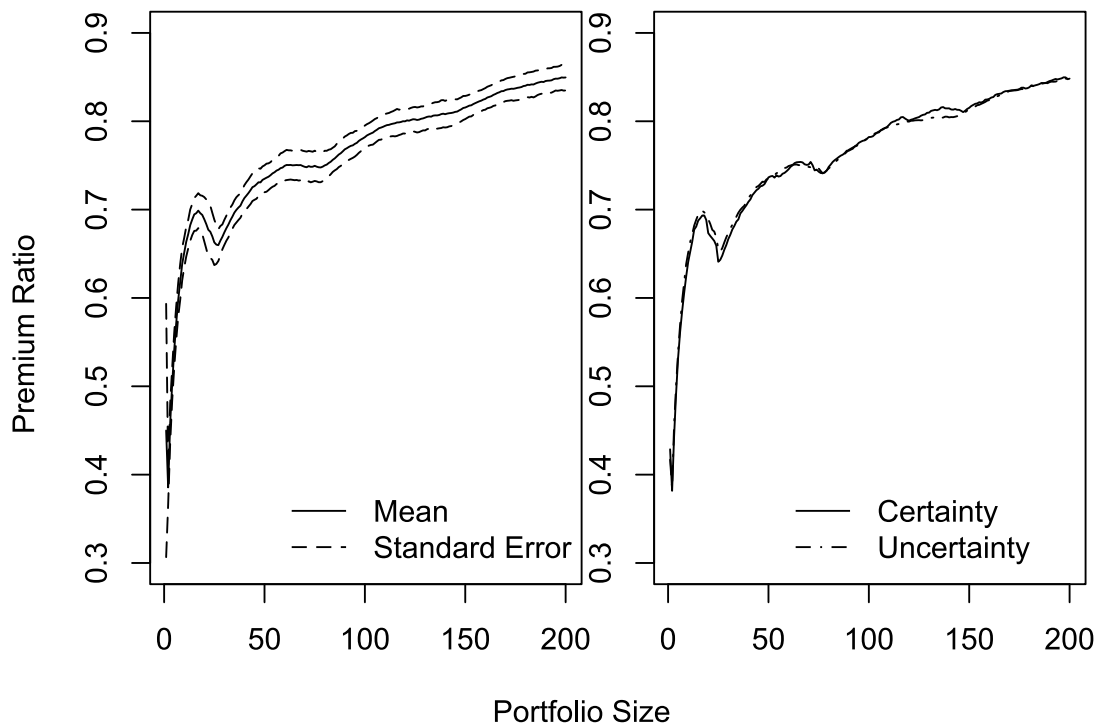
$$\widehat{MSE}_n = \sum_{\forall \alpha} (R_{\pi}^{\mathcal{P}_\alpha} - \bar{R}_{\pi})^2 P(\mathcal{P}_\alpha), \quad (20)$$

where the premium ratio is calculated as in Equation (15), $P(\cdot)$ describes the probability

¹⁸ The gamma distribution converges towards the normal distribution as the sample size increases.

of a certain α to be true, and $\bar{R}_\pi$ is the average premium ratio over different α . We attribute equal probability weights for $P(\mathcal{P}_\alpha)$. The standard error in our premium ratio is given on the left of Figure 6.

Figure 6. Parameter uncertainty with respect to the Pareto index



Note: The left figure shows the premium ratio ($\bar{R}_\pi$) with the standard error ($\sqrt{MSE}$) generated by the parameter uncertainty and the right figure reports the premium ratio if the parameter uncertainty is priced in the premium calculation. Both figures are based on the iid stable distribution.

The second perspective is how much would the premium ratio be affected if both the insurer and insuree would take uncertainty in account when calculating the premium. This would mean the premium is calculated by evaluating a mixture of the stable and parameter distribution. The result for this analysis is shown on the right of Figure 6. Generally, the effect of parameter uncertainty on the outcome is not significant. The confidence interval (left part of Figure 6) is narrow and the premium ratio that uses uncertainty in the pricing is very similar to the premium ratio without uncertainty (right part of Figure 6). This result is due to the fact that the cover limit levels the effect fluctuation in the Pareto index has on the premium calculation (risk premium, capital requirement, value of the default option, and capital costs). Thus, if the cover limit is set low enough, parameter uncertainty in α does not cause a significant problem in the cyber

insurance market.

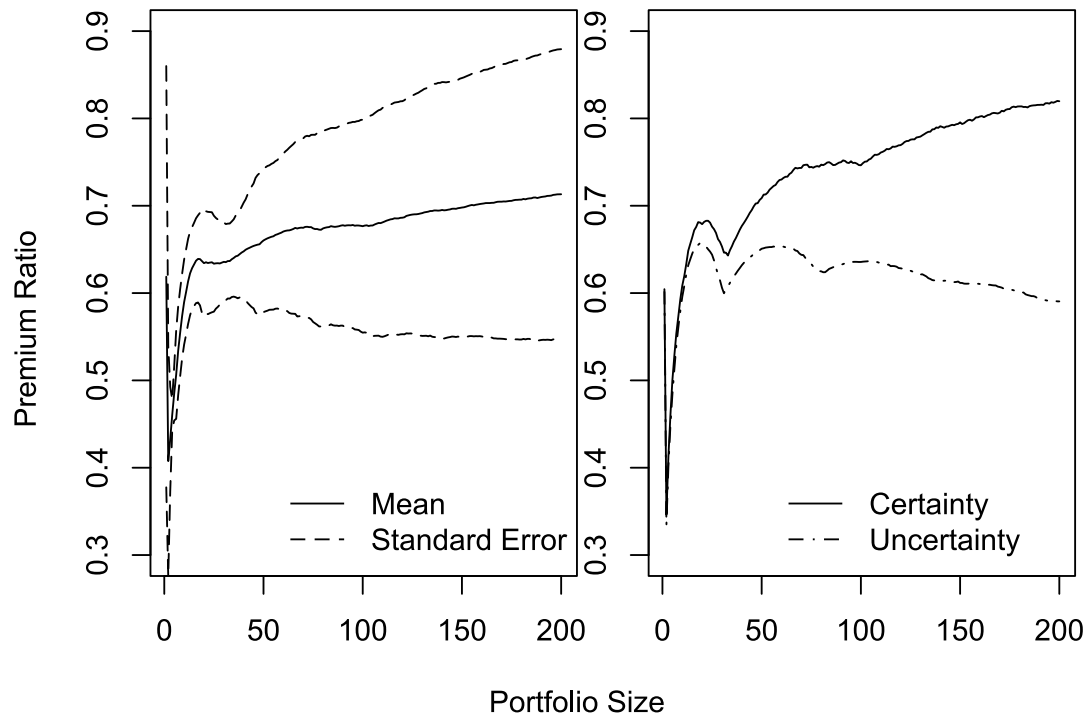
While parameter risk is mainly a problem when samples are small and loss incidents are infrequent, modeling risk is also problematic if samples are larger. We argue that modeling uncertainty is a substantial part for cyber risk, so we propose two methods to quantify modeling uncertainty in a cyber risk context. Adapting Cont (2006), we use the premium (instead of option prices) as an easy to interpret measure. Modeling risk can then be quantified by comparing the premiums calculated by different distribution models $\mathcal{P}_i \in \mathbb{P}$. The mean squared error in estimated premiums can then be defined as:

$$\widehat{MSE}_n = \sum_{i=1}^M (R_{\pi}^{\mathcal{P}_i} - \bar{R}_{\pi})^2 P(\mathcal{P}_i), \quad (21)$$

where the premium is calculated as in Equation (15), $P(\cdot)$ describes the probability of a certain model to be true, and $\bar{R}_{\pi}$ is the average premium ratio calculated by different models. $\mathbb{P}$ contains all the different distribution models we use in this paper (9 in total, namely the iid lognormal, generalized Pareto, POT, beta, Levy, stable, bootstrap, and the correlated and Clayton Levy) and attribute equal probability weights $P(\mathcal{P}_i) = \frac{1}{|\mathbb{P}|}$ to each model. This means $\widehat{MSE}$ contains the uncertainty in the marginal distributions and dependence assumptions. The premium ratio with modeling uncertainty is shown in Figure 7.

The confidence interval (left part of Figure 7) shows that the modeling uncertainty is much more significant than the results for the parameter uncertainty presented in Figure 6. However, a premium ratio of one is not crossed and we can safely conclude that a market does not exist. The right part of Figure 7 shows that the premium ratio would be substantially lower if model uncertainty is considered in the premium calculation. Model uncertainty thus increases the premium relative to the willingness to pay and further hinders the development of a market. The limits with this approach lie in choosing a set of viable distributions P . As we add more models to P , e.g. including alternative parameter specifications, the variation in admissible prices could increase. As Asimit et al. (2017) point out the choice of a visible set of models is left to expert judgment. This shows that the selection of the model is quite important and insurers need to add a substantial premium for modeling uncertainty on top of the risk premium. Modeling uncertainty therefore might also explain why the cyber insurance market fails.

Figure 7. Modeling uncertainty



Note: The left figure shows the premium ratio ($\bar{R}_\pi$) with the standard error ($\sqrt{MSE}$) generated by the modeling uncertainty and the right figure reports the premium ratio if the modeling uncertainty is considered for premium calculation.

Given the above analyzed parameter and modeling uncertainty, robustness tests were conducted to analyze the sensitivity of the results with respect to all modelling assumptions and inputs. All in general yield the same conclusions as the ones presented in the main body of the text (in the sense that a cyber insurance market does not exist) and are presented in the Appendices. We also illustrate the results for alternative risk preferences including risk neutrality and the case where the insurer is more risk averse than its clients. An alternative utility function with constant relative risk aversion instead of constant absolute risk aversion and an alternative dataset is also considered. Furthermore, alternative distributions and risk measure (tail value at risk instead of value at risk) with varying confidence levels are presented that all yield the same general conclusions as the one presented here.

5 Conclusions

We present an insurance market model and using a realistic calibration show that the characteristics of cyber risk make it difficult to establish a cyber insurance market.

Heavy tails and strong dependence hinder diversification and thus reduce the main contribution the insurance industry can provide to the economy and society. Idiosyncratic risks cannot be diversified, leading to high insurance price and consequently the market fails. Limited experience and information asymmetries with this type of risk lead to uncertainty in modeling and parameter choice that further increase the cost for insuring cyber risks relative to other established insurance risks. We show both cases where a market fails for small portfolios (local market failure), but also cases where there is no portfolio size that would be beneficial (global market failure). Our model also illustrates that there is a mismatch between the insurer's and insuree's incentive when it comes to risk taking. Due to the limited liability, the insuree cares about how diversification affects the distribution far out in the tail (i.e. $> VaR_{99.5\%}$), but the insurer is concerned about how diversification affects the "more moderate tail" (i.e. $< VaR_{99.5\%}$). This leads to diverging willingness to pay and competitive premium based on how diversification affects the outer relative to the moderate tale of the portfolio distribution. Thus, heavy tails, as observed for cyber risk, lower willingness to pay relative to the competitive premium and cause a market failure.

We show potential solutions to mitigate the market failure. Pooling could enhance diversification and lower costs sufficiently and help a market to develop. One potential policy recommendation might thus be that insurers should cooperate in pooling their risks and resources. Insures should also cooperate to enhance the available data in order to improve the cyber risk models and thus to reduce modelling and parameter uncertainties. Finally, insurers would also benefit from a reduction in asymmetric information, e.g., by implementing and enforcing minimum IT security standards. Already today cyber insurance can only be sold when sufficient IT security measures are in place and consistently used, also to avoid potential moral hazard implied by insurance coverage.

The government might foster the development of a cyber insurance market. As there is a coordination problem, the government could try to push the cyber insurance market above the critical size needed for diversification. The government could incentivize the use of risk pools or reinsurance. This might also include carrying parts of the risk like done also for other extreme risks (like e.g. terror), which can be used to increase the possible cover limits. This might be welfare enhancing, since the currently used cover limits restrict the market to small risks and do not allow to realize welfare gains from insuring larger cyber risks above the cover limit. Alternatively, some form of sovereign

guarantee might lower the probability of default and thus the value of the default option. Our analyses also show that a reduction in the capital requirements would increase the premium ratio (lower capital costs would overcompensate the higher value of the default option) and thus would benefit the market. Contrary to this argument, regulators should reconsider the usual capital discounts for diversification in case of cyber risk since diversification does not work well for cyber risks. We also note that intervention by the government will only be welfare enhancing if there is a local market failure. Our simulations show that both cases exist and that the results depend on the input parameters. It is thus not clear empirically under which cases an intervention is welfare enhancing or reducing, leading to some ambiguity with respect to potential policy recommendations.

We can relate our results to the findings and discussions in the field of catastrophic risk, also to identify potential ways to overcome the market failure. For catastrophic risk the insurability of risk is improved by pooling of risks, mandatory insurance and public private partnerships (see, e.g., Kunreuther & Michel-Kerjan, 2009). The insurance pool analyzed in this paper in some cases also helps to overcome the market failure. Mandatory insurance might overcome the failure as well because the number of risks would be large from the very beginning on. But it also represents a massive intervention in the free market, will only work if the market failure is of local nature and might bring unintended side effects if the incentives are not properly managed. For example, mandatory insurance needs to be supplemented by mandatory prevention, otherwise significant moral hazard problem might arise. The idea of public private partnerships is to have risk layers with a private deductible, an insurance layer offered by private insurers and a third insurance layer defined by the government for extreme risks. As indicated above the government layer can be interpreted as an increase in the cover limit.

Several limitations of the paper open room for future research. One obvious aspect is that the quality of data in the cyber risk domain is still limited. Although we illustrate our results for two independent datasets, future research has to analyze our results on a broader empirical basis, especially to better understand under which circumstances the market failure for cyber risk is of local or of global nature. One particular interesting element in this context is also the dynamic nature of cyber risks, which indicates that statistical properties of cyber risk might change over time.¹⁹ It is unclear whether the

¹⁹ As a first step it might be helpful to analyze the time dimension in the existing data in more detail in

market failure will become less or more extreme; more data and loss experiences might help to better understand the tails of the cyber loss distribution, but with the increasing connectivity and globalization it might also be that future extreme events will be more severe and happen more often.

6 References

- A.M. Best. (2019). *Best's market segment report*. <http://www3.ambest.com/bestweek-pdfs/sr507453119175full.pdf>
- Asimit, A. V, Bignozzi, V., Cheung, K. C., Hu, J., & Kim, E.-S. (2017). Robust and Pareto optimality of insurance contracts. *European Journal of Operational Research*, 262(2), 720–732.
- Aspnes, J., Chang, K., & Yampolskiy, A. (2006). Inoculation strategies for victims of viruses and the sum-of-squares partition problem. *Journal of Computer and System Sciences*, 72(6), 1077–1093.
- Baer, W. S., & Parkinson, A. (2007). Cyberinsurance in IT security management. *IEEE Security and Privacy*, 5(3), 50–56.
- Berk, J. B., Stanton, R., & Zechner, J. (2010). Human capital, bankruptcy, and capital structure. *Journal of Finance*, 65(3), 891–926.
- Bickel, J. E. (2006). Some determinants of corporate risk aversion. *Decision Analysis*, 3(4), 233–251.
- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: an empirical analysis. *Geneva Papers on Risk and Insurance - Issues and Practice*, 40(1), 131–158.
- Bikker, J. A., & Gorter, J. (2011). Restructuring of the Dutch nonlife insurance industry: consolidation, organizational form, and focus. *Journal of Risk and Insurance*, 78(1), 163–184.

order to identify potential time trends. For example, Maillart and Sornette (2010) illustrate an explosive growth in data breach frequency until 2006 and a stable rate thereafter; severity remained stable over time. These results might be interpreted in that the risk of change underlying cyber risk data might become less of a problem, but overall it remains unclear whether the past cyber risk data can be a reliable indicator for future cyber events.

- Bikker, J. A., & van Leuvensteijn, M. (2008). Competition and efficiency in the Dutch life insurance industry. *Applied Economics*, 40(16), 2063–2084.
- Bliss, R. R., & Panigirtzoglou, N. (2004). Option-Implied Risk Aversion Estimates. *Journal of Finance*, 59(1), 407–446.
- Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. *Workshop on the Economics of Information Security (WEIS)*.
- Bolot, J., & Lelarge, M. (2009). Cyber insurance as an incentive for internet security. In *Managing Information Risk and the Economics of Security* (pp. 269–290). Springer US.
- Bühlmann, H. (1970). *Mathematical methods in risk theory*. Springer-Verlag.
- Bundesamt für Privatversicherungen. (2006). *Technisches Dokument zum Swiss Solvency Test*. http://www.finma.ch/archiv/bpv/download/i/SST_technischesDokument_061002.pdf
- Centre for the Study of Financial Innovation. (2019). *Insurance banana skins 2019*. <https://www.pwc.com/gx/en/financial-services/assets/pdf/insurance-banana-skins-2019.pdf>
- Cont, R. (2006). Model uncertainty and its impact on the pricing of derivative instruments. *Mathematical Finance*, 16(3), 519–547.
- Cummins, J. D., Dionne, G., McDonald, J. B., & Pritchett, B. M. (1990). Applications of the GB2 family of distributions in modeling insurance loss processes. *Insurance: Mathematics and Economics*, 9(4), 257–272.
- Cummins, J. D., & Phillips, R. D. (2005). Estimating the cost of equity capital for property-liability insurers. *Journal of Risk and Insurance*, 72(3), 441–478.
- Denuit, M., Dhaene, J. M. L., Goovaerts, M., Kaas, R., & Laeven, R. J. A. (2006). Risk measurement with equivalent utility principles. *Statistics & Decisions*, 24(1/2006), 1–25.
- Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J., & Winkelmann, Z. (2018). *Estimating the global cost of cyber risk: methodology and examples*. RAND Corporation.
- Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: a closer look at

- data breaches. *Journal of Cybersecurity*, 2(1), 3–14.
- 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. *North American Actuarial Journal*.
- Eling, M., & Wirfs, J. H. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109–1119.
- Embrechts, P., Nešlehová, J., & Wüthrich, M. V. (2009). Additivity properties for value-at-risk under archimedean dependence and heavy-tailedness. *Insurance: Mathematics and Economics*, 44(2), 164–169.
- European Commission (EC). (2015). Commission delegated regulation 2015/35: supplementing directive 2009/138/EC of the European parliament and of the council on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II). *Official Journal of the European Union*, 58(L12), 1–797.
- Fahrenwaldt, M. A., Weber, S., & Weske, K. (2018). Pricing of cyber insurance contracts in a network model. *ASTIN Bulletin*, 48(3), 1175–1218.
- Freifelder, L. R. (1979). Exponential utility theory ratemaking: an alternative ratemaking approach. *Journal of Risk and Insurance*, 46(3), 515.
- Geruso, M. (2017). Demand heterogeneity in insurance markets: Implications for equity and efficiency. *Quantitative Economics*, 8(3), 929–975.
- Gollier, C., Koehl, P.-F., & Rochet, J.-C. (1997). Risk-taking behavior with limited liability and risk aversion. *Journal of Risk and Insurance*, 64(2), 347–370.
- Golubin, A. Y. (2016). Optimal insurance and reinsurance policies chosen jointly in the individual risk model. *Scandinavian Actuarial Journal*, 2016(3), 181–197.
- Herath, H., & Herath, T. (2011). Copula based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2(1), 7–20.
- Huberman, G., Mayers, D., & Smith, C. W. (1983). Optimal insurance policy indemnity schedules. *Bell Journal of Economics*, 14(2), 415–426.
- Ibragimov, R., Jaffee, D., & Walden, J. (2009). Nondiversification traps in catastrophe insurance markets. *Review of Financial Studies*, 22(3), 959–993.

- Ibragimov, R., Jaffee, D., & Walden, J. (2018). Equilibrium with monoline and multiline structures. *Review of Finance*, 22(2), 595–632.
- Ibragimov, R., & Prokhorov, A. (2016). Heavy tails and copulas: limits of diversification revisited. *Economics Letters*, 149(C), 102–107.
- Ibragimov, R., & Walden, J. (2007). The limits of diversification when losses may be large. *Journal of Banking & Finance*, 31(8), 2551–2569.
- Ikefuji, M., Laeven, R. J. A., Magnus, J. R., & Muris, C. (2020). Expected utility and catastrophic risk in a stochastic economy–climate model. *Journal of Econometrics*, 214(1), 110–129.
- Jacobs, J. (2014). *Analyzing ponemon cost of data breach*. <http://datadrivensecurity.info/blog/posts/2014/Dec/ponemon>
- Jean-Baptiste, E. L., & Santomero, A. M. (2000). The design of private reinsurance contracts. *Journal of Financial Intermediation*, 9(3), 274–297.
- Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*.
- Kleiber, C., & Kotz, S. (2003). *Statistical size distributions in economics and actuarial sciences*. Wiley.
- Kunreuther, H. C., & Michel-Kerjan, E. O. (2009). The development of new catastrophe risk markets. *Annual Review of Resource Economics*, 1(1), 119–137.
- Lewis, J. A. (2018). *Economic impact of cybercrime - no slowing down*. <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cyber-crime.pdf>
- Maillart, T., & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *European Physical Journal B*, 75(3), 357–364.
- Marsh-Microsoft. (2018). *By the numbers: global cyber risk perception survey*. <https://www.marsh.com/uk/insights/research/global-cyber-risk-perception-survey.html>
- McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management: concepts, techniques and tools*. Princeton Series in Finance.

- Meyer, J. (1987). Two-moment decision models and expected utility maximization. *American Economic Review*, 77(3), 421–430.
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: to insure IT or not? *Decision Support Systems*, 56(1), 11–26.
- National Association of Insurance Commissioners (NAIC). (2017). *U.S. property and casualty insurance industry*. https://www.naic.org/cipr_topics/topic_insurance_industry_snapshots.htm
- National Association of Insurance Commissioners (NAIC). (2019). *Report on the cyber-security insurance and identity theft coverage supplement*. https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final%281%29.pdf
- Nolan, J. (2003). *Stable distributions: models for heavy-tailed data*. Birkhauser.
- Northrop, P. J., & Attalides, N. (2016). Posterior propriety in bayesian extreme value analyses using reference priors. *Statistica Sinica*, 26(2), 721–743.
- OECD. (2017). *Global insurance market trends 2017*. <https://www.oecd.org/daf/fin/insurance/Global-Insurance-Market-Trends-2017.pdf>
- Outreville, J. F. (2014). Risk aversion, risk behavior, and demand for insurance: a survey. *Journal of Insurance Issues*, 37(2), 158–186.
- Parenty, T. J., & Domet, J. J. (2019). Sizing up your cyberrisks. *Harvard Business Review*, 97(6), 102–110.
- PartnerRe. (2018). *2018 survey of cyber insurance market trend*. <https://partnerre.com/wp-content/uploads/2018/10/2018-Survey-of-Cyber-Insurance-Market-Trends.pdf>
- Ponemon Institute. (2015). *2015 cost of cyber crime study: global*. http://informationsecurity.report/Resources/Whitepapers/5fe1dd7e-b46d-49f6-833a-d192cecb29e3_2015-cost-cyber-crime-study-global-pdf-10-w-2093.pdf
- Privacy Rights Clearinghouse (PRC). (2019). *Data breaches*. <https://www.privacyrights.org/data-breaches>

- Reich, A. (1984). Premium principles and translation invariance. *Insurance Mathematics and Economics*, 3(1), 57–66.
- Reichel, L., & Schmeiser, H. (2018). The liability regime of insurance pools and its impact on pricing. *North American Actuarial Journal*, 22(4), 533–553.
- Shetty, N., Schwartz, G., & Walrand, J. (2010). Can competitive insurers improve network security? *International Conference on Trust and Trustworthy Computing*, 308–322.
- Spiceworks. (2019). *Data snapshot: how common is cyber insurance in the workplace?* <https://community.spiceworks.com/blog/3166-data-snapshot-how-common-is-cyber-insurance-in-the-workplace>
- Statista. (2018). *Operating expense ratio of property and casualty insurers in Canada from 1990 to 2017*. <https://www.statista.com/statistics/471817/operating-expense-ratio-of-property-and-casualty-insurers-in-canada/>
- Statista. (2019). *Cyber insurance - statistics & facts*. <https://www.statista.com/topics/2445/cyber-insurance>
- Subramanian, A., & Wang, J. (2018). Reinsurance versus securitization of catastrophe risk. *Insurance: Mathematics and Economics*, 82, 55–72.
- Swiss Re. (2005). *Insurer's cost of capital and economic value creation*.
- Swiss Re. (2017). *sigma 1/2017 - Cyber: getting to grips with a complex risk*. http://www.swissre.com/library/sigma_01_2017_en.html
- Venter, G. G., & Sahasrabudde, R. V. (2015). A note on parameter risk. *Variance*, 9(1), 54–63.
- Wang, S. S., Young, V. R., & Panjer, H. H. (1997). Axiomatic characterization of insurance prices. *Insurance: Mathematics and Economics*, 21(2), 173–183.
- Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *European Physical Journal B*, 89(1), 7.
- World Economic Forum. (2020). *The global risks report 2020*. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
- Yang, X., Frees, E. W., & Zhang, Z. (2011). A generalized beta copula with applications

in modeling multivariate long-tailed data. *Insurance: Mathematics and Economics*, 49(2), 265–284.

Zanjani, G. (2002). Pricing and capital allocation in catastrophe insurance. *Journal of Financial Economics*, 65(2), 283–305.

Zweifel, P., & Eisen, R. (2012). *Insurance economics*. Springer-Verlag.

7 Appendices

Appendix A. Results for alternative dataset

As an additional robustness test, we conducted the same analysis with another frequently used data set on data breaches (see, e.g., Edwards et al., 2016; Kamiya et al., 2020; Maillart & Sornette, 2010) provided by the Privacy Rights Clearinghouse (PRC, 2019). Compared to our main dataset the PRC data has the advantage of being more homogeneous, but it contains no information on the economic importance of the data breach events (the number of breached data is reported, but not the associated costs). The database contains data breaches that occurred between 2005 and 2019 in the United States. We follow Edwards et al. (2016) and delete all observations with zero breached records and attain a sample of 6'822 observations. The database documents the number of records breached per incident and not the financial losses. To derive at least a rough estimate for the financial losses Z we multiply number of records R with an estimate of the average costs per data breach (Jacobs, 2014; Ponemon Institute, 2015):

$$\ln(Z) = 7.68 + 0.76 \cdot \ln(R). \quad (\text{A1})$$

We note that since the data set only tracks breaches, it might not be representative for cyber risk generally as it does not contain all possible types of cyber incidents. Table A1 shows the fittings of different distributions and estimates for the Pareto index to Z for the PRC data.

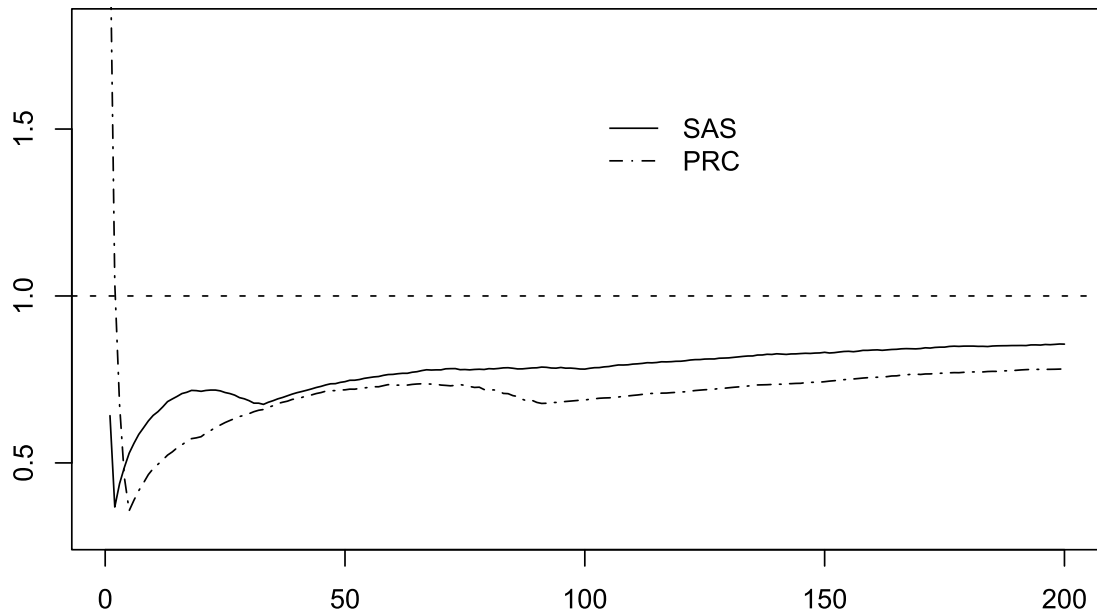
Table A1. Fitted distributions

Distribution	LL	AIC	BIC	KS	AD	α
Lognormal	-13'113	26'230	26'244	0	0	
Generalized Pareto (GPD)	-12'827	25'659	25'680	0	0	0.77
Peak over threshold (POT)	-12'730	25'469	25'504	-	-	0.68
Generalized beta (GB2)	-12'704	25'416	25'444	0	0	0.62
Levy	-16'293	32'588	32'595	0	0	0.5
Stable	-13'076	26'161	26'188	0	0	0.6

Note: LL stands for the logarithmic likelihood of the maximum likelihood estimation, AIC for the Akaike information criterion, BIC for Bayesian information criterion, KS for the Kolmogorow-Smirnow test, AD for the Anderson-Darling test, and α for the tail index. The KS and AD columns report p values. These statistics are not available for the POT due to its discontinuities. The tail (Pareto) indices can only be reported for the power laws. For GPD and POT the indices are calculated as the inverse of the GPD's shape parameters ($\frac{1}{\xi}$), for the GB2 it is aq , and the index for the Levy is fixed at 0.5. The POT approach slices a lognormal body and a Pareto distribution at the 56%-quantile (Eling & Wirfs, 2019).

Similar to Maillart and Sornette (2010) and Wheatley et al. (2016) we find that heavy tailed power law distributions fit the PRC data best and the tail index is around 0.7. Compared to the SAS data, the PRC data is best described by the peak over threshold (POT) and the generalized beta (GB2) distribution. Moreover, the tail indices are larger than for the SAS data and thus the distributions are less heavy tailed. Figure A1 shows the premium ratio for the PRC data. When comparing to the results in the main text, the figure shows that the results are qualitatively very similar for the PRC data. The reason is that the cover limit (set to US\$ 100 million) reduces the effect the tail behavior has on our result.

Figure A1. Premium ratio for PRC data



Note: The figure compares the premium ratio of the PRC data and the SAS data for the iid Levy distributed risks; the parameters are set as in the main text (Table 1).

Appendix B: Results of distribution fitting

We extend the set of distributions considered by Eling and Wirfs (2019) with some more general classes. As shown in Table B1, they perform quite well and all fall into the class of (very) heavy tailed power laws.²⁰ Eling and Wirfs (2019) consider the gamma, exponential, Weibull, GPD, lognormal and log-logistic distributions. A distribution that nests all these distributions (as limiting or special cases), but is more general (includes generalized gamma, Pareto, Burr and many others) is the generalized beta (GB) prime distribution, also called the GB of type 2 (GB2; see, e.g., Kleiber & Kotz, 2003). This distribution has been suggested to fit insurance losses quite well due to its capability of matching skewed and heavy tailed distributions (see, e.g., Cummins et al., 1990; Yang et al., 2011). The distribution can be theoretically justified as it represents losses originated from a heterogeneous risk pool (see, e.g., Kleiber & Kotz, 2003). Since it is a natural candidate for matching cyber risk, we also use it here. GB2 defines a four parameter (shape1= a , scale= b , shape2= p , shape3= q) distribution family.

²⁰ Thus, the tail is declining sub-exponentially, but slower than the lognormal distribution; the normal distribution features an exponential decline.

Table B1. Fitted distributions

Distribution	LL	AIC	BIC	KS	AD	α
Lognormal	-4'588	9'180	9'191	0.0000	0.0000	-
Generalized Pareto (GPD)	-4'553	9'113	9'129	0.0000	0.0003	0.63
Peak over threshold (POT)	-4'486	8'982	9'008	-	-	0.69
Generalized beta (GB2)	-4'483	8'973	8'995	0.0067	0.0017	0.50
Levy	-4'473	8'950	8'995	0.0002	0.0003	0.50
Stable	-4'461	8'929	8'951	0.0000	0.0004	0.44

Note: LL stands for the logarithmic likelihood of the maximum likelihood estimation, AIC for the Akaike information criterion, BIC for Bayesian information criterion, KS for the Kolmogorow-Smirnow test, AD for the Anderson-Darling test, and α for the tail index. The KS and AD columns report p values. These statistics are not available for the POT due to its discontinuities. The tail (Pareto) indices can only be reported for the power laws. For GPD and POT the indices are calculated as the inverse of the GPD's shape parameters ($\frac{1}{\xi}$), for the GB2 it is aq , and the index for the Levy is fixed and not estimated. The POT approach slices a lognormal body and a Pareto distribution at the 56%-quantile (Eling & Wirfs, 2019).

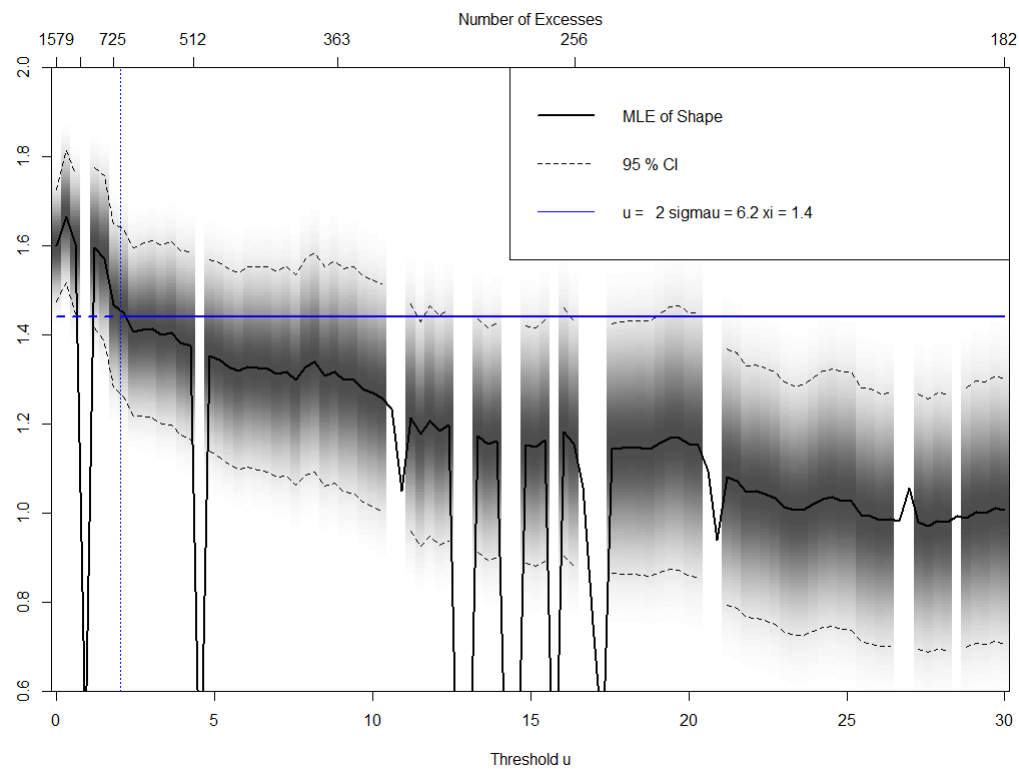
Since the GB2 generalizes GPD and lognormal, it is more flexible and outperforms them. It even outperforms the POT model for all goodness of fit measures. This might be due to the rather unrealistic property of the POT distribution that features a jump at the threshold. The results for AIC and BIC suggest that this result is not due to overfitting. For the GB2 the kurtosis is determined by a and the skewness is controlled by p and q . The right tail of the GB2 is controlled by a and q , while the left tail is determined by a and p . We can also observe that the better fit of GB2 relative to GPD is due to a deviating from 1 that would be required for the GB2 to reduce to the GPD. In our case is estimated to be 1.1. Thus, it is not clear whether it is the right, left, or both tails that contribute to the improvement in the fit. In the limit GB2's right tail behaves according to the tail index $\alpha = aq=0.5$.

We also consider the $(\alpha-)$ stable distributions (see, e.g., Nolan, 2003) as another broad class of distributions that account for heavy tailedness and has useful analytical properties. Since losses are always positive, we restrict the parameters such that the distribution is defined for positive numbers. This can be achieved by setting the location parameter to 0 and the skewness parameter to 1. While the stable distribution fits our dataset best,

the KS and AD are more in favor of the GB2 distribution (but still very low). The stable distribution has a tail index α that determines its tail behavior. As the estimated tail index is 0.5, the Levy distribution would be a well-suited distribution. Thus, we also fit the levy and report its results. As the stable and particularly the Levy distribution have useful analytical properties (closed under portfolio formation), we rely on them in follows. Generally, the tail indices for all distributions estimated are smaller than 1. Thus, all fitted distributions agree on heavy tailed power laws. Since all the distributions tail indices fall in a very narrow range, we expect qualitatively the same results for all models.

We analyze the stability of the estimated Pareto index in Figure B1. It shows the estimated shape index (that is the inverse of the Pareto index) for different thresholds in the context of the POT approach, which combines a lognormal for the body and a generalized Pareto distribution for the tail. The choice of the threshold determines the optimal shape parameter (according to maximum likelihood). More precisely, the optimal Pareto index tends to increase as the threshold is moved upwards. The figure also shows the confidence interval for the shape index. For the major part the shape parameter and its confidence interval lie above one that would yield a Pareto index lower than one. For our choice of the threshold of 2.0 (56%-quantile) and a shape parameter of 1.45 the true value is supposed to lie between 1.25 and 1.65 with a probability of 95%. Thus, we find support for the notion of extremely heavy tail distribution. The discontinuities in Figure B1 are caused by the sparse observations in the empirical distribution over certain ranges.

Figure B1. Pareto index stability



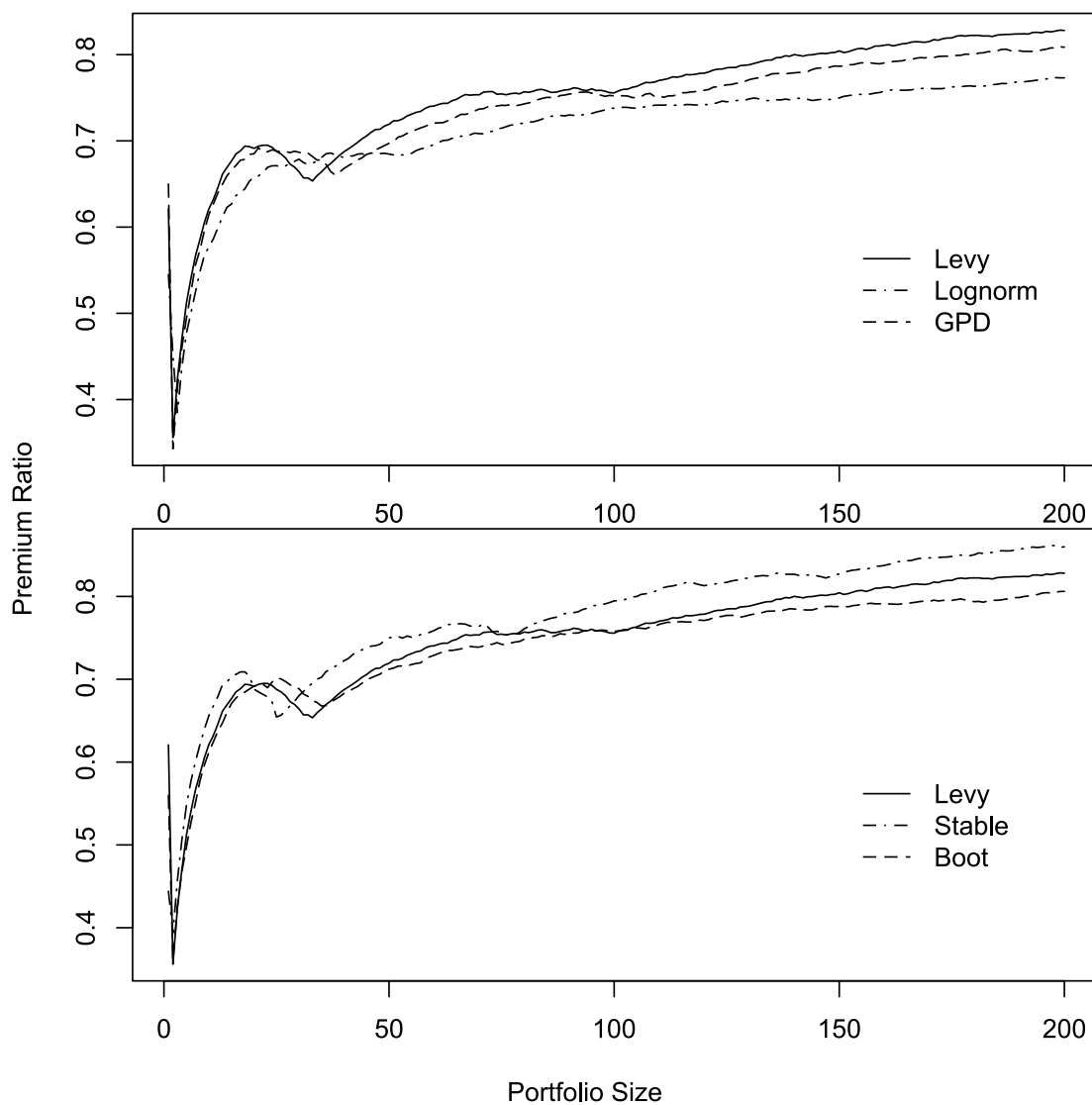
Note: The solid black line shows the maximum likelihood estimate of the POT shape parameter for different thresholds (in million US\$). The dashed black lines indicate the confidence interval for the true parameter and the blue lines mark our choice for the threshold and shape parameter.

Appendix C. Results for alternative assumptions

Appendix C1. Results for alternative distribution models

In Figure C1 we show the premium ratios for additional distribution assumptions, namely the lognormal, the generalized Pareto, the Levy, and the stable distribution. All other parameters are the same as in the main text.

Figure C1. Premium ratio for different distributions

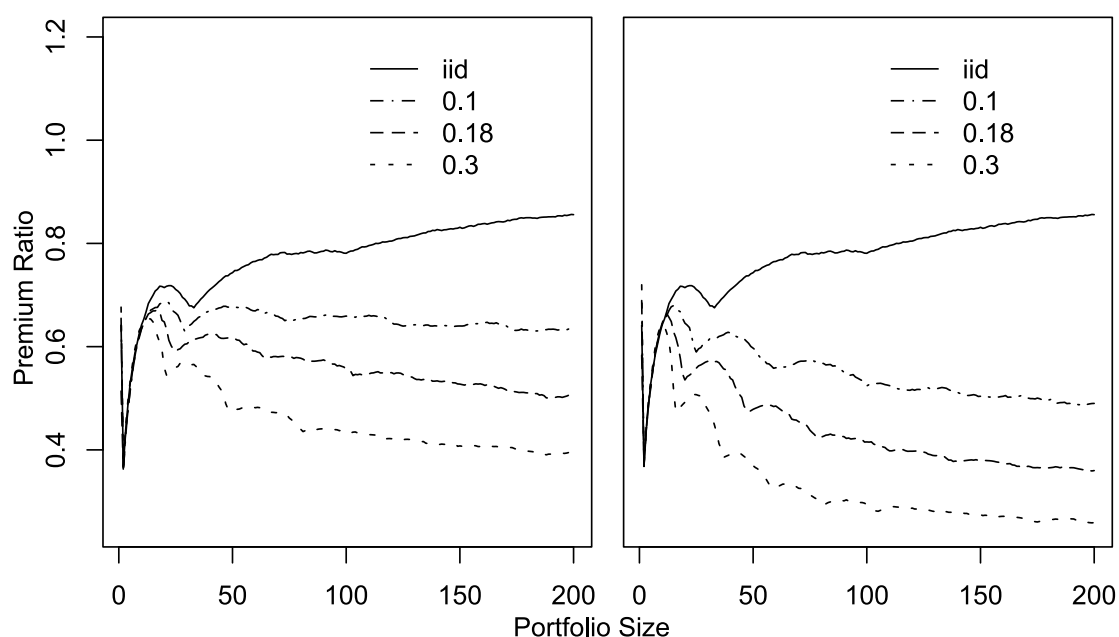


Note: The figure shows the premium ratio for the iid Levy, Lognormal, Generalized Pareto (GPD), and Stable distribution. We also show the result when a simple bootstrapping from the data is applied (Boot). The parameters are set as in the main text (Table 1).

As the analysis shows different distributions do not change the outcome significantly. Next, we also let the correlation assumption vary (see Figure C2). The analysis shows

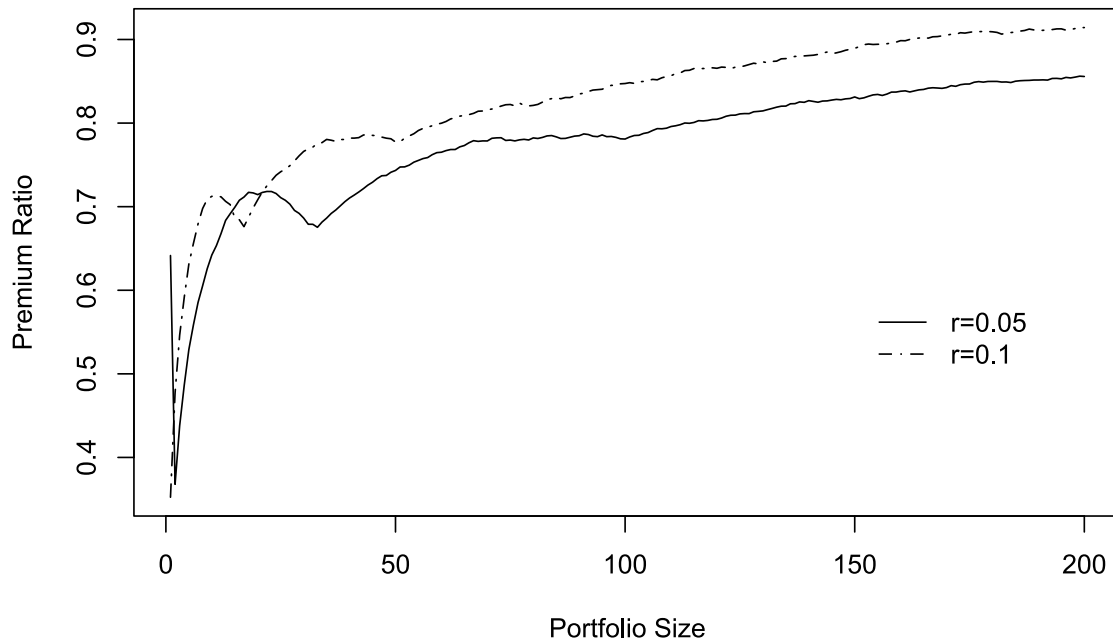
that the stronger the dependence the lower the premium ratio as the competitive premium increases relative to the willingness to pay. The reason is that stronger dependence reduces the benefits from diversification in the insurer's risk portfolio. This effect is even more pronounced for stronger tail dependence (as illustrated by the Clayton copula; see Figure C2 right). In line with the findings for the modeling risk, we identify the dependence structure as a main driver for the market failure.

Figure C2. Premium ratio for different correlations



Note: The figure shows the premium ratio for the Gauss (left) and Clayton dependence model for different correlations (0.1, 0.18, 0.3). Everything else is based on the Levy distribution and the parameters are set as in the main text (Table 1).

Figure C3. Premium ratio for different loss frequency



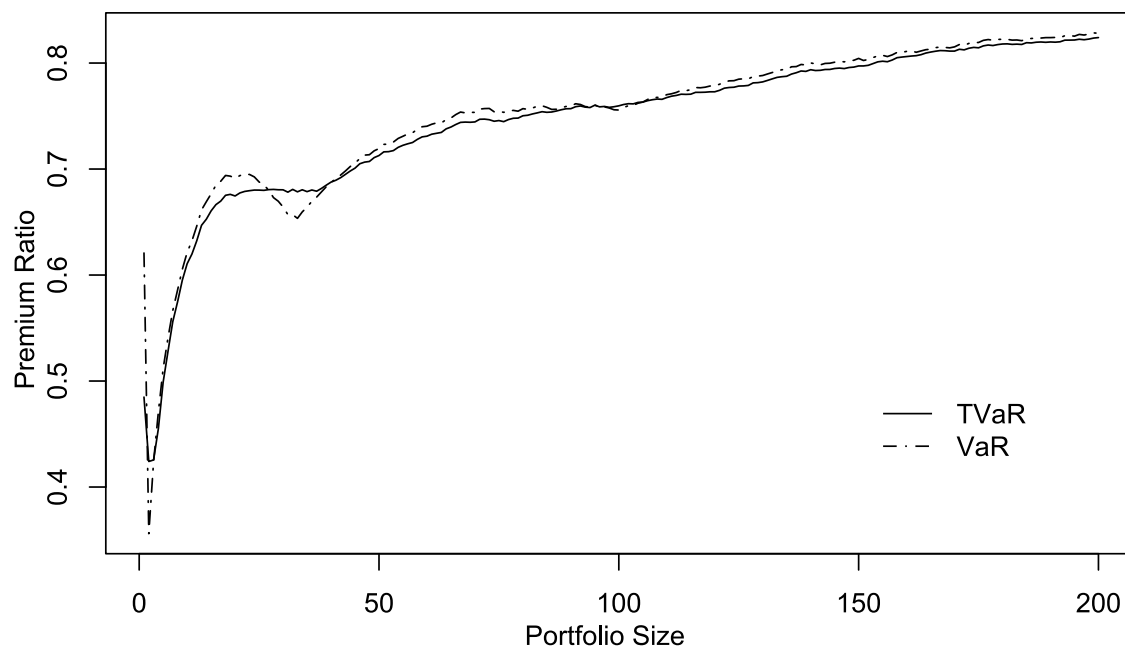
Note: The figure shows the premium ratio for different loss frequency (0.05, 0.1). Everything else is based on the Levy distribution and the parameters are set as in the main text (Table 1).

Finally, we also take a closer look at the effect the loss frequency of cyber risks has on our results. The findings are presented in Figure C3. Even a doubling of the frequency to 10% does not affect the result much. The reason is again that we assume in our model that both market sides have the same information about the frequency. Thus, a higher loss frequency not only increases the competitive premium it also increases the premium the clients are willing to pay. We conclude that the loss frequency is not a main driver for the market failure.

Appendix C2. Results for alternative risk measures

We also analyze the results for regulatory capital requirement based on different risk measures as calculated in Equation (6) in the main text. Some regulatory framework use the tail value at risk (TVaR) instead of the value at risk (VaR). Following the Swiss system we used the 99%-TVaR (Bundesamt für Privatversicherungen, 2006). Figure C4 shows the result for the different capital requirement. Compared to the results for 99.5%-VaR the results are qualitatively very similar.

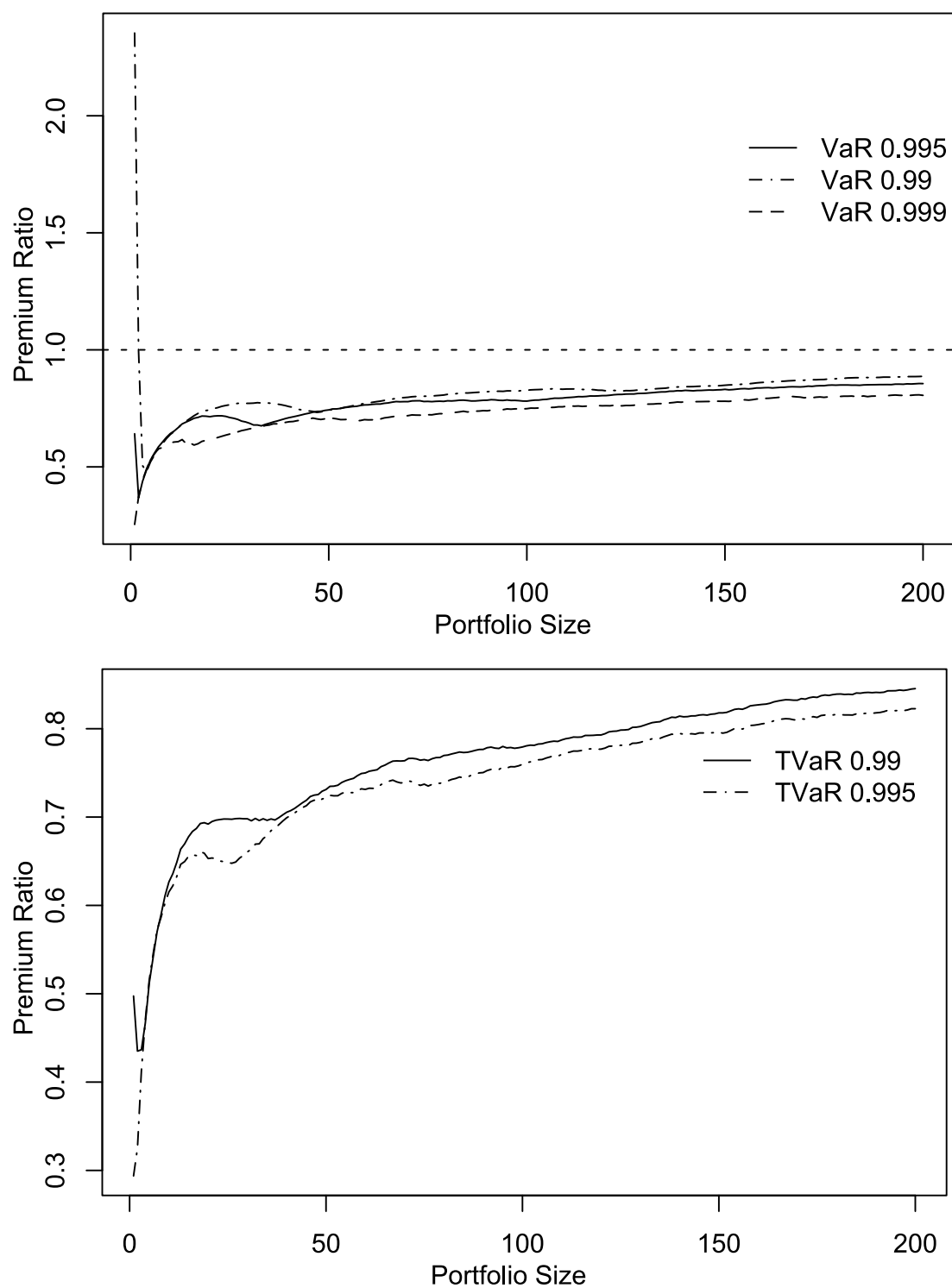
Figure C4. Premium ratio for TVaR



Note: The figure compares the premium ratio for capital requirements based on 99.5%-VaR to the 99%-TVaR for the iid Levy distribution. The parameters are set as in the main text (Table 1).

The confidence level is set at 99.5% (VaR) and 99% (TVaR) in the regulatory frameworks. Figure C5 shows the premium ratio for three alternative confidence levels for each of the two risk measures (99%, 99.5%, 99.9%). The tail value at risk for the 99.9% confidence level cannot be calculated since there are not enough observations in the data to calculate the expectation above a threshold of 99.9%.

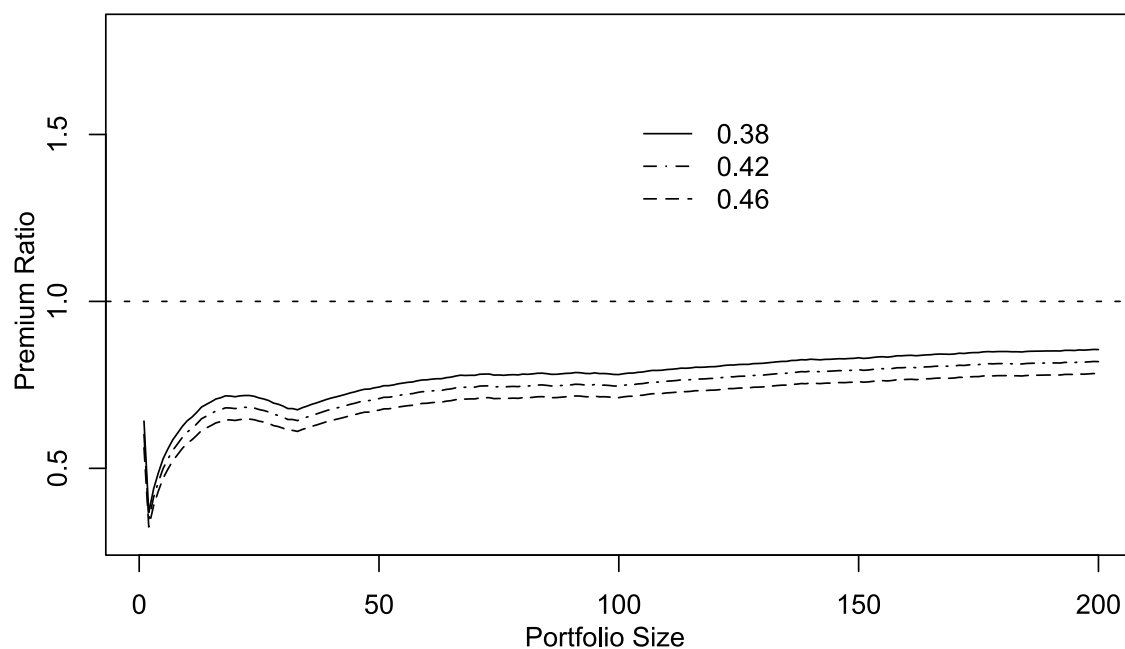
Figure C5. Premium ratio for alternative confidence levels



Note: The figure compares the premium ratio for capital requirements based on different confidence levels (99%, 99.5%, 99.9%). The results are based on the iid Levy distribution and the parameters are set as in the main text (Table 1).

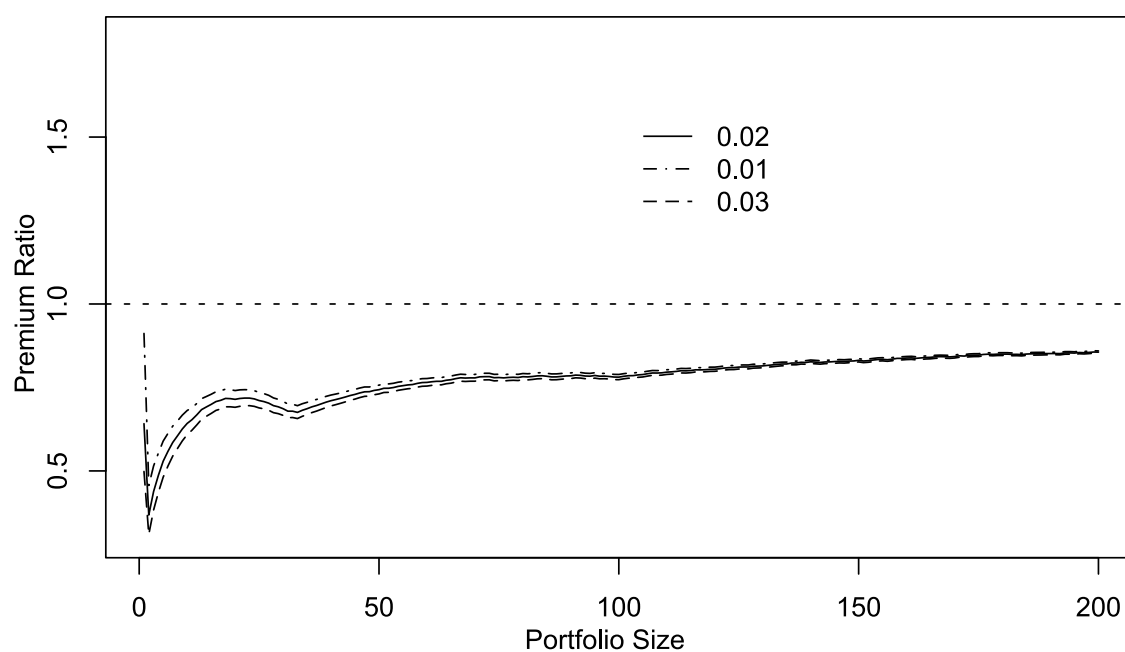
Appendix C. Results for alternative cost functions

Figure C6. Premium ratio for different cost functions



Note: The figure compares the premium ratio for different cost functions $c_{a,1} = (0.38, 0.42, 0.46)$. The results are based on the iid Levy distribution and the other parameters are set as in the main text (Table 1).

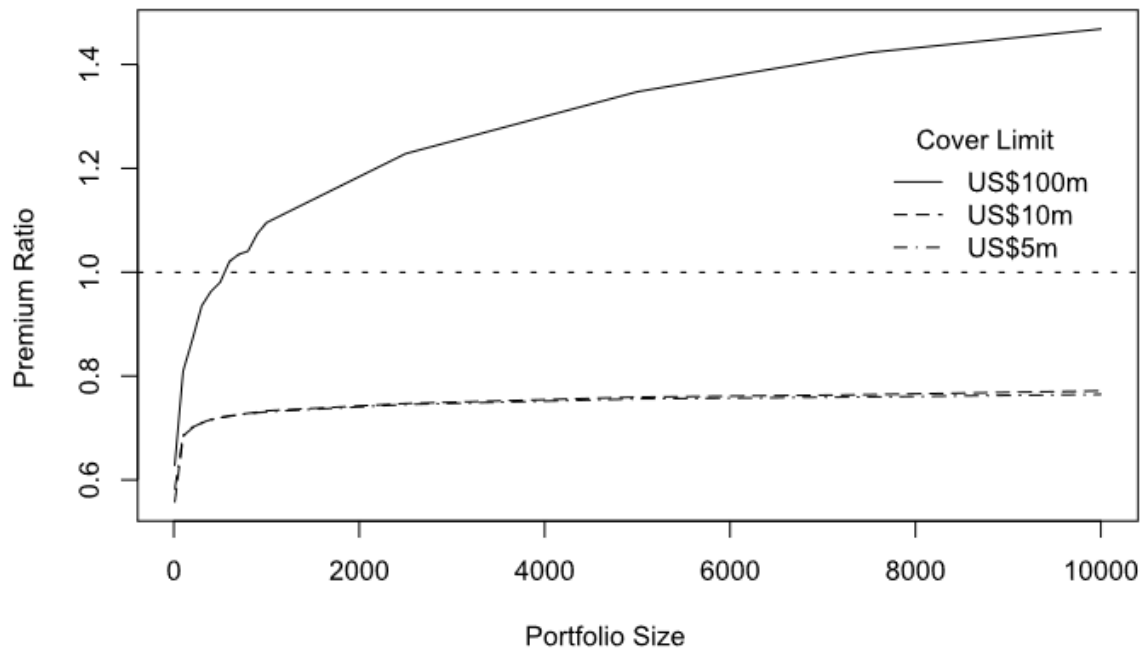
Figure C7. Premium ratio for different frictional capital costs



Note: The figure compares the premium ratio for different frictional capital costs (0.02, 0.01, 0.03). The other parameters are set as in the main text (Table 1).

Appendix C4. Results for alternative cover limits

Figure C8. Premium ratio for alternative cover limits



Note: The figure compares the premium ratio as the portfolio size increases beyond the range analyzed in the main text. The analysis is based on the baseline model (iid Levy) and the parameters are chosen as in the main text.

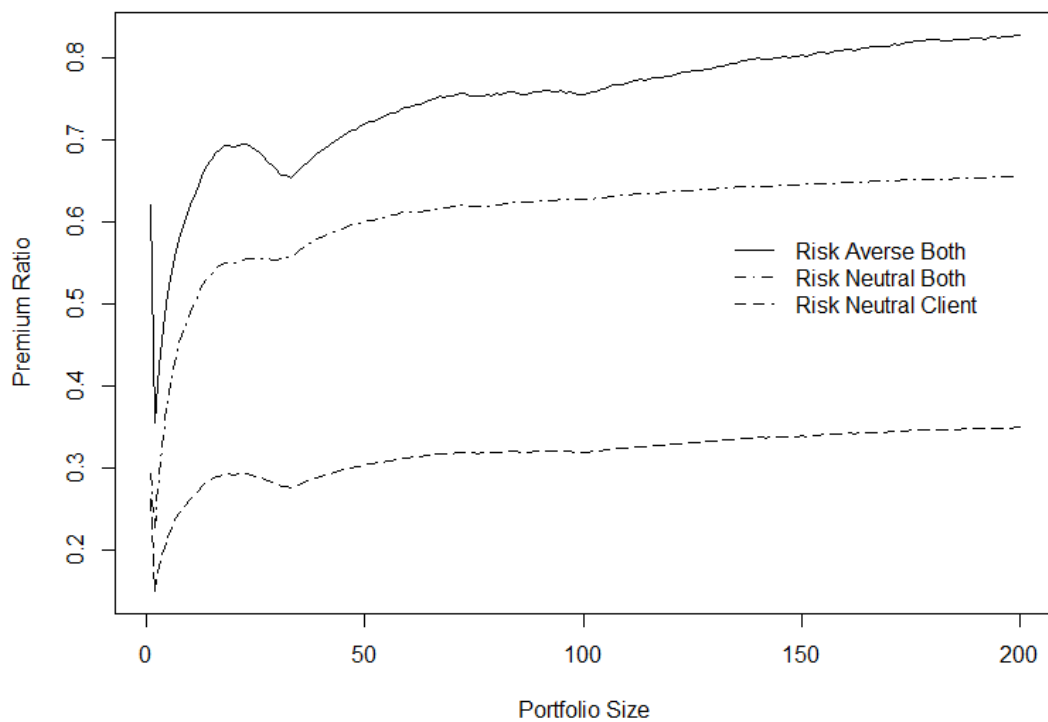
Appendix C5. Results for alternative risk preferences

Risk neutrality

While we argue in the main text that firms behave risk averse, firms are frequently modeled risk neutral. The reason for that is that it is frequently assumed that shareholders hold their assets in well diversified portfolios. If the management acts in line with the shareholders interest, the firm might act under such circumstances risk neutral with respect to idiosyncratic risk. However, since diversification does only affect the idiosyncratic risk, the question is whether we would still need to consider systemic risk. We assume systematic risk is not relevant here, since the correlation between underwriting and stock market returns are usually low. For example, Cummins and Phillips (2005) find that the underwriting systematic risk beta for property and liability insurance is even negative (-0.1) for the U.S. For cyber risk we calculate a correlation between the changes in cyber losses and the S&P 500 index returns on a yearly basis of 0.03 and a corresponding systematic risk beta of 0.11.

Similar to Zanjani (2002, p. 288), we implement a risk neutral approach by evaluating the payoffs with the expectation as the value functional H (Equation 16). We use the expectation under objective probabilities, meaning neither the idiosyncratic nor systemic risk is relevant. Figure C9 reports the results for risk averse and risk neutral decision makers. For the risk neutral decision-makers, we consider both the case of risk neutrality for clients only as well as for clients and decision-makers in the insurance firm.

Figure C9. Premium ratio for risk neutrality



Note: The figure compares the premium ratios of the risk neutral approach and the risk averse model in the main text for the iid Levy distribution. For the three models listed in the Figure, we set the parameters (a_I, a_C) to $(0.02, 0.02)$, $(0, 0)$, and $(0.02, 0)$, respectively.

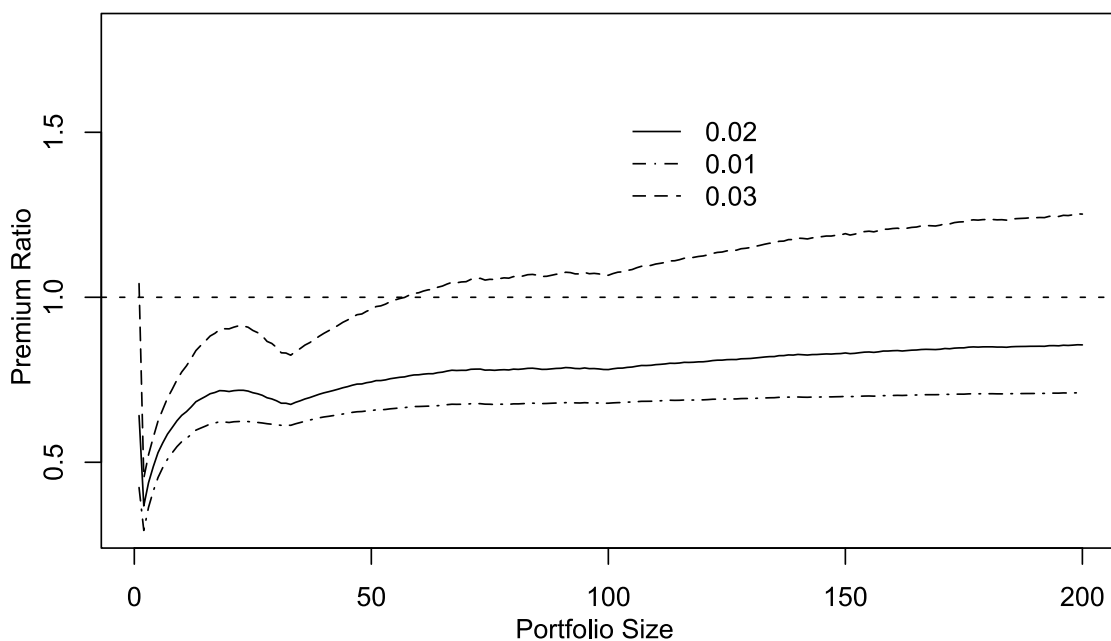
As discussed, regulation causes the risk aversion for clients to be lower than for the insurer. Thus, when the client becomes less risk averse compared to the insurer, the willingness to pay monotonically decreases relative to the competitive premium. When both the insurer and client become simultaneously less risk averse the premium ratio also decreases or, in other terms, the willingness to pay decreases more relative to competitive premium. The reason for this is that the insurer keeps the risks in a diversified portfolio. This reduces volatility and as a consequence sensitivity towards changes in the risk aversion parameter. To conclude, also for alternative risk attitudes we still observe

a market failure in the sense that the premium ratio is always below one.

Different constant absolute risk aversion

Different assumptions regarding the risk aversion parameter are shown in Figure C10. Higher risk aversions for both (insuree and the insure) reduces the premium ratio. This means the willingness to pay increases more than the competitive premium. This can be explained by the fact that the insuree cannot diversify its risks and thus is more sensitive to an increase in the risk aversion.

Figure C10. Premium ratio for different CARA



Note: The figure compares the premium ratios for different risk aversions for the iid Levy distribution. For the three models (as listed in the legend), we set the parameters (a_I, a_C) to $(0.02, 0.01, 0.03)$.

Constant relative risk aversion

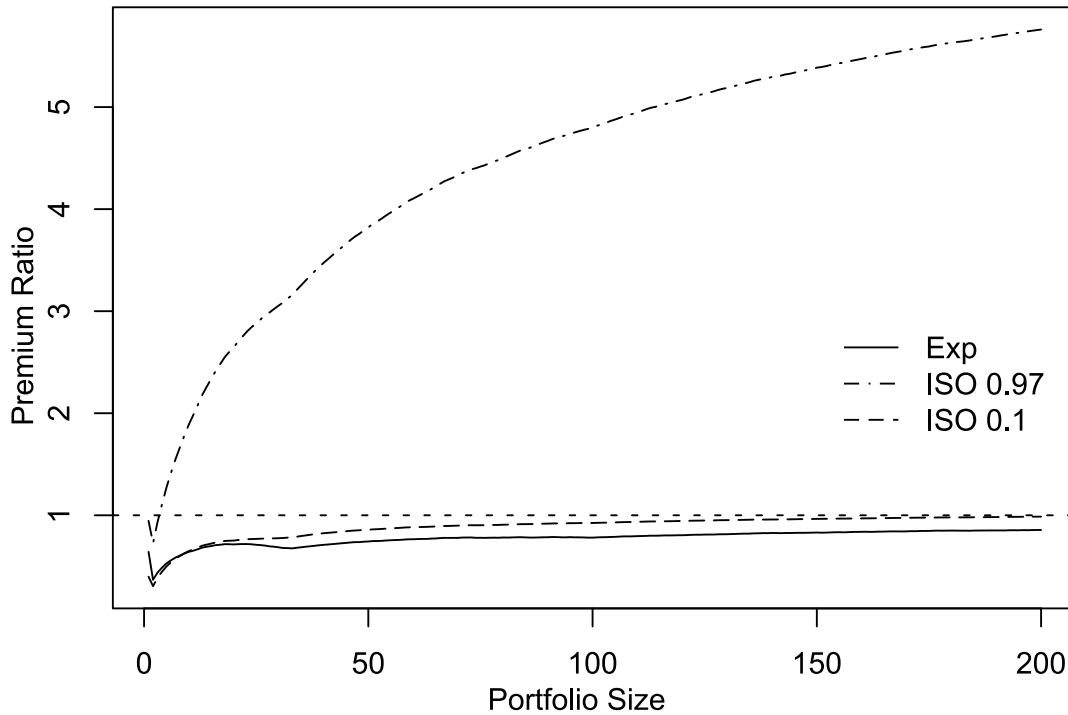
In the main text we use the exponential utility (Equation 17) that assumes constant absolute risk aversion. A utility function that allows the more realistic case of decreasing absolute risk aversion is the isoelastic utility function with constant relative risk aversion. However, because this utility function is not translation invariant it violates the principle of zero utility as stated in Equation (8). The principle requires that the utility before and after accepting the risk must be equal (Bühlmann, 1970). As a consequence, the pre-

mium based on the isoelastic utility function does not necessarily coincide with the competitive premium. The certainty equivalent H for the insuree and insurer respectively, $i \in \{c, I\}$, would then be:

$$H(P_i) = \begin{cases} \left(E(P_i^{1-\eta_i})\right)^{\frac{1}{1-\eta_i}}, & \eta_i \neq 1, \\ e^{E(\ln(P_i))}, & \eta_i = 1 \end{cases} \quad (D1)$$

where we choose $\eta_i = 0.97$ (Ibragimov et al., 2009) and $\eta_i = 0.1$ as alternative value representing a smaller degree of risk aversion. These values are at the lower end of the empirical findings for the relative risk aversion (see, e.g., Bliss & Panigirtzoglou, 2004; Outreville, 2014). As the equation shows H based on the isoelastic utility is scale equivariant (positive homogenous). The result for the isoelastic utility is compared to the exponential utility in Figure C11.

Figure C11. Premium ratio for isoelastic utility



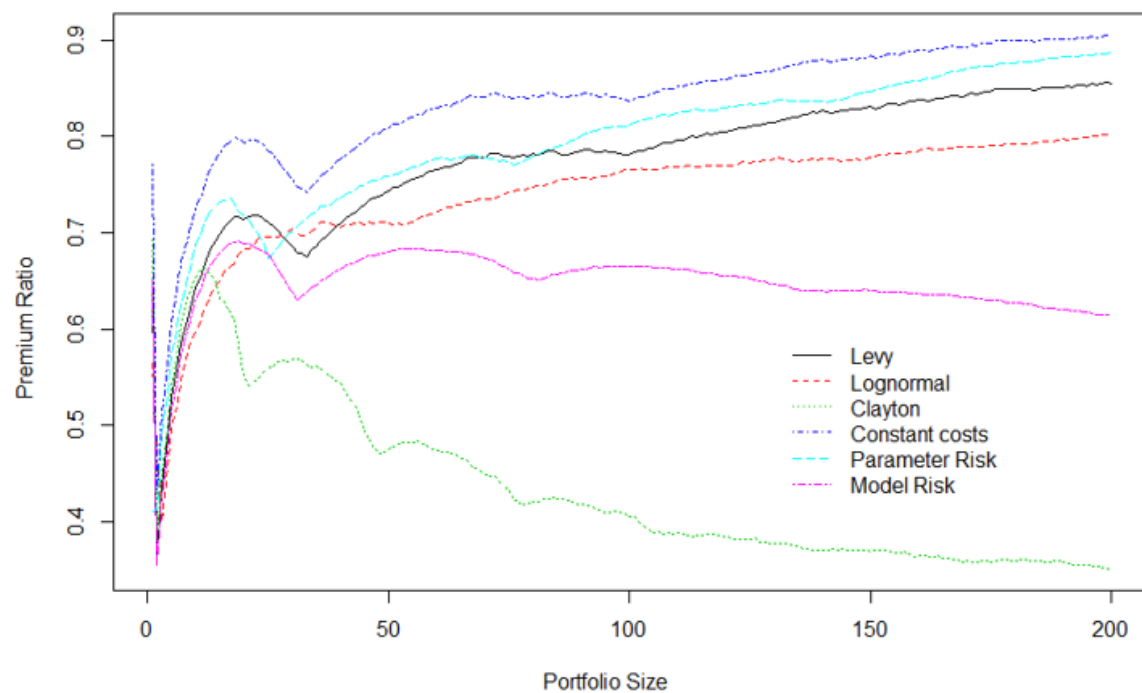
Note: The figure compares the premium ratios for the isoelastic utility function (ISO) and the exponential utility function (EXP) for the iid Levy distributed risks. The risk aversions are $\eta_i = (0.97, 0.1)$ for the isoelastic utility and $a_i = 0.02$ for the exponential utility for both $i \in \{c, I\}$.

While we observe a nondiversification trap for the isoelastic utility as well, the trap depends strongly, as for the exponential utility, on the choice of the risk aversion parameter.

Appendix C6. Comparison of different models

To understand what drives our results, we compare the premium ratio for different models in Figure C12. It shows that the biggest negative effect on the premium ratio and thus the market development have the model and the (tail) dependence risk (note that the dependence risk is also the main driver of the model risk). Lower costs (which we interpret as less asymmetric information) increase the premium ratio and thus would be beneficial for a cyber risk market. The tail parameter and the exact severity distribution play a comparatively minor role, especially because of the cover limit.

Figure C12. Comparison of different models



Note: The figure compares the premium ratio for different models. Each line shows the baseline model (Levy) with one change. These are lognormal distributed severity, Clayton dependent risks, constant cost function with $c_a = 0.25$, and the models with parameter and model risk priced.

Appendix D. Mathematical notes

Deriving Equation (11)

Starting from the translog function where c are the total costs and m is the total output:

$$\ln(c) = \beta_0 + \beta_c \cdot \ln(m)$$

we obtain

$$\ln\left(\frac{c}{m}\right) = \beta_0 + \beta_c \cdot \ln(m) - \ln(m)$$

Per definition $\frac{c}{m} = c_a$, then

$$\ln(c_a) = \beta_0 + (\beta_c - 1) \cdot \ln(m)$$

Let $(\beta_c - 1) = \beta$, then

$$\ln(c_a) = \beta_0 + \beta \cdot \ln(m)$$

After some transformations and $c_{a,1} = e^{\beta_0}$:

$$c_a = e^{\beta_0} \cdot m^\beta = c_{a,1} \cdot m^\beta$$

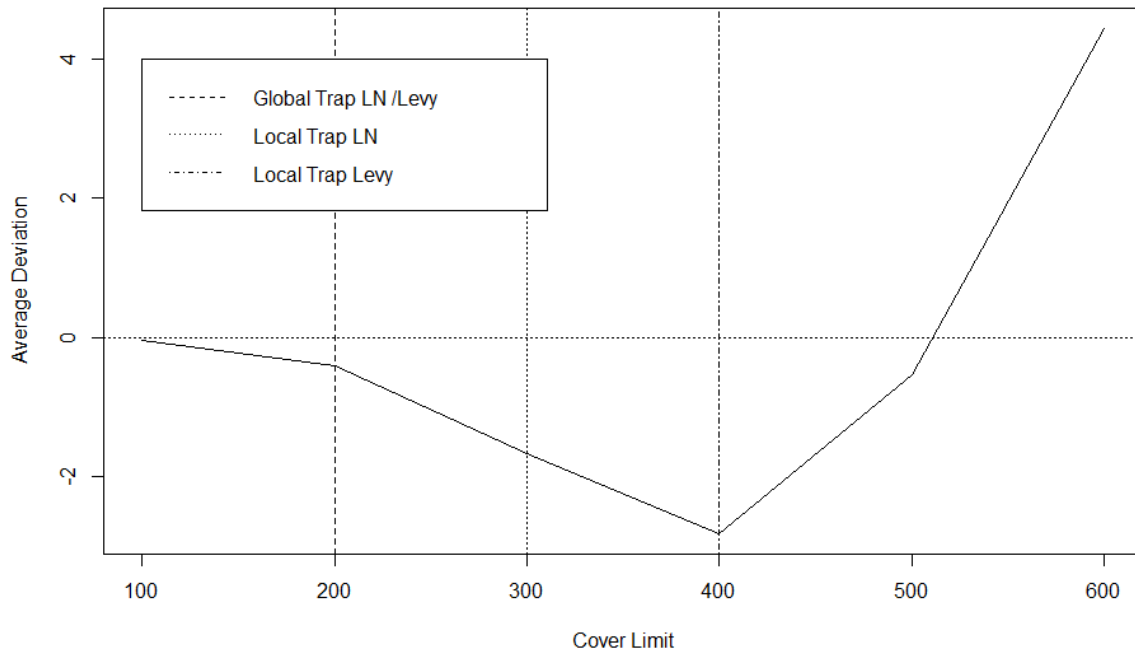
Appendix E. Tail behavior and cover limit

The findings of Ibragimov et al. (2009) might suggest that our results are driven by the heavy tails of the severity distribution. However, the cover limit lets the risks behave like non-heavy tailed. Since cover limit are always observe in real insurance contracts, they make an important difference between our analyses and Ibragimov et al. (2009) who consider cat risks and a different perspective. But as Ibragimov and Walden (2007) indicates, the diversification trap might reappear for sufficiently high cover limits. In the following we analyze the critical cover limit where the heavy tails start hindering diversification. For that we define the mean deviation, MD , of the premium ratio for the non-heavy tailed (lognormal; or more precisely not very heavy tailed) and the very heavy tailed (Levy) distribution over portfolio sizes, n , from 0 to 200:

$$MD = \sum_{i=1}^n R_{LN,n}^\pi - R_{Levy,n}^\pi.$$

Figure E1 shows the MD as a function of the cover limit, cl .

Figure E1. Tail behavior and cover limits



Note: The figure compares the mean deviation of the premium ratios for the lognormal distribution and the Levy distribution. It also shows the thresholds for qualitative changes in the outcome. Below $cl = 200$ both models lead to a global diversification trap, and above $cl = 300$ for the lognormal and $cl = 400$ for the Levy a market would exist (premium ratio always above 1). In-between there is a local trap for both models. All other parameters are set as in Table 1 and numbers are in million US\$.

The figure shows that for small cover limits the premium ratio is higher (and thus insurability better) for the heavy tailed distribution. In contrast to Ibragimov et al. (2009), heavy tailed risks are even beneficial for the development of a cyber insurance market if cover limits are used. However, above a cover limit of US\$ 520 million, the premium ratio for the heavy tailed distribution becomes increasingly lower. This means for higher cover limits than US\$ 520 million the heavy tails would start disturbing diversification and influence our results.

Essay IV

Epidemic cyber risk

Werner Schnell

Abstract

The strongly interconnected cyberspace allows cyber threats to spread quickly around the globe, affect a huge number of targets simultaneously, and potentially become catastrophic. We use a new network approach to model contagiousness and accumulation of cyber risks in a cyber insurance portfolio. Network models not only take nonlinear dependencies adequately into consideration, but they also allow for analysis of worst-case scenarios such as pandemics and systemic events. We analyze the consequences of network dependencies on premium calculation, diversification, risk management, and regulation of cyber insurance. We show that the most important pricing factor is the interconnectedness of a client's information technology (IT) and that diversification of cyber risks in an insurer's portfolio might not always be optimal. Hubs in the network structure can accentuate spreading and need to be accounted for when underwriting cyber insurance. Insurers should carefully select, charge adequate premiums, and require additional IT security measures especially for strongly interconnected clients. We provide insurers with a modeling framework and provide hints about information that should be surveyed to calibrate network models. Regulators are advised to review their insurers' capital requirements since they do not take the complex dependencies observed in network models adequately into account.

Keywords

Cyber risk, pandemic risk, systemic cyber risk, network model, risk accumulation, loss distribution approach

Status

This paper was presented at the *2020 World Risk and Insurance Economics Congress (WRIEC)*.

Acknowledgements

We are grateful to all the discussions and feedback which greatly improved our paper. Specifically, we thank Prof. Martin Eling, Prof. Angelo Ranaldo, Prof. Martin Boyer, PD Cristian Biener, and all the participants of the 2020 World Risk and Insurance Economics Congress for their feedbacks.

1 Introduction

New technologies such as blockchains, the Internet of Things, cloud computing, machine learning, and big data increasingly penetrate every aspect of life. While this technological progress has brought opportunities and prosperity, it has also increased individuals and companies' reliance on IT and amplified society's vulnerability to cyberattacks. Every interruption that threatens the confidentiality, integrity and availability of data and services can have severe consequences. Cyber threats, such as malware, are highly contagious, spread quickly around the globe, and can potentially affect a huge number of targets simultaneously.¹ The shock, while originating in cyber space, might eventually strike the real economy. When providers of critical services or infrastructures (e.g., stock markets, cloud services, power plants, communication services, traffic systems) are affected, the consequences are widespread and might even become catastrophic (WEF 2016). Such catastrophic events can affect insurers not only because they underwrite cyber insurance but also because the same incident might affect other lines of business simultaneously. Since insurers are strongly interconnected with the rest of the financial system (via the reinsurance market), they might even contribute to systemic risk.

Despite its significance, the spreading and cumulation properties of cyber risk are not well understood and consequently it is difficult to undertake appropriate mitigation measures (WEF 2016). Obstacles to understanding cyber risk cumulation better are the lack of data, extreme events, a fast-changing technological environment, and strong opaque interconnections (see, e.g., Biener et al., 2015). The lack of data and the changing underlying risk landscape lead to problems in forming meaningful expectations and projections based on previous observations. It is difficult to account for extreme events if they have not yet been observed, but just because an extreme event has not happened yet does not mean it will never happen. Finally, new models should strive to understand the way cyber risks cumulate. Strong nonlinear dependencies may cause relatively benign risks to cumulate to extreme losses on a portfolio or societal level (systemic cyber

¹ See for example the ransomware "WannaCry" in 2017 as one of the most consequential (infection based) cyber events observed so far. In only one day, the malware infected more than 200'000 computers in 150 countries and caused an estimated damage in the hundred millions if not billions of US\$ (Berr, 2017).

risk). In such circumstances, empirical models reach their limits. Instead, we need to build on technical knowledge about the interactions in IT systems and on worst-case scenarios based on experts' judgments.

To address these challenges, we extend the few previous attempts of using network models for cyber risks (see, e.g., Fahrenwaldt et al., 2018) by using more realistic network properties and adapt it to a concrete insurance cyber risk portfolio. We use a network in which the nodes represent the cyber policies in an insurer's portfolio and the connections between the nodes describe transmission mechanisms of cyber threats. We focus on the spreading and infection of malware, such as viruses, ransomware, trojans, worms, and spyware.² The network links then describe the IT infrastructure that facilitates the spreading of such malware. There are different networks relevant for the spreading of malware such as the physical infrastructure of the Internet (i.e., computers, servers, and routers), communication protocols (i.e., internet protocol (IP), http, cell phone, and email; see, e.g., Daffron et al. 2019), and even social media (e.g., Facebook). We use common empirical properties for such cyber-related networks, like link distribution and infection probability, to build a representation and to simulate infection spreading. Finally, losses over the whole network are aggregated to evaluate the distribution of the insurer's cyber insurance portfolio.

Modeling dependence with networks has some advantages over other approaches. Since networks build directly on the underlying infrastructure, they can more accurately describe the connections between cyber policies and, after aggregation, provide improved estimates of the aggregate (systemic or portfolio) loss distribution. They are also more flexible than parametric models, such as copulas, and allow for describing complex non-linear dependency structures. Moreover, networks are also appealing since they provide a deeper understanding of the underlying transmission mechanisms and thus allow for deriving efficient measures to reduce risk. Since networks can include hubs and IT security at the individual policy level, network models allow one to define and evaluate

² Our model can also describe non-malicious threats such as software bugs and security loopholes. Such cyber risks have been framed as interdependent IT security, where the same IT technology is deployed in multiple entities and causes similar vulnerabilities. In such a case, the network's links can represent the (security) software provider's own network of clients. Finally, other types of cyber risks are more idiosyncratic, such as insider attacks, hacking, hardware failure, and human error, and thus not of main interest here.

different scenarios (e.g., what would happen if a central or unsecured node is infected). An insurer could, for example, charge a higher premium or request enhanced IT security measures according to the role the company plays in the underwriting network. Finally, since networks do not rely directly on observed events, they enable extrapolation to more extreme outcomes in a well-defined and regulated way. The network that represents the transmission mechanism adequately also provides the projection rules for what could happen that has not yet been observed. The most extreme outcomes from simulating a network can serve as a theoretically well-founded (but abstract) worst-case scenario. This contrasts with fitting a distribution directly, as it is difficult to justify why it should describe rarely observed tail events appropriately.

We find that networks generate heavy-tailed, distributed loss frequencies in an insurer's cyber insurance portfolio. Combined with the heavy-tailed severity found in previous literature, this intensifies the extreme distribution of cyber risks. Consequently, this increases the premiums insurers charge for cyber insurance, reduces the benefits from diversifying cyber policies in an underwriting portfolio, and questions the appropriateness of regulatory capital requirements for underwriting cyber insurance. We also use stress tests and find that infecting highly interconnected nodes (exposed clients) greatly inflates the losses an insurer should expect. It also indicates that underwriting measures, such as avoiding exposed clients or requesting enhanced IT security, can reduce risk and capital requirements. Our findings can be used to improve risk management, premium calculation, and regulatory requirements for cyber risk.

The paper is structured as follows. First, the need for new cyber risk dependence models is examined in the literature review. We then propose a model based on a network perspective and discuss how to choose the parameters. After aggregating over the network, we derive and evaluate the loss distribution at the level of the insurer's cyber insurance portfolio. The consequences for pricing, diversification, and capital requirements are discussed. We also present robustness tests for our model and conclude by discussing the consequences for clients, insurers, regulators, and actuarial science.

2 Literature review

The relevant literature originates in two strands: the empirical investigation of cyber risk properties and the theoretical network models. The first strand concentrates mainly on investigating the marginal frequency and severity distribution of cyber risks separately

(collective risk model). The consensus is that cyber risks feature heavy-tailed (Pareto law) severity distribution (e.g., monetary losses, amount of data breached, number of infected computers) (Eling & Wirfs, 2019; Maillart & Sornette, 2010; Wheatley et al., 2016). While it is possible to reliably estimate loss sizes, it is notoriously difficult to estimate the frequency of cyber incidents due to incomplete data (Wheatley et al., 2019).³ Preliminary findings indicate that the frequencies of cyber events are not independent and the rate changes over time (over-disbursed compared to a Poisson distribution) (Edwards et al., 2016). The models used are the beta-binomial (Böhme & Kataria, 2006), negative binomial (Edwards et al., 2016), and Poisson. However, the suitability of such estimations for actuarial applications is questionable. Since they are top down, meaning the frequency is directly estimated on a portfolio or country level, such estimates are not necessarily representative for a small insurer's cyber portfolio. Modeling cyber risk from the bottom up (individual risk model) instead allows for more flexible dependence of frequency (and severity). The few attempts to do so build on correlation (Böhme & Kataria, 2006; Mukhopadhyay et al., 2013) or copulas with stronger tail dependence, such as t-copulas (Böhme & Kataria, 2006), Clayton and Gumbel copulas (Herath & Herath, 2011), and even more flexible copula structures (Eling & Jung, 2018). However, while popular for actuarial modeling and generally more flexible than other models (Staudt, 2010), the copula models do not take the underlining transmission mechanism into account, have a rigid parametric structure, and thus do not describe dependence in cyber risk optimally (Van der Aalst, 2018). By taking all available information into account, network models can significantly improve the understanding of propagation and provide more realistic frequency models. They also allow one to understand the cumulation mechanism and to conjecture extreme events that have not yet been observed (scenarios)

³ The often-used databases for cyber risk (SAS OpRisk by SAS Institute Inc. 2015 and Privacy Rights Clearinghouse 2020) suffer from incomplete data due to reporting and selection biases (Wheatley, Hofmann, & Sornette 2019). The reporting bias occurs if a company has not publicly reported a loss and, thus, it has not been included in the database. Selection bias means that such databases only report events and their severity but not company years with a loss of 0 (more specifically below 100,000, called truncated data; Chernobai et al., 2006) Thus, we do not know the size of the observed sample (or whether it changes over time) and we can only infer the frequency conditional that a company was registered in the database at least once.

The second strand is the literature on network models. Network models have been applied to insurance mainly to model systemic risk and financial assets.⁴ Some research uses networks directly to describe cyber risks, where the network represents the dependence between computers, individuals, or firms (Böhme & Schwartz, 2010; Marotta et al., 2017). However, such research mostly focuses on technical issues or abstract theoretical (game theoretical) arguments (Fahrenwaldt et al., 2018). Purely technical papers use network models to model the spreading of cyber threats and, since networks allow for convenient incorporation of self-protection, analyze optimal IT security investments (Aspnes et al., 2006; Lelarge & Bolot, 2008a, 2008b). Since investments in IT security affect the whole system's security, the main focus is to understand such externalities in the decision making. Several papers extend such endeavors by including the optimal decisions for insurance demand from an individual insurer, client, and societal perspective. The consensus is that if the insurer can observe the client's IT security and charges premiums accordingly, the costs for self-protection can be internalized and optimal IT security can be achieved (Bolot & Lelarge, 2009; Lelarge & Bolot, 2009). Yang and Lui (2014) show that this incentive is strongest for clients with higher centrality. However, if the insurer cannot observe IT security, incentives might vanish and IT security investments become suboptimal (moral hazard) (Schwartz et al., 2010; Schwartz & Sastry, 2014; Shetty et al., 2010). The discussion shows that research to date has concentrated on a technical and theoretical perspective. Only Fahrenwaldt, Weber, and Weske (2018) seem to take an actuarial perspective by proposing a pricing model for malware insurance. Moreover, their model is also unique in that infections are modeled dynamically (infection-spreading model). We use an approach similar to Fahrenwaldt et al.'s (2018) and apply it to a wider range of actuarial applications, such as premium setting, capital requirements, and diversification.⁵

⁴ The network's links then usually represent credit exposures (contractual obligations) between insurers or reinsurers (see, e.g., Kanno, 2016; Lin et al., 2015), the overlapping of the insurer's asset portfolios (see, e.g., Billio et al., 2012), or dependence directly between the insurer's own stocks (see, e.g., Billio et al., 2012). While little evidence suggests that insurers have systemic risk exposure, there is some evidence that large, globally operating reinsurers may be systemically relevant (see, e.g., Kanno, 2016). Thus, underwriting strongly connected cyber risks may increase the systemic threat of the insurance industry, especially if a larger reinsurer is also affected.

⁵ While Fahrenwaldt et al. (2018) use a mean-field approach to approximate moments of the final loss

From an actuarial perspective, the mentioned literature uses unrealistically and oversimplified assumption for the networks. Some papers use degenerated networks consisting of only two agents (Bolot & Lelarge, 2008; Ogut et al., 2005) or two different types of agents (Schwartz et al., 2010) to keep the analyses simple. Also, the network topologies used, such as complete graph (Ogut et al., 2005; Schwartz & Sastry, 2014), star-shaped (Bolot & Lelarge, 2008), tree shaped (Lelarge & Bolot, 2008b), and weakest links (Grossklags et al., 2008), may be appropriate to represent the physical IT infrastructure but not the logical and abstract links in a cyber insurance portfolio. While Fahrenwaldt et al. (2018) also use deterministic networks, they acknowledge that a more realistic model should build on random networks. Only a few papers using random networks, such as the Erdős-Rényi (1960) graph (Lelarge & Bolot, 2008b; Yang & Lui, 2014), and more complex networks, such as scale-free networks, have been endorsed but to our knowledge never analyzed in a cyber insurance context (Böhme & Schwartz, 2010; Van der Aalst, 2018). One reason may be that mean-field approximations are not available for heterogeneous networks and thus are expensive to calculate (Fahrenwaldt et al., 2018). By simulating infection spreading on an empirical-based, scale-free network, we attain a more realistic description of the dependence in an insurer's cyber portfolio.

However, scale-free networks applied to model financial assets and cyber policies can be considered a short position in an asset. Thus, the network's node would represent the assets and the links describe "similarities" such as exposures to a common risk factor (indirect links). Frequently, the correlation between each pair of assets is used as the link's weight (distance). For example, stock markets are characterized by scale-free (heavy-tailed) distributed networks, where a few nodes dominate the whole stock market (Tse et al., 2010). Peralta and Zareei (2016) and Výrost, Lyócsa, and Baumöhl (2019) show how portfolio selection can be improved based on the network topology by over-investing in securities with low centrality⁶ (low systemic risk) that happen to be from old and large firms. Billio et al. (2016) show that networks increase systematic risk exposure and thus reduce the power of diversification. For our purposes, this means that

distribution, we simulate the whole distribution instead. Moreover, we use a static instead of a continuous-time model.

⁶ Centrality measures the importance of a node in a network that is essentially determined by the strength of the node's connectedness (number of connections and connections to highly connected nodes).

networks grow and produce old and large nodes (e.g., the Barabási and Albert model; 1999), insurers should seek cyber exposure at the network's periphery, policies with higher centrality should be charged higher premiums, and the reduced diversification potential might deter insurers from underwriting cyber risk in the first place.

3 Methodology

We assume an insurer holds a number of cyber insurance policies in an underwriting portfolio. To derive the aggregated distribution for the portfolio, we build on the individual risk model (Panjer & Willmot, 1992).⁷ The individual risk model allows one to account for each risk's characteristics (micro or bottom-up perspective) and thus uses the information contained in the network structure. A cyber underwriting portfolio shall consist of n risk. We argue that the loss for each risk $j \in \{1, \dots, n\}$ is the combination of a Bernoulli distributed variable $I_j \in \{0, 1\}$ and a severity variable $Z_j \in \mathbb{R}$. $I_{j,0} = 1$ indicates that policy j registers a loss and $I_{j,0} = 0$ indicates no loss. Z_j models the loss amount if a loss occurs. For all nodes combined, we can write in vector notation $\mathbf{I} \in \{0, 1\}^n$ and $\mathbf{Z} \in \mathbb{R}^n$, both n -variate, generally not identical and independently distributed (iid), random variables. The portfolio loss is then (sum over the combined loss of all policies):

$$X = \mathbf{I}^T \mathbf{Z}. \quad (1)$$

While $\mathbf{Z}$ describes the severity distribution of the losses, $\mathbf{I}$ models the dependency between each node and, when aggregated, yields the frequency of portfolio losses. Thus, we call $\mathbf{I}$ the frequency or dependence model. Research to date has concentrated on understanding $\mathbf{Z}$ and reliable estimates already exist (Eling & Wirfs, 2019). Thus, we do not focus here on $\mathbf{Z}$ and assume some homogeneity in $\mathbf{Z}$. On the contrary, modeling $\mathbf{I}$ is less researched since, as discussed above, the frequency of cyber losses is generally difficult to estimate due to incomplete data (Wheatley et al., 2019). In principle, different models for $\mathbf{I}$ are possible and thus $\mathcal{M}$ denotes the set of different dependence models. In the following, we propose a model for $\mathbf{I}$ based on a network approach that fills the empirical gap of frequency modeling.

To model the spreading of cyber threats, we build on the network epidemic approach

⁷ The model traditionally used in modeling insurance risks is the so-called collective risk model (e.g., compounded Poisson distribution).

that distinguishes between network topology and the spreading dynamics (Pastor-Satorras & Vespignani, 2001). The network topology provides the information regarding policyholders being in contact with each other and the spreading (or epidemic) model defines the dynamics of how the infection spreads on the network topology over time. This separation enables incorporating flexible complex network topologies.

First, we represent an insurer's portfolio and connections between its policyholders by a network topology. Using the actuarial definitions of Equation (1) in network terms, the policies in the insurer's portfolio $j \in \{1, \dots, n\}$ are called nodes, n is the size of the network, and "potential correlations" are the links between nodes. In the following, we use both terminologies: the network terminology for the technical discussion of networks and the actuarial terminology to discuss the results at the portfolio level. Formally, a network topology is defined as a set of links as represented by the adjacency matrix $\mathbf{A} \in \{0,1\}^{n \times n}$, where $a_{i,j} = 1$ indicates a link and $a_{i,j} = 0$ indicates no link between node i and j .⁸ We are interested in any link that allows for the transmission of different cyber threats (see Table 1). Indeed, cyber threats use a whole stack of networks layers, such as the physical infrastructure (connected routers and servers), communication protocols (IP, universal resource locators (URLs), phone calls, email), and services (cloud computing and social media). The latter two are called information networks, meaning the links describe proximity in an informational sense (as opposed to spatial networks where the links represent physical distance). However, note that links can even represent "similarities" between the connected nodes, like the same IT security vulnerabilities, without any causality.

Network topologies $\mathbf{A}$ can be modeled in several ways. Since we do not know the exact portfolio structure of a specific insurer, it is sensible to generate the network randomly.⁹ Thus, we assume that the number of each node's links, called the degree K , is

⁸ We impose several assumptions on $\mathbf{A}$. First, the graph is undirected, meaning $a_{i,j} = a_{j,i} \forall i, j$ ($\mathbf{A}$ is symmetric). Second, we exclude self-interacting nodes, $a_{i,i} = 0, \forall i$. Third, there is no weighting for the strength of the links. While these assumptions do not necessarily reflect reality, they are often made as approximations (see, e.g., Fahrenwaldt et al., 2018). An insurer with more detailed information about the connections between policies might be able to relax some of these assumptions.

⁹ Since the sales personnel do not have a complete picture of the overall exposure of the insurance company, they cannot strategically select risks according to their interdependencies. As a result, the network is generated by random processes. If an insurer has more information, it could model the

distributed as $f(k)$ with an average of $\bar{k}$. Frequently, the links in real networks are not homogeneously distributed but tend to cluster at certain nodes (Barabási, 2016). One class of networks, which describes many real-world networks such as the Internet, router networks, email, and phone calls, is the scale-free network (Böhme & Schwartz, 2010; Tse et al., 2010; Yang & Lui, 2014).¹⁰ Scale-free networks feature power law distributed links (i.e., $f(k) \sim k^{-\alpha}$), where α is the degree exponent (Barabási & Albert, 1999). Smaller α means the links are more extremely distributed, but normally it is assumed that $\alpha > 1$ since for smaller values networks become unstable. The literature suggests that for cyber-related networks α should be between 2 and 4 (see Table 1; Barabási 2016). We use $\alpha = 3$ since this conveniently describes the Barabási-Albert (BA; 1999) model.

By describing how networks build up over time, the BA model provides an algorithm to simulate scale-free networks.¹¹ The BA algorithm is based on the idea of growth and preferential attachment. As the network grows over time, each new node preferentially connects to one that already has a lot of links (rich-get-richer or first-mover advantage). For example, most people are familiar with popular services like Google and Facebook but have never heard of millions of other web pages. The result of the BA algorithm is a network characterized by high clustering, hubs (unusually strongly connected), and ultra-small-world properties (see, e.g., Appendix A, Figure A1). The latter describes a network where only a small number of links (steps) connect (and eventually infect) any two nodes. The hubs in an underwriting portfolio may be ordinary companies with exceptionally strong reliance on IT, such as financial services, or critical IT companies, such as cloud services (e.g., Dropbox), social media (e.g., Facebook), software providers (e.g., Microsoft), and critical infrastructure providers (e.g., Cisco, air traffic systems,

network deterministically.

¹⁰ Other networks have been suggested to model cyber-related networks, such as random networks (Erdős & Rényi, 1960) and small-world networks (Watts & Strogatz, 1998). Since these models feature exponentially bounded degree distribution, they contradict the empirical properties.

¹¹ Subsequent extensions, such as the fitness networks (see, e.g., Bianconi & Barabási, 2001), try to capture an even better picture of the network's evolution over time. However, more complex models come at a cost in terms of additional parameters and parameter uncertainty. Since we are only interested in the final state and not how the network evolves over time, we stick to the more parsimonious model.

central clearing counterparties¹²). However, hubs can also simply describe larger companies that are more strongly interconnected. For an insurance portfolio, we expect these properties to lead to heavy-tailed frequency distribution (thus, Poisson and negative binomial might not be appropriate). Table 1 compares the empirical properties of cyber-related networks with the property of our simulated BA network.

Table 1. Cyber network properties

Network	Nodes	Links	$\bar{k}$	$\overline{k^2}$	α	NT
Internet	Routers	Internet connections	6.3	240	3.4	SW
WWW	Webpages	Links	4.6	482	2.2	USW
Mobile phone	Subscribers	Calls	2.5	12	4.9	SW
Email	Email addresses	Emails	1.8	500	2.7	USW
Power grid	Power plants, transformers	Cables	2.7	10	Exp.	SW
Simulated	Cyber policies	Contacts	3.9	37	3.0	(U)SW

Note: The first part of the table is adapted from Barabási (2016) and summarizes empirical findings on cyber-related networks. $\bar{k}$ is the average degree, $\overline{k^2}$ the second moment of degree, and α is the exponent of the power law degree distribution (“Exp.” means exponentially distributed degree, i.e., less heavy-tailed than the power law). All statistics are averages between incoming and outgoing links. The small-world (SW) property is defined as the average shortest distance between any two nodes growing proportionally to $\ln(n)$ and the ultra-small-world (USW) is where the average path length grows as $\ln(\ln(n))$.

While network **A** serves as the structure on which cyber threats spread, we also need to define the spreading properties (epidemics). Transforming the definitions in Equation (1) into epidemic terminology, the occurrence of a loss is called “infection” and the loss state I_j is equivalent to the infection state, where if node j is infected, $I_{j,0} = 1$, and if not,

¹² An illustrative example would be the Bangladesh Bank heist in 2016 (see, e.g., Kitten, 2016). Hackers used the international payments system, SWIFT, to steal US\$81m from the NY Federal Reserve Bank. The federal reserve bank, as a central counterparty (CCP), and the SWIFT system can both represent hubs in the inter-banking network. Such hubs can cause risks to be correlated and to accumulate in an insurer’s underwriting portfolio.

$I_{j,0} = 0$. First, we need to define how the whole network is initially infected, denoted as $\mathbf{I}_0$. We assume that initially the number and exact choice of infected nodes is random, where every node in the network is initially infected with a probability p_0 . Therefore, $\mathbf{I}_0$ is iid multivariate Bernoulli distributed and the number of infected nodes (sum over $\mathbf{I}_0$) is binomial distributed. Each initial infection can be interpreted as one threat that affects several policies simultaneously or as a different threat (e.g., different malware).

The subsequent spreading, for $t > 0$, is then recursively modeled as the transition probability $p_{t,j}$ of each healthy node j becoming infected, $I_j: 0 \rightarrow 1$. The transition probability $p_{t,j}$ is determined by the probability that an infected node infects a healthy one, the so-called contagion probability $q(t)$, multiplied times j 's number of previously infected nearest neighbors $\mathbf{a}_j \mathbf{I}_{t-1}$. In matrix notation, the vector of transition probability is:

$$\mathbf{p}_t = q_t \mathbf{A} \mathbf{I}_{t-1}. \quad (2)$$

The contagion probability $q(t)$ is assumed to be homogenous, meaning that every healthy node has the same chance to be infected by an infected neighbor.¹³ Moreover, we assume $q(t)$ decays over time, $\frac{dq(t)}{dt} < 0$ (called the finite contagion time model; see Appendix B for the definition of the contagion function). Since $q(t)$ is decaying, the infection state of the network eventually stabilizes over time, denoted by T . Since the claim-settling process usually takes much longer than the spreading, we are only interested in the final infection state $\mathbf{I}_T$.

Due to the interactions in the network, the distribution of $I_{j,t>0}$ is heterogeneous, meaning it is potentially different for each node j depending on the position in the network. Consequently, $\mathbf{I}_{t>0}$ is generally not iid multivariate Bernoulli distributed and the number of infected nodes is no longer binomial distributed. Instead, the exact distribution of $\mathbf{I}_{t>0}$ is unknown and, thus, we need to simulate $\mathbf{I}_{t>0}$ by drawing each time new realizations for the network $\mathbf{A}$, the initial infection state $\mathbf{I}_0$, and the spreading process (Equation 2).

¹³ The contagion probability might also depend on the IT security measure, s , taken by clients, $q(\mathbf{s})$. While we do not consider $\mathbf{s}$ here, it would be a natural extension of the model if an insurer possesses such kind of information.

4 Parameter choice

Even though network models are flexible and describe reality well, it is challenging to estimate reliably the network's parameters. Table 2 summarizes the different parameters required here, how we set them, and from where the estimates are taken. The table also reports our qualitative assessment of how uncertain and sensitive our final results are to each parameter. If a parameter is uncertain and the results are sensitive to it, we subject this parameter to robustness analyses, as described in the second part of the paper.

The first group of parameters govern the network topology. We set the network size n to 50 nodes (Eling & Schnell, 2019; Fahrenwaldt et al., 2018) and by that we acknowledge that the cyber insurance market is still rather small. It is important to note that size is not a critical parameter since the connectivity and the spreading behavior are fundamentally independent of the network size. The network size does not influence the spreading speed or the final infection rate in a scale-free network (Leveille, 2002). Thus, results for the baseline size can be extrapolated to larger portfolios. However, the smaller the network, the more the simulated degree distribution deviates from the theoretical one. Consequently, smaller networks have accentuated simulation errors that need to be compensated by more simulation runs. As shown in Appendix C, we find that the 1,500 runs produce stable results for the statistics of interest.

Table 2. Parameter choice

	Variable		Value	U,S	Source
Network	Network size	n	50	+,0	Eling & Schnell (2019)
	Average number of links	$\bar{k}$	3.9	+,+	Table 1
	Degree exponent	α	3.0	0,+	Table 1
Spreading	Initial infection probability	p_0	0.02	++,++	Simulations (Appendix B)
	Contagion probability	q_0	0.20	++,++	Simulations (Appendix B)
	Final infection rate	p_T	0.27	0,++	Literature (Appendix B)
Others	Correlation	ρ	0.18	+,+	Böhme & Kataria (2006)
	Expected loss	$E(Z)$	US\$ 43m	0,0	Eling & Wirfs (2019)

Note: U stands for the uncertainty in the estimated parameter and S for the sensitivity of our results with respect to this parameter. 0, +, ++ mean unproblematic, problematic, and very problematic, respectively.

The other parameters of the network topology that govern the degree distribution are discussed above. Both the average number and distribution (degree distribution) of links are critical for the outcome and their estimates are quite reliable. The average number of links increases the infection speed and rate since more links mean higher transition probabilities (Equation 2). Heavier tailed degree distribution (lower degree exponent) would yield more extreme outcomes as some infections tend to die out and others infect the whole network.

The second group of parameters determines the spreading behavior of cyber threats. Generally, the parameters that rule the micro dynamics of the spreading, p_0 and q_0 , are difficult to observe. It is easier to find reliable estimates for the final infection rate p_T and then work backward. However, why is a network model required if we can work directly with the final infection rate? The true value of a network model is not in providing a better estimate for the final infection rate but rather in providing the distribution of the final infection rate. Thus, we first fix the final infection rate and the spreading model then yields possible solutions for the space of p_0 and q_0 (see Appendix B). If one of the two parameters is fixed, we get a unique estimate for the other. Since both p_0 and q_0 are not only difficult to observe but also greatly influence the results, we subject both to extensive sensitivity analyses. We find that our results are more sensitive to the initial infection probability than the contagion probability. Note that the contagion probability is equivalent to the average number of links. If an infection spreads on twice as many links but with half the contagion probability, then, *ceteris paribus*, the outcome is the same. Thus, the sensitivity analysis for q_0 can also be considered a sensitivity analysis for $\bar{k}$.

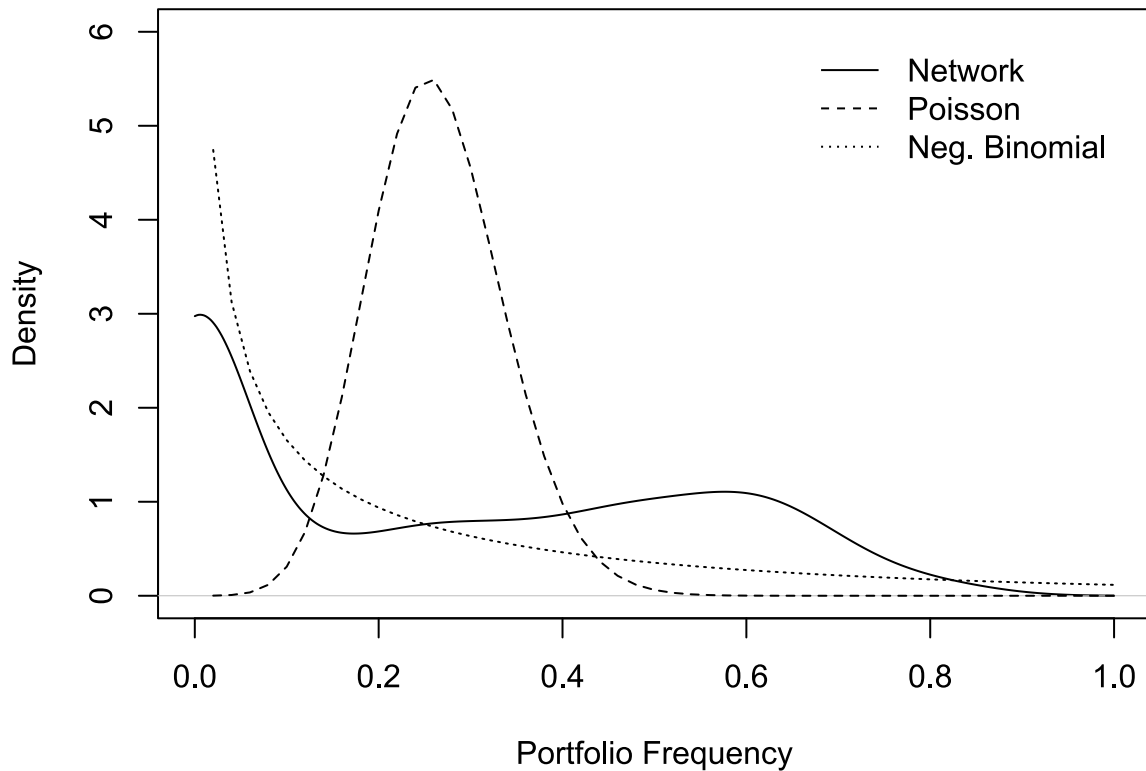
Finally, we compare the outcome for the network with a linear dependence model, where the correlation is set to 0.18 between each node. The severity of losses is assumed to be fixed and homogenous and is set as the expected loss $E(Z)$.

5 Results

First, we simulate the loss frequency (i.e., final infection rate in network terms) of the insurance portfolio P_T . Theoretically, the infection rate distribution is defined as the sum of each risk's infection state, $P_T = \mathbf{w}^T \mathbf{I}$, where $\mathbf{w} = \frac{1}{n}$. The distribution is then estimated by simulating $\mathbf{I}$. Figure 1 shows the simulated distribution of $P_{T,i}$ for the network model

and other dependence models $i \in \mathcal{M}$. The frequency distribution for the network model consists of two peaks, as sometimes there is no infection at all ($\hat{p}_T = 0$) and sometimes it converges toward a higher stable level ($\hat{p}_T = 0.6$). In effect, the frequency distribution is heavy-tailed and convex in the midrange. The expected portfolio frequency is $p_T = E(P_T) = E(\mathbf{w}^T \mathbf{I})$. When we take the average over all simulations, we get an estimate for the final infection rate $\hat{p}_T = 0.27$ (see Table 2).

Figure 1. Distribution of cyber portfolio loss frequency



Note: The figure shows the simulated distribution of the insurer's portfolio loss frequency. The frequency of the network model is compared to the Poisson and negative binomial distributions. The parametric distributions are estimated by means of maximum likelihood. The network's frequency density is estimated by applying a Gaussian kernel to the simulated data. For illustrative purposes, the frequency is assumed to be approximative continuous while in effect there is a tick size of n^{-1} .

We compare the network frequency to distributions that have been endorsed for modeling the aggregate frequency of insurance and especially cyber risks. These models are called collective risk models since they directly attempt to model the frequency for the whole portfolio (see, e.g., Kuon et al., 1993). The consequence is that these models assume independent and identical distributed frequencies (clearly not the case in a network) and allow for less rich dependency structures. The most often used distributions are the

Poisson and the negative binomial (NB) distribution (Edwards et al., 2016). Figure 1 shows that both parametric distributions underestimate the probability for medium to high frequencies; the Poisson performs especially badly. This is not surprising since the Poisson distribution is the limiting distribution of the sum of iid Bernoulli's, an assumption violated by the network model.¹⁴ The frequencies of different nodes, however, are clearly dependent and not identically distributed. Since the Poisson is the limiting distribution of the binomial distribution, this finding also holds for the binomial distribution. The NB distribution in turn performs better because of the separation of the mean and variance parameters. Dependence in the infection rates of different nodes can be accounted for by a higher variance of the NB (see, e.g., Wang, 1998).

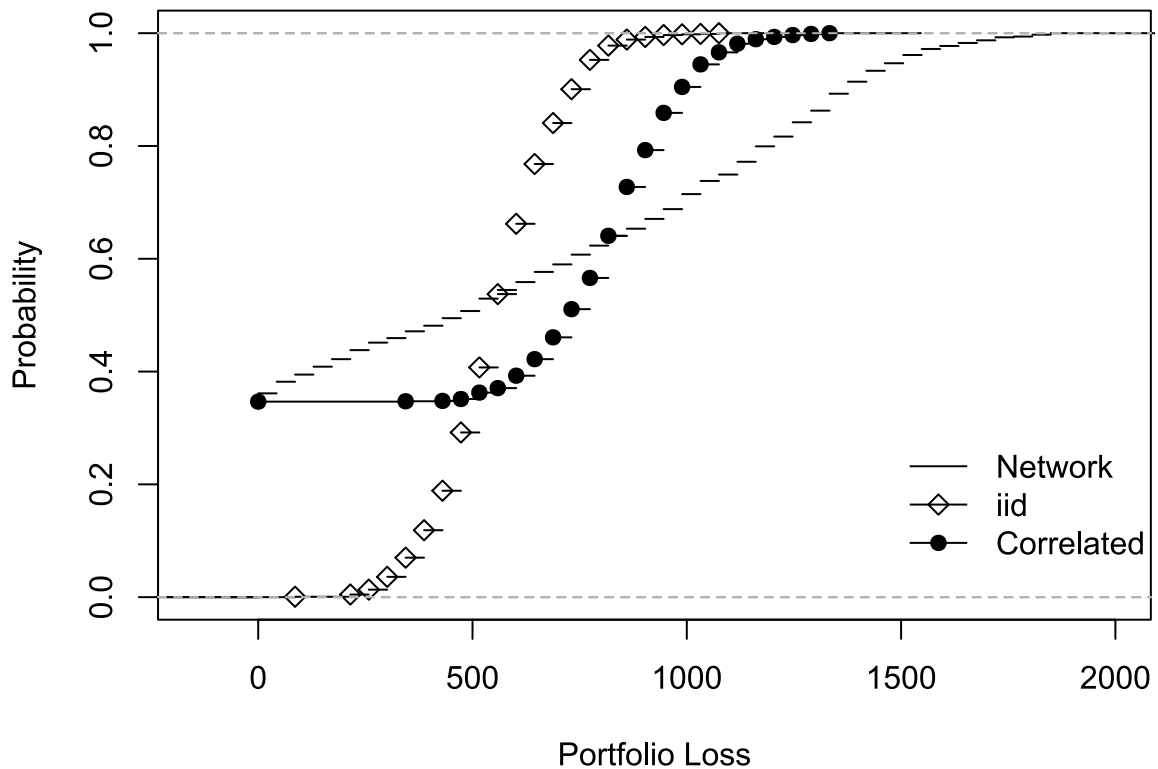
Instead of approximating the aggregated portfolio frequency directly (collective risk model), we can also compare the network frequency to the frequency distribution produced by different copulas. While copulas with strong tail dependence such as the Gumbel copula can produce heavy-tailed frequencies, they fail to replicate the bimodal (two peaks) distribution observed in the network (see Appendix E). This can be explained by the fact that Archimedean copulas generally use only one dependence parameter and thus fail to account for the network's heterogeneity (link distribution). To conclude, if the network model captures at least part of the real processes at work, standard parametric frequency distributions and copula models cannot describe cyber risks in an insurer's portfolio appropriately. The interactions in the network are too complex and thus can hardly be captured by a rigid and sparse parametric model.

When we combine, as in Equation (1), the network's frequency distribution I_i with the severity distribution Z , we attain the distribution of the aggregated cyber portfolio loss, X_i , for different dependence models $i \in \mathcal{M}$. Figure 2 shows that the portfolio distribution based on the network is heavier tailed than the distribution based on iid or linear correlation model. Thus, we find that the frequency distribution generated by networks

¹⁴ Since the initial infection is the sum of Bernoulli trials, we attain a binomial or an approximation of a Poisson (or normally distributed frequency) if there are no further infections. For both approximations, the number of nodes is too small. Moreover, the infectability following the initial infection leads to complex interactions and causes the final distribution to deviate from these distributions. A homogenous network has similar effects as one of the central limit theorems is observed (despite the dependencies) and the final infection rate can be approximated by a normal distribution (Van der Aalst, 2018). However, under the heterogenous assumptions here, this approximation is not viable.

indeed reinforces the heavy-tailed severity distribution already observed (Eling & Wirfs, 2019).

Figure 2. Distribution of cyber portfolio loss



Note: The figure shows the simulated cumulative loss distribution of an insurer's portfolio. The network loss distribution is compared to the distribution for the iid and linear correlated frequency models. The loss is in mUS\$.

Next, we apply several statistics to evaluate the distribution of the underwriting cyber portfolio. First, we investigate the effect our model has on the insurance premium π . For that, we assume that the insurer is risk averse, meaning the premium is calculated as the expected loss plus a loading for the (portfolio) risk. Risk aversion is natural to assume for insurance companies for three main reasons. First, employees may be laid off if the company performs badly and it would lose part of its human capital. Thus, employees that may lose their job would be risk averse in their decision making. Second, regulatory frameworks increase costs for taking too much risk. Finally, the quality of insurance critically depends on the safety of the insurance company. The higher the probability of bankruptcy, the lower clients' willingness to buy products. A utility model allows for incorporating risk aversion and we calculate the premium as the certainty equivalent of the portfolio's loss X_i :

$$\pi_i = \frac{U^{-1}E(U(X_i))}{n}, \quad (3)$$

where the utility function is concave in the losses and $i \in \mathcal{M}$ indexes the different models. We use the exponential utility that gives rise to the frequently used exponential premium principle (see, e.g., Denuit et al., 2006). The exponential utility is governed by the absolute risk aversion that we set at 0.005.¹⁵ We derive the absolute risk aversion parameter by requiring that the premium according to Equation (3) produce a loss ratio $\frac{E(X)}{\pi}$ that is consistent with the observed data. We choose a loss ratio of 0.7 (see, e.g., OECD, 2020).

Second, our results have profound consequences for regulatory capital requirements and risk management. Thus, we also calculate the frequently used risk measures, value at risk $VaR_q(X_i)$ and tail value at risk $TVaR_q(X_i)$. The confidence level of the VaR is chosen according to the Solvency II requirements $q = 0.995$ (EC 2015) and the $TVaR$ is based on the Swiss Solvency Test $q = 0.99$ (Bundesamt für Privatversicherungen, 2006). Both risk measures have advantages and disadvantages for describing cyber risks. The $TVaR$ can be considered the average of a percentage of worst-case scenarios (such as the financial crisis). Thus, $TVaR$ is more sensitive to the tail distribution and accounts better for heavy tails as observed here for the cyber risk frequency distribution. The VaR in turn is less sensitive to the tail distribution. This is an advantage whenever the observations in the tail are sparse and thus the tail distribution estimate is highly uncertain. The VaR is a more robust estimator and performs better out of sample. In our model, this would mean that the VaR should be less sensitive toward both the network inherent risk and modeling uncertainty (parameter choice). Thus, whether the VaR or $TVaR$ is preferred for a network approach to cyber risk is a matter of trade-off between model uncertainty and taking extreme events properly into account. Being more confident about the network model representing the real processes properly demands use of the $TVaR$.

Finally, to compare our findings with regulatory frameworks, we retrieve risk factors.

¹⁵ The exponential utility function is defined as $u(x) = \frac{1-e^{-ax}}{a}$, $a > 0$ and a describes the absolute risk aversion. The certainty equivalent (Equation 3) for the exponential utility simplifies to $\pi = \frac{1}{a} \ln(E(e^{ax}))$.

Risk factors are convenient since they are measures relative to the business volume and thus can be compared easily and extrapolated to different portfolio sizes. We concentrate on Solvency II but acknowledge that the US risk-based capital framework is very similar and the results also apply. The simplified capital requirement, cr , is defined as (EC 2015):

$$cr_i = 3 \cdot s \cdot E(X_i), \quad (4)$$

where s is the risk factor defined by the regulator. Since no s is specified specifically for cyber risk, we need to consider risk categories that the regulators consider to cover cyber risk. In previous work, we calculate a risk factor for underwriting the cyber risk exposure of $s = 0.14$ (Eling & Schnell, 2019).¹⁶ Now we can compare this value to the risk factor implied in our network model, $\hat{s}$. For that, we build on the fact that the regulator aims at a survival probability of 99.5%; thus, $cr = VaR(X_i) - E(X_i)$. After some transformations, we can retrieve an estimate for $\hat{s}$ for each dependency model $i \in \mathcal{M}$:

$$\hat{s}_i = \frac{VaR_{99.5\%}(X_i) - E(X_i)}{3 \cdot E(X_i)}. \quad (5)$$

Table 3 shows the different statistics, expectations, premiums, VaR , $TVaR$, and risk factors for different dependency models.

Table 3. Statistics of cyber portfolio loss

Model i	μ	π	$VaR_{0.995}$	$TVaR_{0.99}$	$\hat{s}$
iid	11.4	12.4	946	989	0.05
Linear correlation	11.1	16.5	1'247	1'277	0.17
Network (baseline)	11.4	23.5	1'806	1'814	0.39
Systemic institution	18.2	29.8	1'935	1'978	0.45
Pandemic	29.9	33.4	2'021	2'042	0.48

Note: The table reports the statistics for different frequency models i . μ stands for the mean, π for the premium, VaR for the value at risk, $TVaR$ for the tail value at risk, and $\hat{s}$ for the risk factor. The numbers are in mUS\$.

Since the mean of the sum of individual risks (whether dependent or not) is equal to the

¹⁶ This derivation contains several aggregations over different risk categories and consideration of correlation and diversification. Moreover, we simplify by assuming that the volume measure is identical to the expected value, $E(X_i)$.

sum of the means, iid, linear correlation, and network have the same mean (neglecting minor simulation errors). Despite that, the linear correlated and network risk are more extremely distributed. This is the reason why the (risk) premium, the VaR , and $TVaR$ are larger for the correlated risks and even larger for the network model. Diversification reduces risk less in a network model and thus the risk loading is higher (the models are calibrated so that they have the same expectation). To conclude, a risk-averse insurer charges higher risk premiums if its calculations are based on the network model. Whether the client is willing to pay this additional premium is an open question. Similarly, the survival probability is lower and the loss considering default is higher for the network model given a certain capital endowment because the risk factor suggests that more capital is needed due to the network dynamics. The next question we address is the reliability of this finding.

5.1. Sensitivity analysis

As discussed above, we identify the initial infection probability, p_0 , and the contagion probability, q_0 , as the most uncertain and influential parameters and thus subject them to sensitivity analyses. For this purpose, we define a broader plausible range for the two spreading parameters around their point estimate, $PQ = \{(p_0, q_0) \in \mathbb{R}^2 \mid 0.01 < p_0 < 0.04, 0.05 < q_0 < 0.4\}$. Table 4 shows the expected semi-elasticity of our risk measures for the baseline model with respect to p_0 and q_0 , where the expectation is taken over the whole parameter space PQ .¹⁷

Table 4. Sensitivity to infection and contagion probability

Elasticity	μ	π	$VaR_{0.995}$	$TVaR_{0.99}$	$\hat{s}$
$\hat{\varepsilon}_{p_0}(\cdot)$	35.7	13.9	5.2	6	8.8
$\hat{\varepsilon}_{q_0}(\cdot)$	6.4	6.3	3.3	3.8	5.7

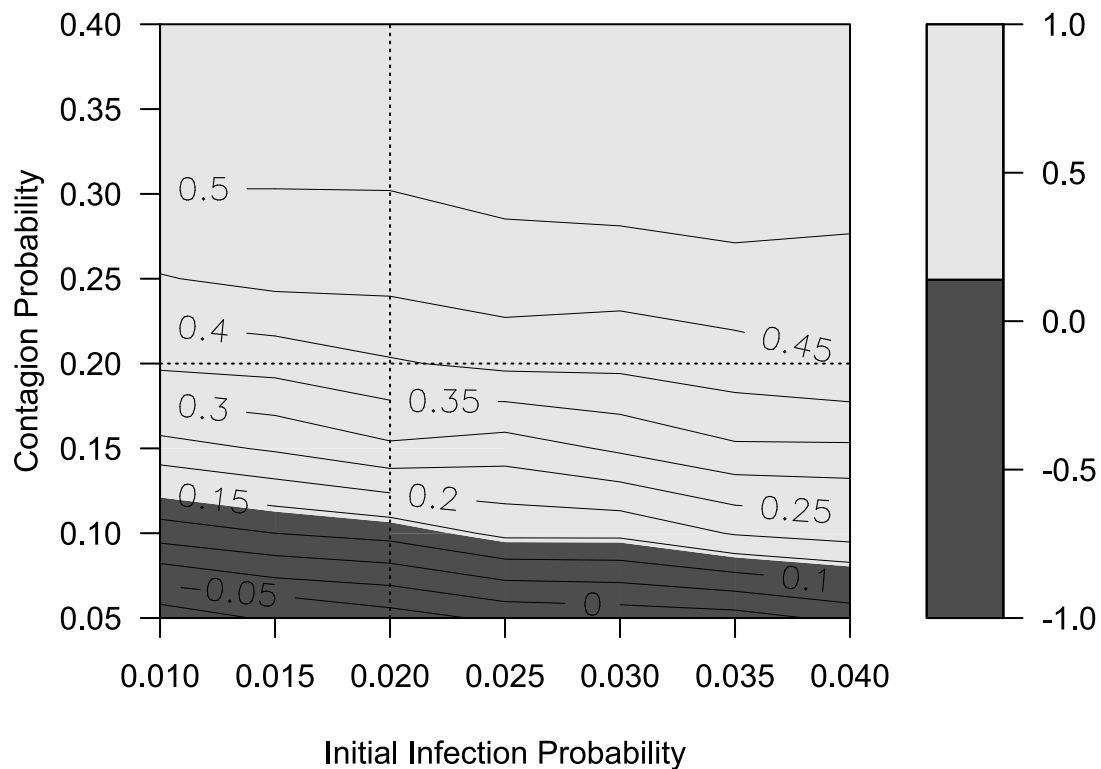
Note: The table reports the expected semi-elasticity of the different statistics with respect to p_0 ($\hat{\varepsilon}_{p_0}$) and q_0 ($\hat{\varepsilon}_{q_0}$) for the baseline model. μ stands for the mean, π for the premium, VaR for the value at risk, $TVaR$ for the tail value at risk, and $\hat{s}$ for the risk factor.

¹⁷ Formally, we define the mean semi-elasticity as $\varepsilon_x(\cdot) = E\left(\frac{\partial \ln(\cdot)}{\partial x}(p_0, q_0)\right)$ and approximate with the sample average $\varepsilon_x \approx \hat{\varepsilon}_x$.

For example, the risk factor increases by 8.8% and 5.7% if p_0 and q_0 increase by 100 points (e.g., from 4% to 5%), respectively. Generally, the results are more sensitive to the initial infection probability than the contagion probability. Moreover, the VaR , the $TVaR$ and the risk factor are less sensitive to changes in both spreading parameters than the mean and the premium. This is because there is a limit to how many nodes can be infected (i.e., the total number of risks) and the frequency distribution is truncated at 100%. Consequently, our estimates for the capital requirements (VaR , $TVaR$, risk factor) are more reliable than the one for the mean or premium.

To fully understand the consequences for the risk factor, Figure 3 shows the risk factor for the whole parameter space PQ (see Appendix D for the other statistics). The regulatory risk factor is only sufficient if the contagion probability and the initial infection probability are sufficiently small. In particular, the contagion probability needs to be very small; for $p_0 = 0.02$, this would mean $q_0 < 0.08$ and $p_T = 0.09$. It is interesting to note that the trade-off between the initial infection probability and contagious probability features diminishing returns (the results for the contagion probability also apply to the average number of links since the two parameters are equivalent). Regulators can use Figure 4 to derive new risk factors for cyber risk underwriting based on their (changing) expectation about the spreading parameters.

Figure 3. Sensitivity of the risk factor



Note: The figure shows the risk factor contours for the parameter space, PQ. The dark grey represents the area where the regulatory risk factor exceeds the risk factor required by our model. All other parameters are set as in the baseline model (Table 2).

5.2. Pricing

Instead of using a flat-rate premium as calculated in Equation (3), the heterogeneity of risks exposed to a network calls for premium differentiation and also provides clues on how this can be achieved. Ideally, an insurer differentiates the premium according to the client's riskiness since the consequences of a lack of price differentiation are moral hazard, adverse selection, and eventually market failure. A distorted premium might cause inefficiencies, such as too much or too little investment in IT security. From the insurer's perspective, price differentiation is also relevant to meeting capital requirements and financing capital costs fairly. In our model, the riskiness of each client from an individual perspective is determined by the infection probability. However, an insurer also cares about how often a policyholder infects others in the portfolio and a pricing scheme that internalizes such costs is preferred. Several factors influence the client's risk, including size, industry, IT security measures, and data sensitivity. However, it should be possible for an insurer to survey the relevant information that can be used to approximate the risk.

In our model, a substantial part of such risk factors can be approximated by the measures of centrality. The simplest centrality measure is the relative number of links a node has, but more sophisticated measures also consider how many links the node's neighbors have (second- and higher order links). Higher centrality in general is associated with higher returns for financial assets, and it can be regarded as a systematic risk factor that cannot be diversified. To see that, we adapt Billio et al.'s (2016) extended asset pricing model $\pi = E(X) + \beta \cdot f + \epsilon^*$; thus, the premium is the expected value, plus a systematic component $\beta \cdot f$ and error terms ϵ^* . The systematic component is neglected here since cyber risks are only weakly related to systematic factors. The extension of Billio et al.'s model is that it allows for network interactions, described by $W(A)$, in the idiosyncratic shocks ϵ and thus losses of each node $\epsilon^* = W \cdot \epsilon$ are no longer independent and identically distributed. Because of the network's interaction, idiosyncratic shocks propagate and an endogenously systematic risk component emerges. As this network exposure component cannot be diversified, it is relevant for pricing (see, e.g., Richmond, 2019).

The relationship between the network A and the weighting is $W = (1_n - \lambda A)^{-1}$, where λ captures the response of one node to losses in other nodes. When the error vector is set to 1, we can recover the Katz (1953) centrality vector $c = W1$. Thus, here, the Katz centrality can be regarded as a natural measure for the network centrality. We choose $\lambda = 0.18$ as the largest eigenvalue λ_{max} of A (called the eigenvalue centrality). We define a linear premium model dependent on each node's centrality c (see, e.g., Ahern, 2013):

$$\pi(c) = \mu + rp + \beta_c \cdot c, \quad (6)$$

where $\mu = E(X)$ and $rp = E(\pi) - \mu$. The premium is separated into three different components. The first component is the expected loss. The second is the expected risk premium, rp , due to the risk aversion (with respect to absolute risk not the systemic risk factor models imply). Third, β_c is the factor price of the network exposure. We can also represent the linear model actuarially with proportional loadings on the expected value (see, e.g., Zweifel & Eisen, 2012, p. 219):¹⁸

¹⁸ For $rp^* = \frac{rp}{\mu}$ and $\beta_c^* = \frac{\beta_c}{\mu}$, Equation (7) results.

$$\pi(c) = (1 + rp^* + \beta_c^* \cdot c) \cdot \mu. \quad (7)$$

The factors in Equation (7) are now defined relative to the expected value. β_c^* is again the loading for the network exposure. We estimate Equation (6) and derive the risk factors in Equation (7) by regressing the fair premium π (Equation 3 applied to each node individually) on the standardized c :

$$\widehat{rp}^* = 1.1, \widehat{\beta}_c^* = 0.30, \text{ and } R^2 = 0.95$$

The model explains a substantial proportion of the variation in the premium (the rest being uncertainty from the simulations of the initial and global infection probability), and centrality c is significantly positively priced. We also calculate the elasticity $\frac{\partial \ln(\pi)}{\partial \ln(c)}$ by estimating the log-log model of Equation (6). The elasticity is 0.44. A 10% increase in the infection probability or riskiness would mean the insurer should charge 4.4% more in premiums. If riskier clients not only have higher infection rates but also tend to feature higher losses, the premium would react more strongly. To conclude, the infection probability has a strong effect on the fair premium and should be considered in pricing cyber policies.

As discussed above, another important factor for calculation of the fair premium is the IT security a client has in place. This influences the node's infection probability $q_t(s)$ as well as how often the node infects others. If links are directed, certain nodes may be infected frequently but rarely infect others. Such a node's effort not to infect others can be internalized by a discount on the premium according to Equation (6). The insurer's clients would then not only invest in IT security for their own sake but, motivated by the discount, also on behalf of the insurer's whole portfolio.

5.3. Diversification

The network model also has implications for the diversification. Under the classical assumption of expected utility and thin-tailed risk (without any frictions), diversification is always optimal even if the risks are correlated. The benefits from diversification enable the insurance industry to provide risk transfer for a price that consumers are willing to pay and generates welfare gains for society. However, Ibragimov, Jaffee, and Walden (2009) point out that diversification might not be optimal if we deviate from the classical assumption, such as heavy-tailed distributions and nonlinear dependence. For financial assets, network dependencies reduce the diversification benefits (see, e.g., Billio et al.,

2016). Here we extend the findings of Ibragimov et al. (2009) by showing that diversification also might not work as expected when the frequencies are generated by our network model. For that, we apply the expected utility of the insurer's payoff for different portfolio sizes n :

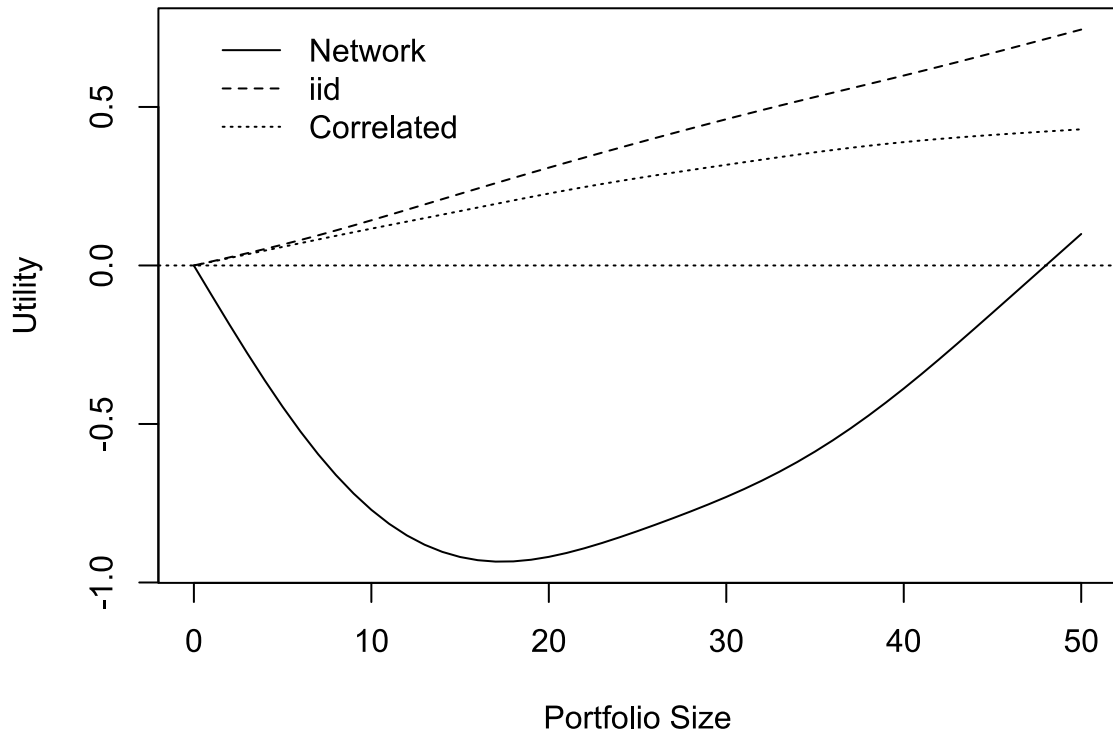
$$u_{i,n} = E \left(U(k + \mathbf{1}_n^T \pi_i - X_{i,n}) \right), \quad (8)$$

where we use the isoelastic utility with a relative risk aversion parameter of 0.97 (Ibragimov et al., 2009).¹⁹ The term in the inner bracket is the aggregated payoff of the insurer, consisting of the initial capital endowment plus the premium payments minus the losses on the policies. The premium is derived by applying Equation (3) to the loss distribution of one policy.

Figure 4 shows the insurer's utility in pooling risks for different dependency models. The figure shows that for the iid and linear correlation models the results are as expected. As the portfolio size increases, diversification reduces risks and the utility of the insurer increases. Also, as expected, the merit of diversification is less for correlated risk than for iid risk. For the network model that features nonlinear correlation (or convex frequency distribution, see Figure 1), things are different. For the specific parameters used here, we have a so-called local diversification trap. This means that for small portfolios diversification actually increases risk and thus the utility decreases. After the portfolio reaches a minimum size (here 48 risks), diversification again yields benefits. If the insurer cannot reach a critical portfolio size or if it takes time to build such a portfolio, the insurer will never choose to underwrite cyber risk in the first place. As a consequence, the market might not develop at all.

¹⁹ The isoelastic utility function is defined as $u(x) = \frac{x^{1-\eta}-1}{1-\eta}$, $\eta > 0$, $\eta \neq 1$ and η describes the relative risk aversion.

Figure 4. Diversification for network risks



Note: The figure shows the expected utility $u_{i,n}$ of underwriting cyber policies as a function of the portfolio size. The utility for the network model is compared to different frequency models (iid, linear correlation). The parameters are chosen as in the baseline setting (Table 2).

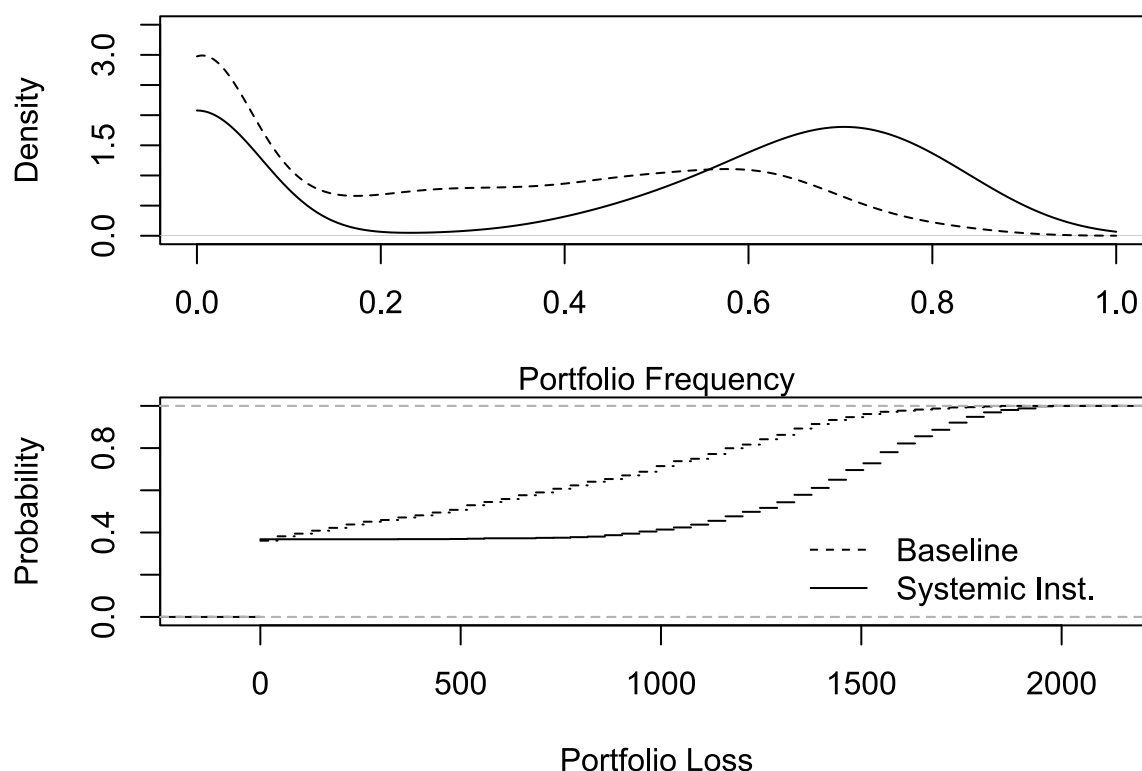
Compared to Ibragimov et al. (2009), who use a model with iid risks, our results show that the nonlinear frequency dependency is sufficient to observe a local market failure. We do not need to assume heavy-tailed severities and limited liability (Ibragimov et al., 2009). However, heavy-tailed severity would cause the nondiversification trap to be more pronounced.

5.4. Scenario analysis

We propose and analyze three approaches to include scenarios in the insurer's cyber insurance portfolio, namely, systemically important institution, pandemic spreading, and spillover. First, the notion of systemic risk is that a financial institution is "too big to fail." From the perspective of cyber risk, such critical companies can be identified, and they might be called "too interconnected to fail". Such an institution can be a monopolistic

software provider or a cloud service provider.²⁰ In our network model, we chose to infect the node with the highest connection density (critical institution) and analyze the outcome. Figure 5 shows the results. We find that the final infection rate increases from 27% in the baseline model to 58% if a systemically important institution is infected.

Figure 5. Portfolio distribution for systemic institution



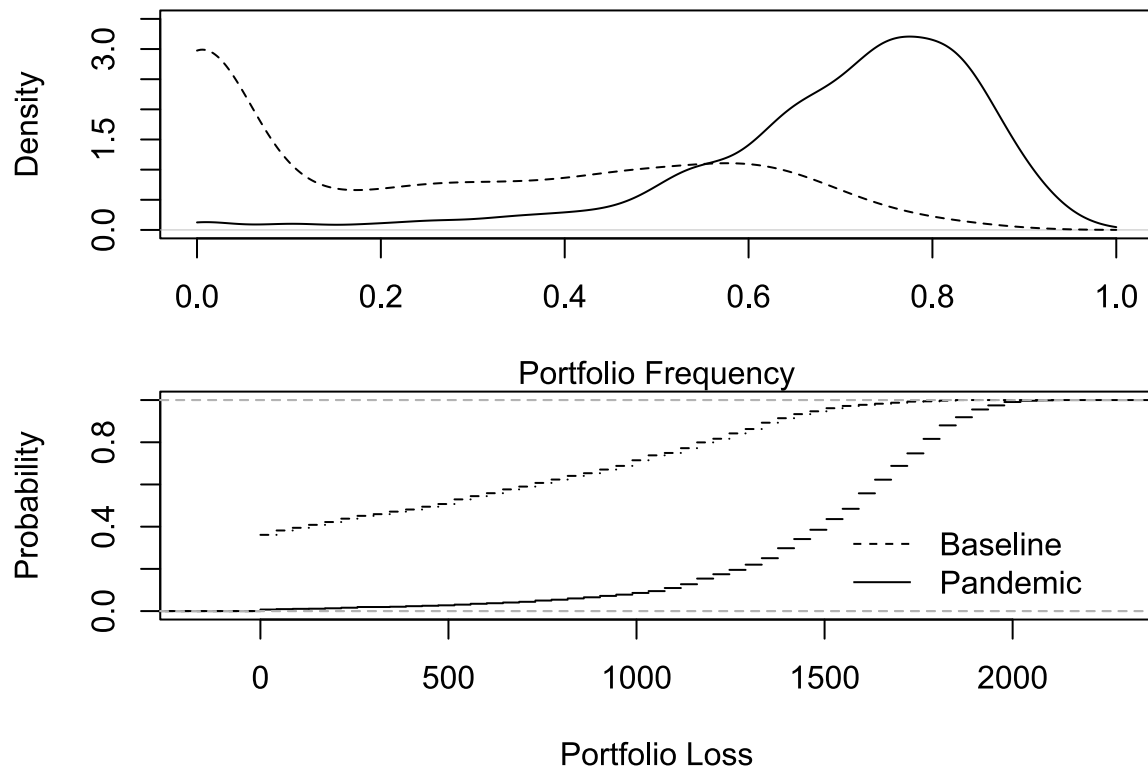
Note: The figure compares the insurer's portfolio loss distribution for the systemically important institution scenario to the baseline model. The top figure shows the simulated frequency density and the bottom figure the cumulative loss distribution. For illustrative purposes, the loss frequencies are estimated by applying a kernel and are assumed to be continuous. The losses are in mUS\$.

The results show that losses become greater when a critical institution is infected. Cloud service can lead to high concentration. As a consequence, insurers are advised to require their clients to have some diversification in cloud service providers or to insource the services. For the society, this would mean that the cloud architecture, which became

²⁰ The market for cloud services is highly concentrated with only four big companies (Amazon AWS, Microsoft, IBM, and Google) providing 50% of the market (Risk Management Solutions Inc., 2016). It seems this concentration is due to significant economies of scale for such kind of services.

fashionable recently, must be reevaluated. Blockchain technology, which provides services and stores data in a decentralized format, may mitigate some of the weaknesses of the cloud architecture (see, e.g., Mrvosevic, 2019; Wolfson, 2018).

Figure 6. Portfolio distribution for pandemic spreading



Note: The figure compares the insurer’s portfolio loss distribution for the pandemic scenario to the baseline model. The top figure shows the simulated frequency density and the bottom figure the cumulative loss distribution. For illustrative purposes, the loss frequencies are estimated by applying a kernel and are assumed to be continuous. The losses are in mUS\$.

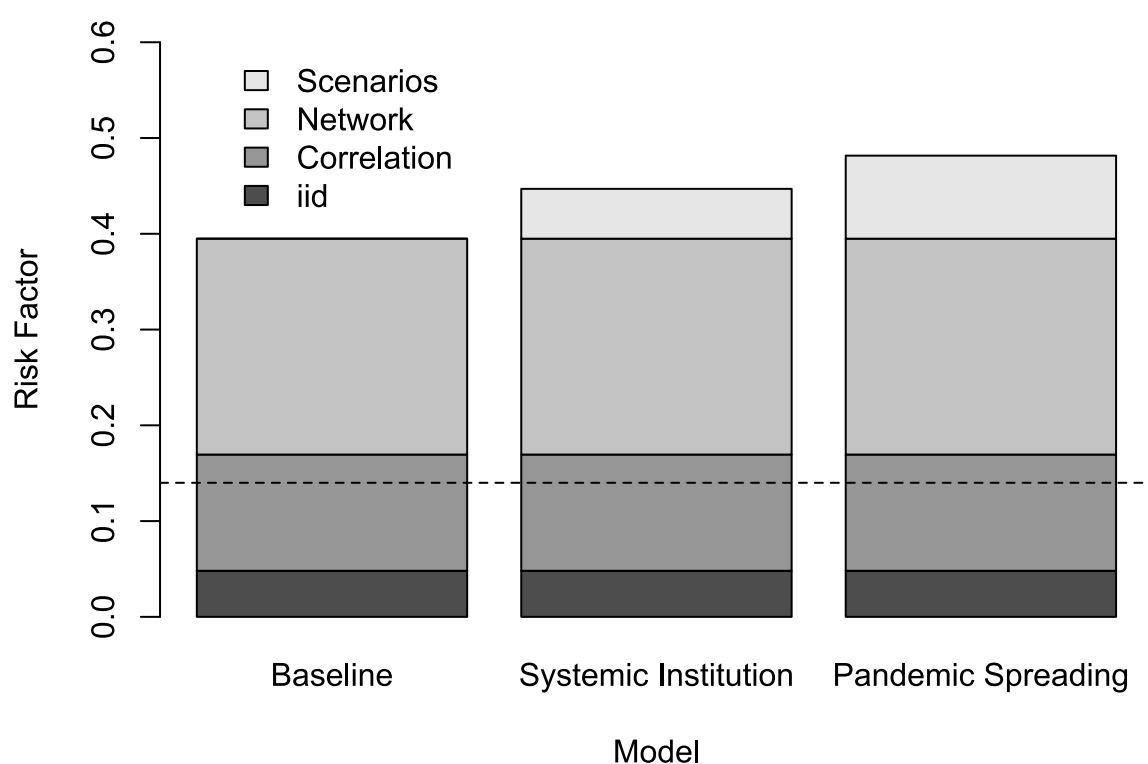
The second approach is to model systemic risk; “pandemic spreading” assumes that the systemic event manifests by many infected nodes in the larger economy. The insurer’s portfolio in turn is embedded in and connected to the larger economy. If more companies are infected outside, more paths of infection for the insurer’s portfolio exist. This increases the likelihood of each node being initially infected and thus translates here to a higher expected initial infection rate. We assume that on average 10% of the nodes are initially infected (each node’s initial infection is Bernoulli distributed with $p_0 = 0.1$ instead of $p_0 = 0.02$ as before). Figure 6 shows the distribution for the new scenario.

The results show that in the pandemic scenario the frequency of cyber losses increases and the cyber insurance portfolio features larger losses. The losses are not only higher

than expected but are also more severe according to the value at risk (see Table 3).

The risk factors are compared in Figure 7 (and Table 3) for the different models. First, we see that the network model requires an extra capital charge compared to the standard Solvency II model. This is because Solvency II considers linear correlations only. In a sense, this extra capital charge reflects systemic risk in the portfolio itself. The other two scenarios require even more capital. This is capital for systemic risk in a narrower sense that results from more severe distress in the economy.

Figure 7. Capital requirements for different scenarios



Note: The plot shows the risk factors(s) for different scenarios. s is split according to the contribution of iid risks, linear correlated risks, network exposure (heterogenous dependent risks), and systemic risk based on the two scenarios. The dotted line indicates the regulatory risk factor defined by Solvency II.

Since complex networks do not generally fulfill the Markov property, the initial infection rate and the exact infection location matter. Insurers should identify critical hubs in their underwriting portfolios, limit their exposure, and demand higher security measures. Generally, we find the stronger the clustering, the more IT security trumps insurance solutions. Moreover, the infection rate is likely to depend on the IT security in which the client invests. We did not include it here since it is difficult to come up with a sound

estimation. However, insurers can include an IT security rating in the network model and thus differentiate premiums accordingly. For clients that resemble hubs in the underwriting network, insurers can even require a minimum standard for IT security before underwriting them.

While micro and macro prudential approaches share similar instruments (risk measures), they have a different focus (ECB 2014). The analysis so far has taken a micro prudential approach that aims at ensuring the survival of the individual company and protection of its stakeholders. Micro prudential regulations focus on a firm's idiosyncratic risk. The macro prudential approach in turn is concerned with the survival of the whole system and minimizing the externality of the collapse of the entire system. Thus, the macro prudential approach puts more emphasis on the interdependency between institutions (feedback loops). The macro prudential perspective internalizes effects that would not be the case for the micro prudential perspective. It also takes the interaction with the rest of the economy into consideration.

One such macro prudential instrument is the systemic risk buffer (SRB) implemented in the European Union; the SRB is intended to prevent and mitigate serious consequences for the financial system and the real economy and complements the counter-cyclical capital buffer (ECO 2020). It can be applied to all or a subset of banks with similar risk profiles. While the insurance regulatory frameworks do not generally include a charge for systemic risk, we ask whether the systemic risk buffer for banks can be applied to insurers that underwrite cyber risk. Most countries have set SRB at around 0.03 of the risk-weighted assets (ESRB 2019). However, in insurance regulation, the capital requirements are specified based on debt not assets and some transformations are in place. After the necessary transformations, we attain a risk factor of 0.2 (instead of 0.14).²¹ That is still significantly below our model's risk factor and when comparing the systemic events (see Figure 7) to the high initial infection and contagion probability, the portfolio would not be sufficiently buffered.

²¹ If we assume that the risk-weighted assets (RWA) can be approximated by equity (E) and debt (D) and the required capital (cr) is equal to equity (E), we have $cr = s \cdot RWA = s(cr + D) = \frac{s}{1-s} D = \frac{0.14+0.03}{1-(0.14+0.03)} D = 0.201 \cdot D$.

6 Conclusion

In this paper, we propose a new network approach to model dependence in an insurer's underwriting portfolio of cyber risks. By building on the individual risk model, networks provide a way to model the real underlining structure on which cyber risk spreads. This micro or bottom-up approach allows for higher flexibility dependence modeling and more heterogeneity for different risks than other actuarial approaches, such as collective frequency models or copulas. Moreover, by separating the infection state (or frequency) from severity, the model allows for incorporating any dependence structure between the frequency and severity. It also allows one to account for IT security measures taken by each node. We combine the dependence model with the severity distribution, as investigated in the literature, to attain estimates for the portfolio losses in cyber insurance.

As we show, networks that facilitate the spreading of cyber threats feature heavy-tailed degree distributions. Such networks are characterized by high centralization, formation of hubs (such as IT companies), and ultra-small-world property. In these networks, cyber threats spread quickly if a hub is affected but might die out if a node in the periphery is affected. We show that an insurer's underwriting cyber portfolio being scale-free distributed leads to extremely and irregularly distributed loss frequency; this cannot be modeled adequately by any type of proposed collective frequency model, like Poisson or negative binomial distribution, or by any individual frequency model, such as the Gauss or Gumbel copula. The extreme frequency distribution exaggerates the observed heavy tails for the loss severity. Moreover, allowing heterogeneity in the severity distribution (i.e., hubs are not only infected more often but also feature higher losses) would make the distribution of the portfolio even more extreme.

Our results have important consequences. Compared to other dependency models, the extreme frequency distribution means higher premiums, higher measures of risk, higher capital requirements, and insufficiency of regulatory capital. Higher premiums and more capital expenses would pose an obstacle to development of the cyber insurance market. To our knowledge, we are the first to show that scale-free networks can render diversification suboptimal for some portfolio sizes, called the nondiversification trap (Ibragimov et al., 2009). In such circumstances, insurers that cannot reach a critical portfolio size would not be willing to underwrite cyber risks. Consequently, an insurance market would not exist for cyber risk and insurance as a risk management tool would not be

available. Moreover, the network model also allows us to implement worst case scenarios conveniently, including a systemic institution that is affected and systemic spreading. We show that the outcome can be devastating (low tipping point and even full infection).

The bottom-up approach provided by networks also allows us to derive recommendations for insurers. Insurers should carefully manage their underwriting portfolio. They should completely avoid exposure to hubs, charge a higher premium, or require companies to take additional IT security measures. We also propose a model for how insurance premiums for cyber insurance can be fairly calculated as a linear function of the client's connectivity. Generally, the insurer should strive for an underwriting portfolio that is characterized by low density and low clustering. First, cyber models need to take the dependency structure we find here into account. We should also emphasize that insurers need to collect very detailed information about the client's IT infrastructure and business model to be able to calibrate a network model adequately. For example, insurers should require their clients to diversify their sourcing of IT services or charge a premium if a concentration exists. However, our proposed network model provides guidance on what kind of information needs to be obtained and which parameters are truly important.

In turn, regulators should require more capital for the underwriting of cyber policies (see Eling & Schnell, 2019). The discount usually implicitly included in the capital requirements for diversification needs to be reconsidered since diversification does not always reduce risk. Additionally, capital for hubs in the underwriting network should be considered. Our model provides guidance on what kind of systemic scenarios are plausible and how regulators can implement them. However, more importantly, regulators should take a broader perspective that emerges when each insurer's underwriting network is considered as part of a national or global network. One question is whether the emphasis on the micro prudential approach of the current regulations is sufficient or whether systemic cyber risk should be addressed with a macro prudential approach (see, e.g., Hanson et al., 2011). Regulators should include system-wide distress in their macroprudential models. Another question is whether critical companies such as software, cloud service, and communication service providers should be classified as systemic and be regulated accordingly (similar to the additional capital buffer for systemic banks under Basel III). Other suggestions include establishing a new international governance body that monitors systemic cyber risk (similar to the financial stability board) and whether a "systemic cyber risk tax" should be introduced (Benoit et al., 2017). Finally, companies

can reduce systemic risk by increasing resilience to systemic cyber risk, for example, with redundant and geographically diversified systems.

As more data on cyber risk emerge, future research can improve the network model proposed here by allowing for different link strengths (weighting), directional links, alternative link distributions, or completely different models, such as fitness network models. Moreover, using multilayer (interdependent) and dynamic networks (see, e.g. Kivelä et al., 2014; Zhao et al., 2018) can also improve the representation of real systems. For example, cyber risks can eventually affect the power system (see, e.g., Bashan et al., 2013). An insurer that underwrites cyber risks and insures the power grid is essentially exposed to two layers of interacting networks. The interaction of the cyber insurance network and the reinsurance network would allow for analyzing systemic risk on an industry level. We conjecture that such interaction would make catastrophic events more likely. Spreading models can also be improved with more data and adapted to specific threats, such as viruses.

7 References

- Ahern, K. R. (2013). Network centrality and the cross section of stock returns. *SSRN Electronic Journal*.
- Aspnes, J., Chang, K., & Yampolskiy, A. (2006). Inoculation strategies for victims of viruses and the sum-of-squares partition problem. *Journal of Computer and System Sciences*, 72(6), 1077–1093.
- Barabási, A.-L. (2016). *Network science*. Cambridge University Press.
- Barabási, A.-L., & Albert, R. (1999). Emergence of scaling in random networks. *Science*, 286(5439), 509–512.
- Bashan, A., Berezin, Y., Buldyrev, S. V., & Havlin, S. (2013). The extreme vulnerability of interdependent spatially embedded networks. *Nature Physics*, 9(10), 667–672.
- Benoit, S., Colliard, J.-E., Hurlin, C., & Pérignon, C. (2017). Where the risks lie: a survey on systemic risk. *Review of Finance*, 21(1), 109–152.
- Berr, J. (2017). “WannaCry” ransomware attack losses could reach \$4 billion. CBS News. <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses>

- Bianconi, G., & Barabási, A.-L. (2001). Competition and multiscaling in evolving networks. *Europhysics Letters*, 54(4), 436–442.
- Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: an empirical analysis. *Geneva Papers on Risk and Insurance - Issues and Practice*, 40(1), 131–158.
- Billio, M., Caporin, M., Panzica, R., & Pelizzon, L. (2016). The impact of network connectivity on factor exposures, asset pricing and portfolio diversification. *SSRN Electronic Journal*.
- Billio, M., Getmansky, M., Lo, A. W., & Pelizzon, L. (2012). Econometric measures of connectedness and systemic risk in the finance and insurance sectors. *Journal of Financial Economics*, 104(3), 535–559.
- Böhme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. *Workshop on the Economics of Information Security (WEIS)*.
- Böhme, R., & Schwartz, G. (2010). Modeling cyber-insurance: towards a unifying framework. *Workshop on the Economics of Information Security (WEIS)*.
- Bolot, J., & Lelarge, M. (2009). Cyber insurance as an incentive for internet security. In *Managing Information Risk and the Economics of Security* (pp. 269–290). Springer US.
- Bolot, J., & Lelarge, M. (2008). A new perspective on internet security using insurance. *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, 1948–1956.
- Bundesamt für Privatversicherungen. (2006). *Technisches Dokument zum Swiss Solvency Test*. http://www.finma.ch/archiv/bpv/download/i/SST_technischesDokument_061002.pdf
- Coburn, A. W., Daffron, J., Quantrill, K., Leverett, E., Bordeau, J., Smith, A., & Harvey, T. (2019). *Cyber risk outlook*. Centre for Risk Studies, University of Cambridge.
- Crowdstrike. (2018). *Global survey reveals supply chain as a rising and critical new threat vector*. <https://www.crowdstrike.com/blog/global-survey-reveals-supply-chain-as-a-rising-and-critical-new-threat-vector/>
- Daffron, J., Ruffle, S., Andrew, C., Copic, J., Quantrill, K., Smith, A., & Leverett, E.

- (2019). *Bashe attack: global infection by contagious malware*. Centre for Risk Studies, University of Cambridge.
- Dejung, S. (2017). *Economic impact of cyber accumulation scenarios*. Swiss Insurance Association SVV Cyber Working Group.
- Denuit, M., Dhaene, J. M. L., Goovaerts, M., Kaas, R., & Laeven, R. J. A. (2006). Risk measurement with equivalent utility principles. *Statistics & Decisions*, 24(1/2006), 1–25.
- Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: a closer look at data breaches. *Journal of Cybersecurity*, 2(1), 3–14.
- Eling, M., Elvedi, M., & Falco, G. (2020). The economic impact of extreme cyber risk scenarios. *Working Paper*.
- Eling, M., & Jung, K. (2018). Copula approaches for modeling cross-sectional dependence of data breach losses. *Insurance: Mathematics and Economics*, 82, 167–180.
- 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. *North American Actuarial Journal*.
- Eling, M., & Wirfs, J. H. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109–1119.
- Erdős, P., & Rényi, A. (1960). On the evolution of random graphs. *Institute of Mathematics, Hungarian Academy of Sciences*, 5(1), 17–60.
- European Central Bank (ECB). (2014). Micro- versus macro-prudential supervision: potential differences, tensions and complementarities. *Financial Stability Review*, 139.
- European Commission (EC). (2015). Commission delegated regulation 2015/35: supplementing directive 2009/138/EC of the European parliament and of the council on the taking-up and pursuit of the business of insurance and reinsurance (Solvency II). *Official Journal of the European Union*, 58(L12), 1–797.
- European Council (ECO). (2020). *Capital requirements for the banking sector*. <https://www.consilium.europa.eu/en/policies/banking-union/single-rule-book/capital-requirements/>

- European Systemic Risk Board (ESRB). (2019). *Systemic risk buffer*. https://www.esrb.europa.eu/national_policy/systemic/html/index.en.html
- Fahrenwaldt, M. A., Weber, S., & Weske, K. (2018). Pricing of cyber insurance contracts in a network model. *ASTIN Bulletin*, 48(3), 1175–1218.
- Grossklags, J., Christin, N., & Chuang, J. (2008). Secure or insure? a game-theoretic analysis of information security games. *Proceedings of the 17th International Conference on World Wide Web*, 209–218.
- Hanson, S. G., Kashyap, A. K., & Stein, J. C. (2011). A macroprudential approach to financial regulation. *Journal of Economic Perspectives*, 25(1), 3–28.
- Herath, H., & Herath, T. (2011). Copula based actuarial model for pricing cyber-insurance policies. *Insurance Markets and Companies: Analyses and Actuarial Computations*, 2(1), 7–20.
- Ibragimov, R., Jaffee, D., & Walden, J. (2009). Nondiversification traps in catastrophe insurance markets. *Review of Financial Studies*, 22(3), 959–993.
- Kanno, M. (2016). The network structure and systemic risk in the global non-life insurance market. *Insurance: Mathematics and Economics*, 67, 38–53.
- Katz, L. (1953). A new status index derived from sociometric analysis. *Psychometrika*, 18(1), 39–43.
- Kitten, T. (2016). *Bangladesh bank heist: lessons learned*. Bank Info Security. <https://www.bankinfosecurity.com/bangladesh-bank-heist-lessons-learned-a-9064>
- Kivelä, M., Arenas, A., Barthelemy, M., Gleeson, J. P., Moreno, Y., & Porter, M. A. (2014). Multilayer networks. *Journal of Complex Networks*, 3, 203–271.
- Kuon, S., Radtke, M., & Reich, A. (1993). An appropriate way to switch from the individual risk model to the collective one. *ASTIN Bulletin*, 23(1), 23–54.
- Lee, T. B. (2017). *The WannaCry ransomware attack was temporarily halted. But it's not over yet*. Vox. <https://www.vox.com/new-money/2017/5/15/15641196/wannacry-ransomware-windows-xp>
- Lelarge, M., & Bolot, J. (2008a). A local mean field analysis of security investments in

- networks. *Proceedings of the 3rd International Workshop on Economics of Networked Systems*.
- Lelarge, M., & Bolot, J. (2008b). Network externalities and the deployment of security features and protocols in the internet. *ACM SIGMETRICS Performance Evaluation Review*, 36(1), 37–48.
- Lelarge, M., & Bolot, J. (2009). Economic incentives to increase security in the internet: the case for insurance. *IEEE INFOCOM 2009 - The 28th Conference on Computer Communications*, 1494–1502.
- Leveille, J. (2002). Epidemic spreading in technological networks. *School of Cognitive and Computing Sciences, University of Sussex at Brighton*.
- Lin, Y., Yu, J., & Peterson, M. O. (2015). Reinsurance networks and their impact on reinsurance decisions: theory and empirical evidence. *Journal of Risk and Insurance*, 82(3), 531–569.
- Maillart, T., & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *European Physical Journal B*, 75(3), 357–364.
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. *Computer Science Review*, 24, 35–61.
- Mrvosevic, M. (2019). *Blockchain based decentralised cloud computing*. <https://medium.com/@eternacapital/blockchain-based-decentralised-cloud-computing-277f307611e1>
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: to insure IT or not? *Decision Support Systems*, 56(1), 11–26.
- Nicastro, D. (2016). *Salesforce customers lose CRM data in 20 hour outage*. <https://www.cmswire.com/customer-experience/salesforce-customers-lose-crm-data-in-20-hour-outage>
- OECD. (2020). *Global insurance market trends*. <http://www.oecd.org/daf/fin/insurance/globalinsurancemarkettrends.htm>
- Ogut, H., Menon, N., & Raghunathan, S. (2005). Cyber insurance and IT security in-

- vestment: impact of interdependence risk. *Workshop on the Economics of Information Security (WEIS)*.
- Panjer, H. H., & Willmot, G. E. (1992). *Insurance risk models*. Society of Actuaries.
- Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic dynamics and endemic states in complex networks. *Physical Review E*, 63(6), 66117.
- Peralta, G., & Zareei, A. (2016). A network approach to portfolio selection. *Journal of Empirical Finance*, 38, 157–180.
- Ponemon Institute LLC. (2018). *2018 cost of a data breach study: global overview*. <https://www.ibm.com/downloads/cas/861MNWN2>
- Privacy Rights Clearinghouse. (2020). *Data breaches*. <https://privacyrights.org/data-breaches>
- Richmond, R. J. (2019). Trade network centrality and currency risk premia. *Journal of Finance*, 74(3), 1315–1361.
- Risk Management Solutions Inc. (2016). *Managing cyber insurance accumulation risk*. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf
- Ruffle, S. J., Bowman, G., Caccioli, F., Coburn, A. W., Kelly, S., Leslie, B., & Ralph, D. (2014). *Stress test scenario: sybil logic bomb cyber catastrophe*. Centre for Risk Studies, University of Cambridge.
- SAS Institute Inc. (2015). *SAS® OpRisk global data*. https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf
- Schwartz, G., & Sastry, S. (2014). Cyber-insurance framework for large scale interdependent networks. *Proceedings of the 3rd International Conference on High Confidence Networked Systems*, 145–154.
- Schwartz, G., Shetty, N., & Walrand, J. (2010). *Cyber-insurance: missing market driven by user heterogeneity*.
- Shetty, N., Schwartz, G., & Walrand, J. (2010). Can competitive insurers improve network security? *International Conference on Trust and Trustworthy Computing*, 308–322.
- Staudt, A. (2010). Tail risk, systemic risk and copulas. *Casualty Actuarial Society E-*

Forum.

- Tse, C. K., Liu, J., & Lau, F. C. M. (2010). A network perspective of the stock market. *Journal of Empirical Finance*, 17(4), 659–667.
- Van der Aalst, T. A. F. (2018). *A network approach to interrelated insurance risk*. https://www.ag-ai.nl/view/40309-180609_cyberriskthesis.pdf
- Výrost, T., Lyócsa, Š., & Baumöhl, E. (2019). Network-based asset allocation strategies. *North American Journal of Economics and Finance*, 47, 516–536.
- Wang, S. S. (1998). Aggregation of correlated risk portfolios: models and algorithms. *Proceedings of the Casualty Actuarial Society*, 85(163), 848–939.
- Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of ‘small-world’ networks. *Nature*, 393(6684), 440–442.
- Whalen, K. (2018). *Frequency and complexity of DDoS attacks is rising*. <https://www.netscout.com/news/press-release/complexity-ddos-attacks>
- Wheatley, S., Hofmann, A., & Sornette, D. (2019). *Data breaches in the catastrophe framework & beyond*. <https://arxiv.org/ftp/arxiv/papers/1901/1901.00699.pdf>
- Wheatley, S., Maillart, T., & Sornette, D. (2016). The extreme risk of personal data breaches and the erosion of privacy. *European Physical Journal B*, 89(1), 7.
- Wolfson, R. (2018). *Blockchain-based data storage solutions help secure user data*. Forbes. <https://www.forbes.com/sites/rachelwolfson/2018/09/25/blockchain-based-data-storage-solutions-help-secure-user-data/#790ac5eb7512>
- World Economic Forum (WEF). (2014). *Global risks 2014 - ninth edition*. http://reports.weforum.org/global-risks-2014/?doing_wp_cron=1548774994.0724980831146240234375
- World Economic Forum (WEF). (2016). *Understanding systemic cyber risk*. http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf
- Yang, Z., & Lui, J. C. S. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, 74, 1–17.
- Zhao, L., Wang, G.-J., Wang, M., Bao, W., Li, W., & Stanley, H. E. (2018). Stock market as temporal network. *Physica A: Statistical Mechanics and Its Applications*, 506,

1104–1112.

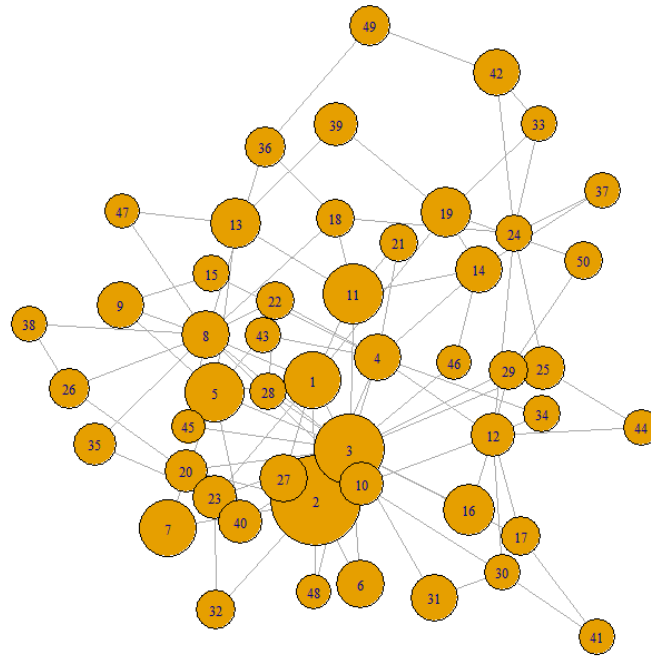
Zweifel, P., & Eisen, R. (2012). *Insurance economics*. Springer-Verlag.

8 Appendices

Appendix A. Example network

Figure A1 shows an example of our network. These kinds of networks are strongly clustered in that a few nodes are strongly interconnected while others have only a few links.

Figure A1. Cyber underwriting network



Note: The plot shows one simulation of the cyber underwriting network with 50 policies. The sizes of the nodes are proportional to their number of links.

Appendix B. Cyber risk spreading

We use an exponential decaying infection probability. The function is defined as:

$$q(t) = q_0 \cdot e^{-\frac{t}{\tau}}, \quad (\text{B1})$$

where τ stands for the mean half-life that we set to $\tau = 5$. Table B1 lists the relevant literature that uses scenarios, case studies, or surveys to derive estimates for the network model. It seems that most attacks are resolved within days and the company is no longer

infected (this does not mean that the damage is resolved, especially if physical infrastructure is also affected). A mean half-life τ of five days seems to be sensible.²² This means that each infected policy holder is on average infectious for five days. After that, we assume that the security leak has been addressed and the node cannot be attacked.

Table B1. Literature on network parameters

Scenario	Parameter Estimate	Reference
DoS	Frequency: Half of all major U.S. companies experienced a DDoS attack in 2015 and one in eight of those attacks rendered their websites unavailable. Recovery Time: Outages of hours to one week.	Risk Management Solutions Inc. (2016), Dejung (2017)
Cloud Service Failure	Recovery Time: A few hours up to one month of persistence are conceivable.	Risk Management Solutions Inc. (2016), Dejung (2017), WEF (2014)
SCADA/ICS	Recovery Time: Potential to persist for three weeks.	Dejung (2017)
Financial Transaction Cyber Compromise	Recovery Time: Up to 12 months until the complex and obscure criminal operation is fully understood.	Risk Management Solutions Inc. (2016)
Telecommunication scenarios	Recovery Time: Attack persistence of seven days is assumed in the first scenario, while the persistence in the second scenario is expected to be shorter.	Dejung (2017)
Strategic cross-sector attack scenario	Frequency: Ruffle et al. (2016) estimate the frequency of such an event at 1%. Relatively short period of a few days as the attack is expected to be carried out on a single day at numerous companies	Risk Management Solutions Inc. (2016), Ruffle et al. (2014)
Event		
SCADA/ICS	Recovery Time: Four days	Nicastro (2016)

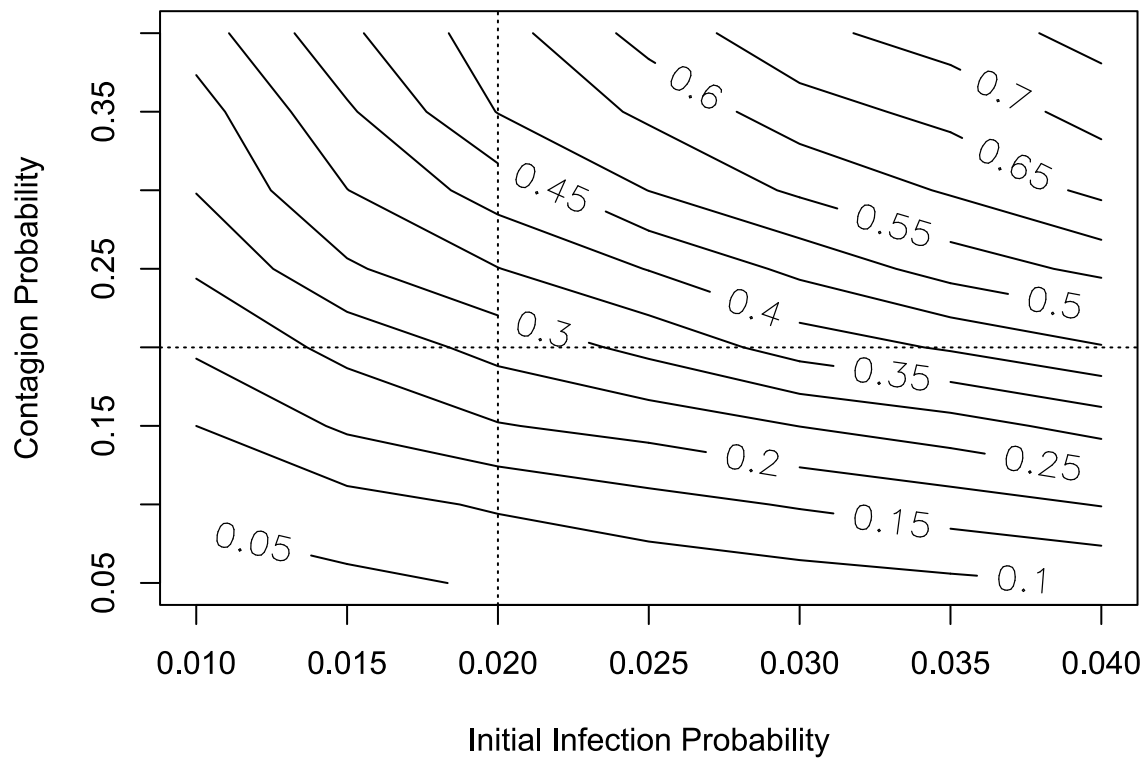
²² For example, the malware “WannaCry” first outbreak in 2017 finished after 4 days as security patches were available and dispatched by that time (Lee, 2017).

WannaCry	Frequency: 34% of all NHS trusts in England	Coburn et al. (2019)
Survey		
Data Breach	Frequency: Likelihood of a recurring material breach over the next two years 27.9%, South Africa: 43%, Germany: 14.3% Recovery Time: Mean time to contain: 69 days	Ponemon Institute LLC (2018)
Cyber-Induced Business Interruption	Frequency: In a 2018 survey of 1,300 companies across the U.S., Canada, the U.K., Mexico, Australia, Germany, Japan, and Singapore, two-thirds of companies said they have been targeted with a supply chain attack costing an average of US\$1.1 million per attack, with 34% of companies reporting that their operations had been disrupted. Recovery Time: Though U.S. organizations averaged a 12-hour response time, attacks can take up to 63 hours to detect and remediate.	CrowdStrike (2018), Coburn et al. (2019)
DDoS	Frequency: After suffering from a DDoS attack, 57% of targeted organizations report reputation and brand damage as the primary business impact (40% as large organizations faced an average of eight attacks per day)	Whalen (2018), Coburn et al. (2019)

Note: This table is partially based on Eling, Elvedi, and Falco (2020), where more details can be found.

Table B1 also provides an overview on the current literature on the frequency of cyber risk incidents. The frequency of companies that suffer damage from an attack varies greatly from 0.14 to 0.57. We think a final infection probability, p_T , of 0.27 is reasonable. While it is possible to estimate p_T , we need to calibrate the initial infection probability p_0 and contagion probability q_0 in our model. These two parameters are difficult to estimate since no data are available. Thus, we reengineer backward what combination of $\{p_0, q_0\}$ would lead to a final infection frequency of 0.27. Figure B1 shows the final infection rate for different combinations of $\{p_0, q_0\}$.

Figure B1. Sensitivity of final infection frequency



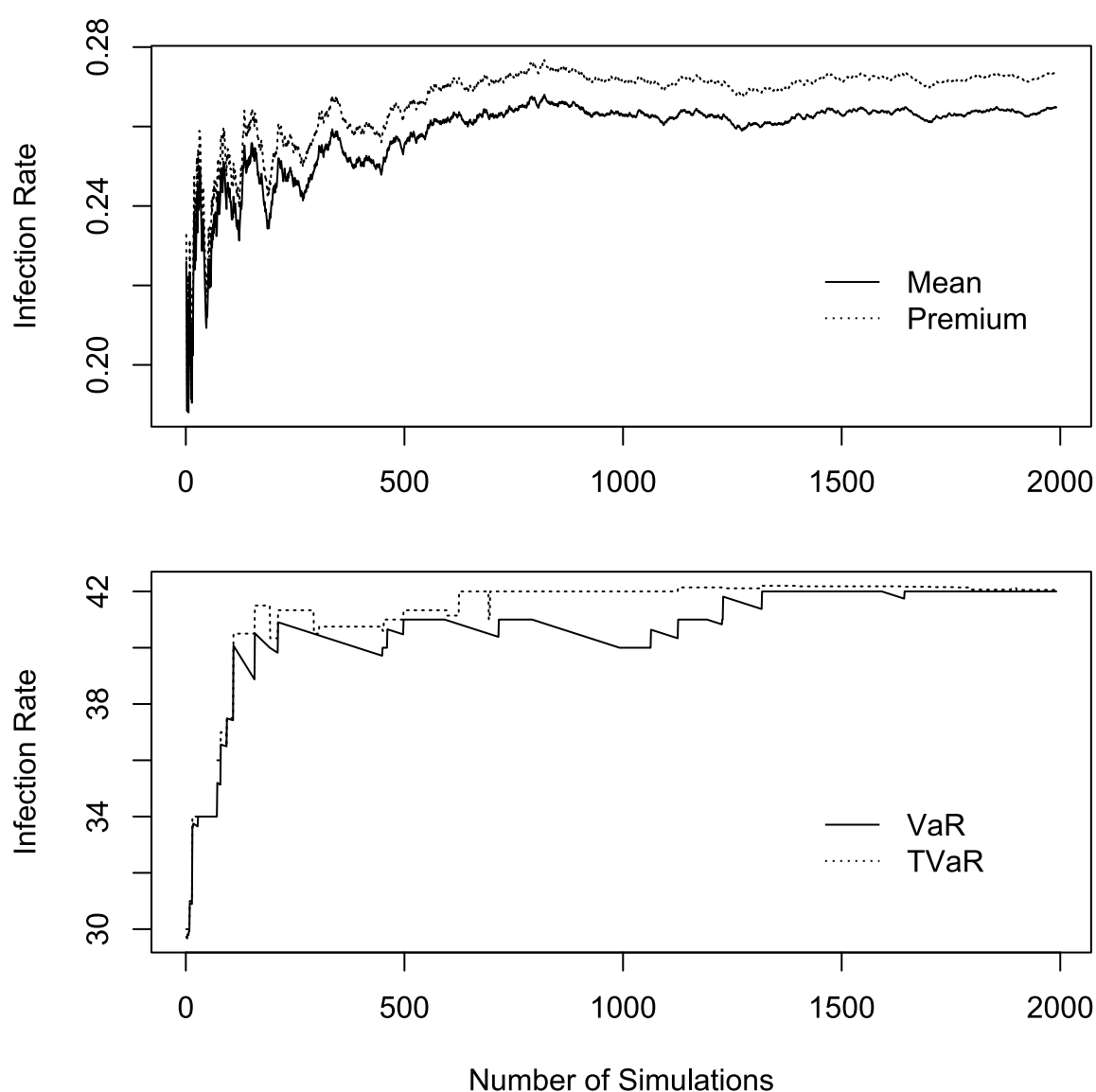
Note: The figure shows the final infection frequency for the space of initial infection and contagion probability. The two dotted lines show the parameter choice for the baseline model ($p_0 = 0.02$, $q_0 = 0.2$).

The analysis shows that a convex combination of p_0 and q_0 solves for the same final infection frequency of 0.27. We set $p_0 = 0.02$ and $q_0 = 0.2$ for the baseline model. However, we also report the same results for different parameter spaces (Figure 3 and Appendix D).

Appendix C. Stability of simulations

Figure C1 shows the expectation, premium, VaR , and $TVaR$ of the portfolio frequency for the baseline model (Table 2). The analysis shows that the expectation and premium (based on the expected utility) stabilize faster than the VaR and the $TVaR$. The $TVaR$ is the most unstable parameter since it is based on only a few simulated observations in the distribution's tail. In any case, all the statistics seem to stabilize eventually at around 1,500 simulations. Thus, we use 1,500 simulations for all the analyses conducted.

Figure C1. Statistics for increasing number of simulations

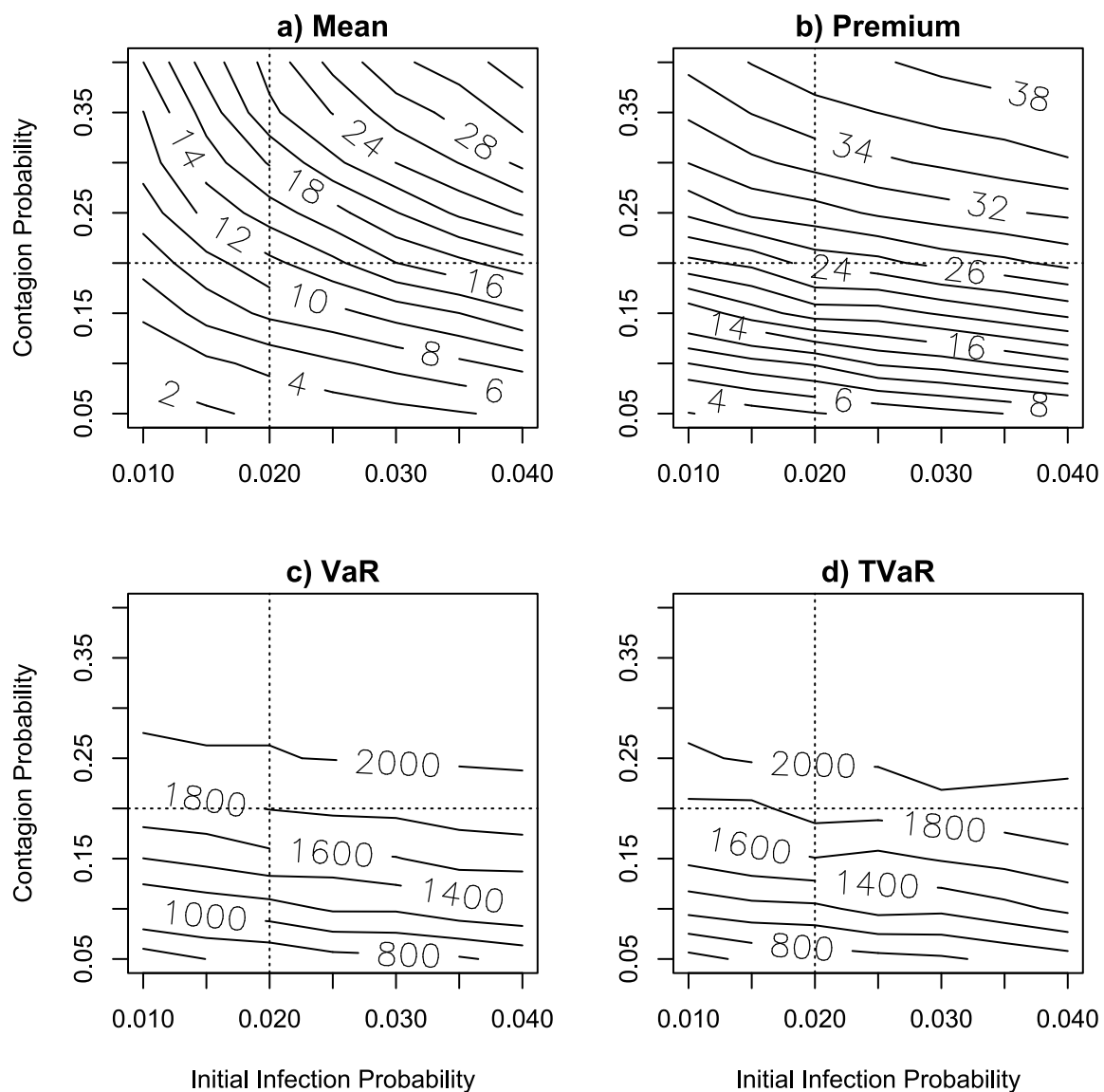


Note: The figure shows the evolution of mean, premium (upper figure), value at risk, and tail value at risk (lower figure), based on the portfolio frequency for an increasing number of simulations.

Appendix D. Additional sensitivity analyses

In the following, we investigate how the statistics depend on the parameter space of initial infection and contagion probability, $PQ = \{(p_0, q_0) \in \mathbb{R}^2 \mid 0.01 < p_0 < 0.04, 0.05 < q_0 < 0.4\}$. Figure D1 shows that all the statistics are sensitive to the choice of (p_0, q_0) and the trade-off is convex. Moreover, the indifference curves for the risk-sensitive measures, namely, premium, VaR , and $TVaR$, are less steep than the one for expectation. As p_0 becomes lower, a smaller increase in q_0 is needed to produce the same value for the risk-sensitive statistics. This indicates that lower p_0 produces more extreme distributions. Thus, capital requirements can still be calculated based on our network model even if the initial infection probability is uncertain.

Figure D1. Statistical sensitivity to contagion and infection probability



Note: The figures show the mean, premium, value at risk, and tail value at risk for the parameter space of initial infection and contagion probability. All the other parameters are set according to the baseline model. The numbers are in mUS\$.

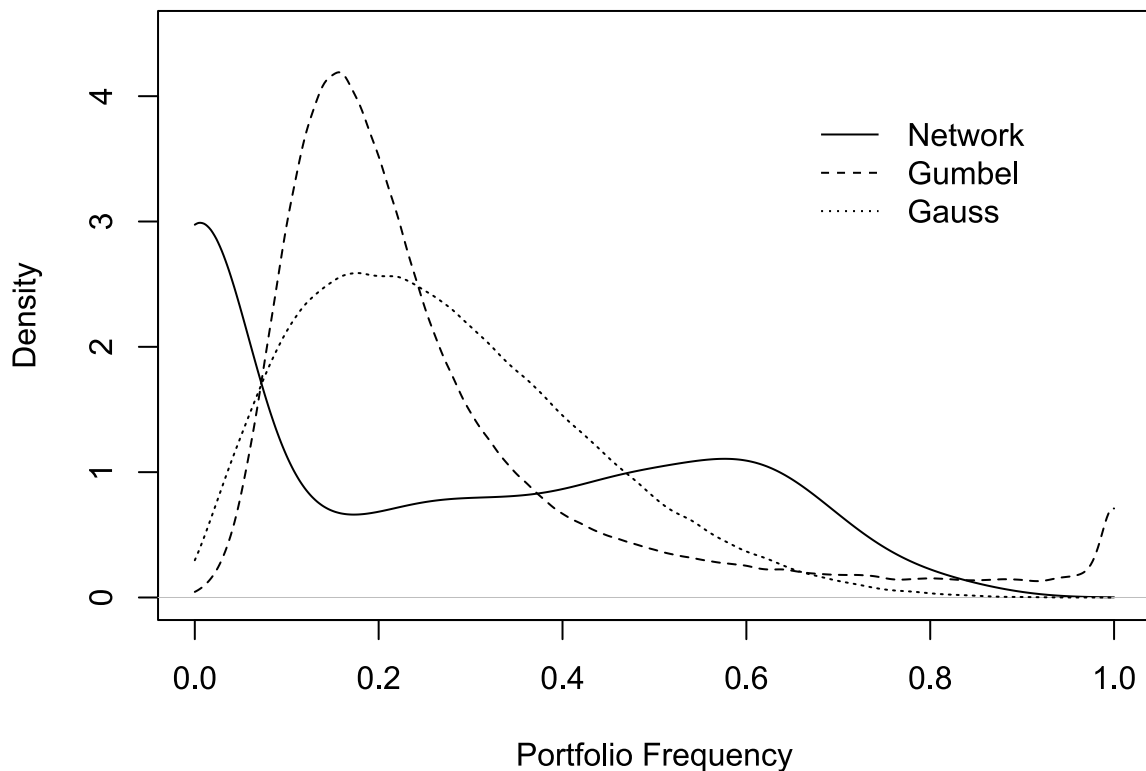
Appendix E. Copula frequency

A frequently applied alternative bottom-up approach to model the dependency between risks is the copula. We compare the network frequency with the distribution generated by the Gauss (linear correlation) and Gumbel copula. We use the Gumbel copula because it is well suited to capture the stronger dependency in the upper tail, meaning if one policy registers a loss the probability that the others also suffer is high (Herath & Herath, 2011). The Gumbel copula is defined as:

$$C_{\theta} = e^{-\left(\sum(-\ln(u_i))^{\theta}\right)^{\frac{1}{\theta}}}, \quad (\text{E1})$$

where θ is the dependence parameter. For the Gauss copula, we use the same correlation parameter as in the main text, namely, $\rho = 0.18$, for every pair of risks in the portfolio, while for the Gumbel we make use of the fact that $\theta = \frac{1}{(1-\rho)} = 1.2$. Both copula models are calibrated to guarantee that the same average infection rate as for the main model $\hat{p}_T = 0.27$ is achieved. Figure E1 shows that the network frequency features a bimodal (two peaks) distribution function.

Figure E1. Frequency distribution based on copula



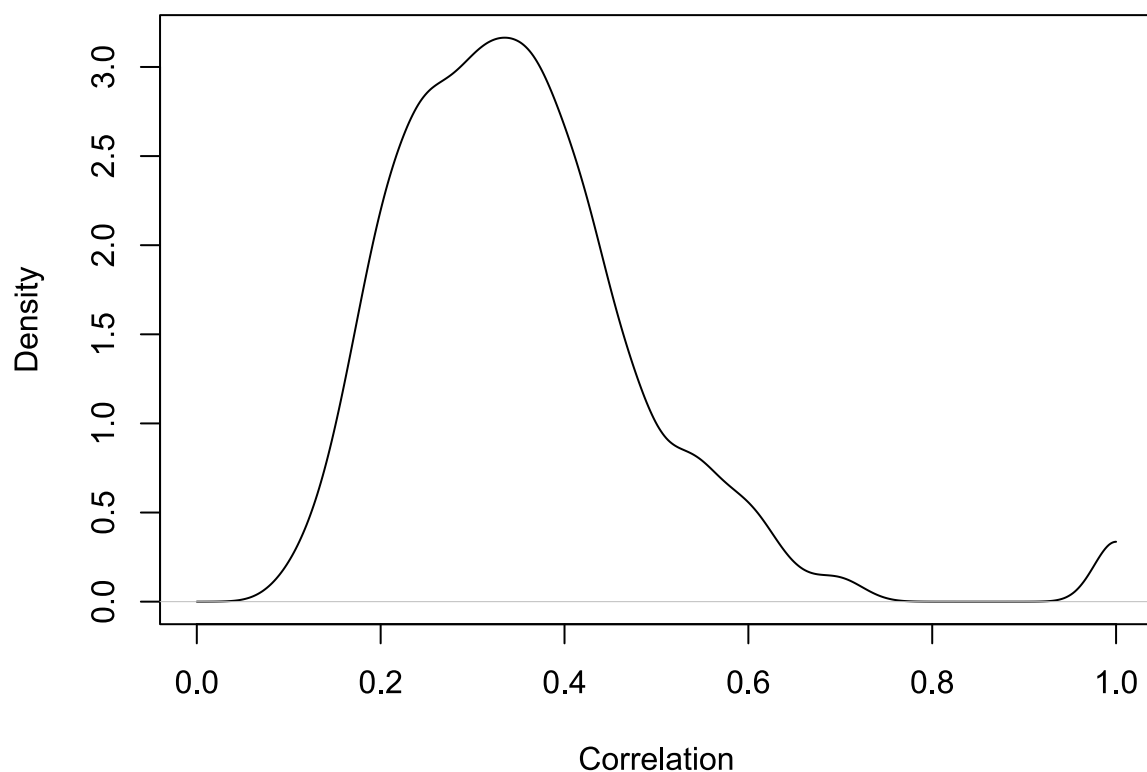
Note: The figure compares the frequency distribution for the network with the distribution generated by the Gauss and Gumbel copulas. The densities are estimated by applying a Gaussian kernel to the simulated data.

In comparison, both the Gaussian and Gumbel copula models are less dense for very low frequencies, peak around 0.2, and are rather low for higher frequencies. However, the Gumbel copula shows a peak for a frequency of 1. As θ increases the Gumbel density thins out in the midsection and the upper peak becomes more pronounced. Neither copula model, even for higher ρ , fits the network frequency particularly well. This can be explained by the fact that both copulas use only one dependence parameter that cannot capture the network's heterogeneity (link distribution). More promising are copula models that allow for different correlations or dependency parameters between each risk pair. One such category is vine copulas. However, this only shifts the problem to the question of how many parameters can be estimated.

Appendix F. Correlating distribution

The network model can also be used to derive a correlation distribution for the insurer's portfolio. If each policyholders position in the network would be unknown to the insurer, the correlation between each policyholder would be perceived as random by the insurer as shown in Figure F1.

Figure F1. Correlation distribution for the insurer's portfolio



Note: The figure shows the distribution of the correlation over different nodes derived from the network model.

The figure shows that the correlation observed in our network model differs strongly between nodes. An insurer using a homogeneous linear correlation model would need to account for high uncertainty in the correlation parameter.

Curriculum Vitae

Personal Information

Name: Werner Schnell

Date of Birth: March 16th, 1983

Place of Birth: Maienfeld (GR), Switzerland

Nationality: Swiss

Education

01/2016 – **Ph.D. in Finance**, University of St.Gallen, Switzerland

04/2011 – 08/2013 **M.A. in Banking and Finance**, University of St.Gallen, Switzerland

09/2008 – 08/2010 **B.A. in Economics**, University of St.Gallen, Switzerland

Work Experience

01/2016 – **Project manager and research assistant**, Institute of Insurance Economics (I.VW), University of St.Gallen

09/2013 – 01/2016 **Risk manager**, KPMG and Helvetia