Institute of Insurance Economics

University of St.Gallen

In collaboration with

Swiss Re

Cyber Risk: Too Big to Insure?

Risk Transfer Options for a Mercurial Risk Class

Martin Eling / Jan Hendrik Wirfs

I·VW HSG Schriftenreihe, Band 59

Cyber Risk: Too Big to Insure?
Risk Transfer Options for a Mercurial Risk Class

Martin Eling
Jan Hendrik Wirfs

ISBN 978-3-7297-2006-0

Imprint

Publisher
Institute of Insurance Economics I.VW-HSG, University of St. Gallen,
www.ivw.unisg.ch

Cover Pictures
https://de.fotolia.com/id/86011671 and https://de.fotolia.com/id/87719003, March 16, 2016.

Acknowledgements

We would like to thank all participants in the market survey for their feedback. Furthermore, we are grateful to all experts who made themselves available for discussing and interpreting the results and to Swiss Reinsurance Company Ltd. for its financial contribution to implement this study. We are especially grateful to Dr. Maya Bundt and Dr. Stephan Schreckenberg for their significant contribution and support. In addition, we would like to express our appreciation to Dr. Christian Biener, Michael Kuhn, and Andreas Lindemuth for their helpful comments. Finally, we thank Xhengis Ramadani, Werner Schnell, and Andreina Zink for their assistance in preparing this study.

Table of Contents

List of Figures

List of Tables

Management Summary

Cyber risk is an increasingly important, but under-researched topic. Moreover, the cyber insurance market is very small and its development has been hampered by problems of insurability. Some market participants claim that cyber risks present such a danger to global business that insurance pools are needed or even that governments need to step in to cover the risks. Does this mean that cyber risks are too big to insure?

This study is the first systematic discussion of potential risk transfer options for cyber risks. We compare several risk transfer options, including insurance, reinsurance and alternative risk transfer. Moreover, we discuss the potential role of the government and the capacity of insurance pools to improve insurability. On the methodological side, we rely on both qualitative and quantitative analyses to justify our conclusions. We use Berliner's insurability framework and expected utility analysis of different cyber specific scenarios. We then compare our theoretical findings with the opinions of market participants in an empirical study.

Our main conclusion is that cyber risks "of daily life" are not too big to insure. We show that the broader use of reinsurance would help to improve insurability. An insurance pool might also be useful to generate common knowledge, establish standards, and improve diversification. In contrast, "extreme scenarios" (e.g., a breakdown of the critical infrastructure) are difficult to insure, especially given the lack of data, cumulative risk, and other problems of insurability. A discussion between the government and the industry regarding those extreme scenarios seems useful. Both need a strategy for treating extreme scenarios, which – as we show empirically – are not unlikely to materialize in the next ten years. We discuss minimum standards for self-protection and reporting obligations for cyber incidents as measures in this context.

Consequently, we call for a two-tier approach to improve the insurability of cyber risks: First, we recommend improving the insurability for cyber risks "of daily life" by a within-industry collaboration. Second, we propose improving the insurability for "extreme scenarios" by integrating the government in various ways. Insurability should be an aspect of any national strategy against increasingly serious cyber threats.

Highlights

1 Motivation and Aim of the Study

Every reported data breach or system failure makes decision makers more aware that current risk management practices have failed to protect against cyber risks. There are many examples of the high economic importance of cyber risk. For example, the G-20 group cited cyber attacks as a threat to the global economy (Ackerman, 2013). Both in probability of occurrence and potential severity, cyber risks and the failure of critical information infrastructure are two of the top five global risks. The World Economic Forum (2010) estimates a 10% probability of a critical information infrastructure breakdown within the next 10 years and the financial consequences within the first few days alone amounting to about US$ 250 billion. As we will show in this study, estimates of the likelihood for such an event are now even higher.

In combination with other risk management measures, insurance is seen as one possible way to manage cyber risks. However, the underdeveloped cyber insurance market has fallen far below expectations with an annual premium volume of approximately US$ 3 billion (Advisen, 2015).[1] In contrast, the global annual losses for cyber risk are estimated to be more than US$ 400 billion (McAfee, 2014; ACGS, 2015). According to market participants, the balance sheets of insurance companies are simply not large enough to cover cyber risk (Gray, 2015). In a recent survey of insurance managers, PwC (2015b) discusses the problems insurers face with digitalization and show that cyber risk is the most important strategic challenge for the non-life insurance industry.

In spite of its increasing relevance for businesses today, research on cyber risk remains fairly limited. A few papers can be found in the technology domain, but little research has been done in the risk and insurance domain. Table A1 (Appendix A) outlines all published articles on cyber insurance and their contributions. Many of these articles emphasize the complexity and dependent risk structure (e.g., Hofmann and Ramaj, 2011; Ögüt, Raghunathan, and Menon, 2011) or adverse selection and moral hazard issues (e.g., Gordon, Loeb, and Sohail, 2003). More recent research is concerned with potentially huge losses from worst-case scenarios such as the breakdown of critical information infrastructure (e.g., WEF, 2010; Cambridge Center for Risk Studies, 2014; Lloyd's, 2015; Long Finance, 2015). In short, the literature highlights challenges in the insurability of cyber risks.

[1] The premium volume in the US is estimated at US$ 2.4 billion, the European premium volume is estimated at US$ 0.2 billion; see Advisen (2015).

Challenges in the insurability of cyber risks thus hamper the development of a cyber-insurance market. However, recent studies and discussions with stakeholders in the insurance and reinsurance industry clearly illustrate the growing interest in the topic and show that the companies would be willing to enter the cyber-insurance market, if the insurability of cyber risk is improved. In this context some market participants emphasize the need for within-industry collaboration and some even call for government intervention and mechanisms like those already in place for catastrophic risk from natural events (Gray, 2015). We build upon these discussions and analyze the question of how risk transfer for cyber risk can be organized.

To our knowledge this study is the first to systematically discuss and compare potential risk transfer options for cyber risk. For this purpose we compare four risk transfer options and then consider the potential role of the government and insurance pools in improving the insurability of cyber risks. On the methodological side we use both qualitative (Berliner's insurability framework) and quantitative analyses (scenario analyses in an expected utility framework). Scenario analysis is a meaningful way to probe how the proposed risk transfer options might handle the financial implications of cyber-related scenarios.

Our main findings are that the cyber risks "of daily life" are not too big to insure, but "extreme scenarios" are. Based on these observations we recommend improving the insurability of "daily life" cyber risks by creating within-industry collaborations (e.g., by establishing data pools). To improve the insurability of "extreme scenarios" we propose having government take measures such as setting minimum standards for self-protection and reporting requirements for cyber incidents – measures which also improve the insurability of the "daily life" cyber risks. Our results are supported both by the results of our theoretical analysis and by the feedback of market participants who were part of our feasibility study. Overall, this study identifies meaningful concepts to improve the insurability of cyber risk.

To reach this aim, we first analyze the definition and nature of cyber risk (Section 2). How is cyber risk different from other types of risk? To answer this question, we provide statistical information on historical cyber losses along with an overview of today's cyber insurance market. From this summary we derive the central properties of cyber risk that hamper the insurability. Then in Section 3, we discuss potential risk transfer mechanisms for cyber risk, starting with private risk pools, over conventional insurance, reinsurance and capital markets to the government. In Section 4, we analyze several risk transfer options (Section 3) in light of the special nature of cyber risk

(Section 2). The question is which risk transfer option is attractive under which scenario. In Section 5 we discuss in greater detail the establishment of an insurance pool and the role of the government. Section 6 presents results of a survey among stakeholders on the feasibility of the suggested solutions. Finally, we conclude in Section 7.

2 What are the Central Properties of Cyber Risk?

2.1 Definition of Cyber Risk

The term "cyber risk" encompasses to a multitude of sources of risk affecting the information and technology assets of a firm, governments or individuals. Some prominent examples of cyber risk are outlined by the National Association of Insurance Commissioners (NAIC, 2013) and include identity theft, disclosure of sensitive information, and business interruption. Many attempts have been made to define "cyber risk." Table 1 lists several definitions of the term. Some of these definitions are rather narrow; for example, Mukhopadhyay et al. (2005, 2013) associate cyber risk with malicious electronic events that cause disruption of business and monetary loss. Others take a broader perspective by linking it to information security (Ögüt, Raghunathan, and Menon, 2011) or to the failure of information systems (e.g., Böhme and Kataria, 2006).

Table 1 Definition 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 und Kataria (2006)	Failure of information systems
Cebula and Young (2010)	Operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems
Ögüt, Raghunathan, and Menon (2011)	Information security risk
National Association of Insurance Commissioners (NAIC, 2013)	Provides typical examples to describe cyber risk: e.g., identity theft, disclosure of sensitive information and business interruption
Swiss Re (2014)	Any risk emanating from the use of electronic data and its 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 insurance addresses the first- and third-party risks associated with e-business, the internet, networks and informational assets.[2]

The term "cyber" is short for the word "cyberspace," which is generally understood as the interactive domain composed of all digital networks used to store, modify, and communicate information. It includes all information systems used to support businesses, infrastructure, and services (GCHQ, 2012). We employ a broad definition of cyber risk, one that is based on how regulators of insurance and financial markets categorize cyber risk – that is, as operational risk. However, we focus on operational cyber risk here, referring to those operational risks relevant for information and technology assets. We thus define cyber risk as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or

[2] In particular, cyber risk encompasses also material/physical damage, which is often provided in traditional coverages, as well as damage to (intangible) electronic data and liabilities arising therefrom, which is often only available through a specific policy.

integrity of information or information systems" (Cebula and Young, 2010).[3] Following the operational risk frameworks in Basel II (BIS, 2006) and Solvency II (CEIOPS, 2009), we categorize cyber risk into four classes: (1) actions of people, (2) systems and technology failures, (3) failed internal processes, and (4) external events.[4]

It should be noted that the classification of cyber risk very much depends on the context. For buyers of cyber insurance, cyber risk can be interpreted as an operational risk. For insurance companies, however, the allocation of cyber risk depends on which part of the business is considered. If we consider insurance companies as providers of insurance coverage, then cyber risk is an insurance risk. If, however, we consider an insurance provider as a company that can be hacked, for example, then cyber risk is again interpreted as operational risk. The allocation of cyber risk thus depends on the context. In this study we consider both contexts. For the sake of data identification, we look at cyber risk as part of operational risk in different firms (including insurance companies).

Table 2 shows a more detailed categorization of cyber risk based on its source. The group of non-criminal sources consists of acts of nature, technical defects and human failure. Criminal sources can be separated into physical attacks, hacker attacks and extortion.

[3] An advantage of the definition in Cebula and Young (2010) is that we can categorize cyber risk into four classes following the Basel II and Solvency II frameworks. A further advantage is that there are databases for operational risk, from which cyber risk incidents can be identified.

[4] More details on the categorization, with examples, are presented in Appendix B. Note that reputational risk is typically excluded when operational risk is considered; see, e.g., BIS (2006). Reputational effects, however, are an important aspect of cyber risk so they should be (and are) included in the discussion (potential approaches for modeling: Cummins, Lewis, and Wei, 2006 or Cannas, Masala, and Micocci, 2009).

Table 2 Sources of Cyber Risk

Non-criminal Sources	
Act of nature	Power outage after a natural catastrophe, destruction of servers or computer facilities by flooding, fire, etc.
Technical defects	Hardware failure, e.g., data loss after a head crash of the hard-drive or a computer crash; bug in software
Human failure	Unintentionally disclosure of information on webpage, false report
Criminal Sources (Cybercrime)	
Physical attacks	Physical data theft, e.g., theft of confidential bank data by an employee
Hacker attacks	Espionage of customer data or sabotage of company processes, e.g., DoS attack, key logger, or malware[5] (virus, worms, spam-mails, Trojan horses)
Extortion	Threats by internet, e.g., Mexican drug cartel

In Table 3 we qualitatively derive the main characteristics of cyber risks in comparison to other risk categories. Panel A compares cyber with the general categories of property and liability risk, while Panel B looks at the specific risk categories of terror, catastrophic (or cat) and operational risk. In contrast to the property and liability category it is notable that cyber risk is a mixture of short- and long-tail risks, which can be of a first- and third-party nature. Cyber risk thus is a combination of both categories. In contrast to the terror and cat risk one striking result is that cyber is a low frequency/high severity risk with respect to extreme scenarios, but it also has a high frequency component, which we could call the cyber risks "of daily life" (e.g., hacker attacks). Again it seems that unlike other risk categories, that cyber is a mix of categories.

[5] DoS stands for Denial-of-Service Attack. This instrument tries to paralyze a (computer) system by, for instance, sending a massive number of emails simultaneously to that system. A key logger is software which gathers the keyboard entries of a user and transmits it to the attacker. The goal is to gain access to passwords and credit card information. Malware describes every kind of malicious software, such as viruses or worms.

Table 3 Main Characteristics of Cyber Risk

Panel A – Comparison with Property and Liability				
#	Definition	Property Risk	Liability Risk	Cyber Risk
Time Horizon	Short tail vs. long tail	Mostly short tail	Mostly long tail	Can be both, but usually short tail[6]
Risk nature	First vs. third party (property vs. liability)?	First party	Third party	Both, but focus more on property than on liability[7]
Frequency	High frequency vs. low frequency	High frequency (e.g., motor insurance; extreme weather events is the Top 2 and natural catastrophes is the Top 6 risk by likelihood, see WEF, 2015)	Low frequency (e.g., law suits)	- Small losses are rather high frequency business (data fraud or theft is Top 9, cyber attack is Top 10 by likelihood, see WEF, 2015) - Blackout scenario is rather low frequency
Severity	High severity vs. low severity	Wide variety of severity levels possible (e.g., low severity for motor insurance, high severity in fire insurance/natural catastrophe insurance)	Wide variety of severity levels possible (e.g., lawsuits can produce a wide range of losses, product liability processes, e.g., Volkswagen)	- Small losses are common (hacker attack) - Blackout scenario rather high severity (critical information infrastructure breakdown is Top 7 by severity, see WEF, 2015)
Measurability	Measureable vs. not measurable	Relatively easy to measure	In some instances, not easily measurable in advance (e.g., legal costs, claims of damages)	- Small losses rather easily measurable (hacker attack) - Blackout scenario not measurable
Independence	Independent vs. correlated	Can be closely correlated (e.g., hail damages)	In general are not correlated; however, there might be incidents in which losses accumulate (e.g., class action lawsuit)	- Small losses rather independent (hacker attack) - Blackout scenario closely correlated losses (all stakeholders are affected)
Standardization	Is the definition standardized (e.g., standardized insurance coverage)?	In general yes	In general yes	Definition no; coverage no

[6] To answer this question at least for our dataset (Table 4), we compare the actual year of settlement (i.e., the year in which the loss materialized) and the first year of the event (i.e., when the actual loss occurred). For cyber risk the average difference is 4.03 years (standard deviation 4.05 years), and for the operational risk the average is 6.06 years (standard deviation 8.19 years). This indicates the average period from occurrence to settlement is longer for operational risk than for cyber risk, so the note made here (can be both, but rather short tail) seems reasonable in comparison with operational risks.

[7] The data sample analyzed in Section 2.2 shows about 60% property, and 20% liability losses. In the remaining 20% both types were present (e.g., an incident in the Target Corporation produced losses at Target but also for a third party, Union First Market Bancshares Corp.).

Panel B – Comparison with Terror, Cat and Operational Risk					
#	Definition	Terror Risk	Cat Risk	Operational Risk	Cyber Risk
Time Horizon	Short tail vs. long tail	Short- and long-tail	Short tail	Short- and long-tail	Can be both, but usually short tail
Risk nature	Property vs. liability (first or third party)?	In general first party, but also third party	First party	both	Both, but focus more on property than on liability
Frequency	High frequency vs. low frequency	Low	Low	- Small losses are rather high frequency business - Extreme losses are rather low frequency	- Small losses are rather high frequency business (data fraud or theft is Top 9, cyber attack is Top 10 by likelihood, see WEF, 2015) - Blackout scenario is rather low frequency
Severity	High severity vs. low severity	High	High	- Small losses are common (theft if not cyber) - Blackout scenarios, which then would be high severity, conceivable (e.g., nuclear catastrophe in Chernobyl, product failure)	- Small losses are common (hacker attack) - Blackout scenario rather high severity (critical information infrastructure breakdown is Top 7 by severity, see WEF, 2015)
Measurability	Measureable vs. not measurable	Daily terror measurable, e.g., political risk indices; extreme events not well measurable (e.g., 9/11)	Yes	In most instances not measurable in advance	- Small losses rather easily measurable (hacker attack) - Blackout scenario not measurable
Independence	Independent vs. correlated	Can be closely correlated	Can be closely correlated (e.g., hail damages)	In general rather uncorrelated	- Small losses rather independent (hacker attack) - Blackout scenario closely correlated (all stakeholders are affected)
Standardization	Is definition standardized (e.g., standardized insurance coverage)?	Definition yes; coverage no	Definition yes; coverage relatively standardized (e.g., cat bonds)	Definition yes; coverage no	Definition no; coverage no

2.2 Statistical Information on Cyber Risk

In order to give a sense of the economic magnitude and the statistical properties of cyber risk, we first present publicly available information on cyber losses. Then, in a second step we present the results of an own empirical study which relies upon operational risk data.[8] The goal is to lay an empirical basis for the scenario analysis in Section 4.

It is very difficult to estimate the economic magnitude of cyber risk using publicly available information since there is no unique and accepted source of such information. There are some estimates which are often cited, but these must be interpreted with caution given that many of them are published by data security firms.[9] Symantec (2013), for example, estimates the total global costs of cybercrime at US$ 113 billion; McAfee (2014) estimates the annual cost to the global economy from cybercrime to be even more than US$ 400 billion.[10] AGCS (2015) has estimated the total cost of cybercrime per year for the global economy to be US$ 445 billion.[11] All these results illustrate that the publicly available estimates vary greatly. In any case, the reported losses are in the hundreds of billions of US dollars, emphasizing the economic relevance of cyber events. On a more disaggregated level, the Ponemon Institute (2015b) finds that data breaches result in an average financial impact of US$ 3.8 million. This average values of a "data

[8] The empirical study relies upon an extended version of the dataset considered in Biener, Eling, and Wirfs (2015).

[9] These firms might have an incentive to present large numbers. See Anderson et al. (2013) who discuss methodological flaws of such estimates and suggest an improved alternative, which also yields a number in the hundreds of billions of US dollars. However, Anderson et al. (2013) write that an aggregate measure of the cost of cybercrime is meaningless, given the huge number of assumptions.

[10] While Symantec estimates only direct costs, McAfee (2014) looks at both direct and indirect costs and takes into account the loss of intellectual property, the theft of financial assets and sensitive business information, opportunity costs, additional costs for securing networks, and the cost of recovering from cyberattacks, including reputational damage to the hacked company. Based on this, the likely annual cost to the global economy from cybercrime is more than US$ 400 billion. A conservative estimate would be US$ 375 billion in losses, while the maximum could be as much as US$ 575 billion. According to McAfee (2014) financial losses from cyber risk could cause as many as 150,000 Europeans to lose their jobs. There are also other estimations for the global costs of cybercrime, ranging from US$ 100 billion to US$ 1 trillion, see, e.g., Kshetri (2010).

[11] AGCS (2015) also provide a country ranking by GDP for the world's top 10 economies: 1. US: US$ 108 billion estimated costs (0.64% of GDP); 2. China: US$ 60 billion estimated costs (0.63% of GDP): 3. Japan: US$ 980 million estimated costs (0.02% of GDP); 4. Germany: US$ 59 billion estimated costs (1.60% of GDP); 5. France: US$ 3 billion estimated costs (0.11% of GDP); 6. UK: US$ 4.3 billion estimated costs (0.16% of GDP); 7. Brazil: US$ 7.7 billion estimated costs (0.32% of GDP); 8. Russia: US$ 2 billion estimated costs (0.10% of GDP); 9. Italy: US$ 900 million estimated costs (0.04% of GDP); 10. India: US$ 4 billion estimated costs (0.21% of GDP).

breach" varies by country: approximately US$ 6.5 million in the US, US$ 4.9 million in Germany, US$ 4.3 million in Canada and France, and US$ 3.7 million in the UK (Ponemon Institute, 2015b).[12] KPMG (2013) estimates average losses from theft of data at US$ 2.1 million. According to Kaspersky Lab (2013) a successful targeted attack on a large company's IT infrastructure can cost US$ 2.4 million on average. Ponemon Institute (2015b) also provides information on the cost of data breach per record (US$ 217 (US), US$ 211 (Germany), US$ 207 (Canada), US$ 186 (France), and US$ 163 (UK). Symantec (2013) estimated the average cost per victim of cybercrime (US$ 298; up from US$ 197).[13]

For our empirical analysis of cyber risk we rely on the dataset used in Eling and Wirfs (2016) —the SAS OpRisk Global Data—which is the world's largest collection of publicly reported operational losses. The database consists of 26,541 incidents of operational loss that were reported between January 1995 and March 2014. The incidents occurred all over the world and each loss is categorized in accordance with the Basel II event and effect classification standard (BIS, 2006). Furthermore, all observations are partitioned into business and sub-business lines. All losses are adjusted by currency and a consumer price index so as to make them comparable. The dataset estimates the complete costs of operational risk events (both direct and indirect effects); however, reputational loss due to an operational risk event is not covered since this sort of loss is typically excluded from operational risk.

Based on this dataset, we identified cyber risk incidents based on the definition given in Section 2.1. Specifically, to be categorized as a cyber risk, the event must meet three criteria: (1) a *critical asset* such as a company server or database needs to be affected, (2) a relevant *actor* needs to be involved in causing the incident (e.g., hackers, employees, system, nature), and (3) a relevant *outcome* such as the loss of data or

[12] The Ponemon Institute (2015a) in a second survey on cybercrime also identifies variation in total average costs of cybercrime over the countries: US US$ 15.42 million, Germany US$ 7.5 million, Japan US$ 6.81 million, UK US$ 6.32 million, Brazil US$ 3.85 million, Australia US$ 3.47 million, and Russia US$ 2.37 million.

[13] The mean estimates from our own empirical study are higher since extreme scenarios are also included in our data, while the other references consider only the data breaches "of daily life"; moreover, there might be reporting effects involved: Ponemon Institute (2015b) for instance, collects data from more than 1,500 separate interviews in organizations that had faced a data breach incident. Our dataset is conducted from losses reported in the media. Only looking at incidents that are directly related to data breach in our empirical study, the average and median loss is given by about US$ 9 million and US$ 3 million and thus comparable to those estimations in the industry, resulting in single-digit US$ million numbers per event when the median is considered.

misuse of confidential data needs to be present. For each category we defined a comprehensive set of keywords, which we then scanned for in the incident descriptions of our SAS OpRisk Global Data database (Appendix C for details). The resulting dataset includes a total of 1,579 cyber risk incidents, which is about 5.9% of the total sample of operational risks.

Table 4 summarizes the cyber risk sample and compares its characteristics with those of non-cyber risk. All the descriptive statistics for cyber risk (mean, median, standard deviation, value at risk (VaR), tail value at risk (TVaR), etc.) are significantly smaller than those for non-cyber risk, i.e., the other operational risks.[14] The maximal loss in our sample is US$ 14.6 billion compared to US$ 97.7 billion for non-cyber risk.[15] Thus, both on average as well as in extreme cases, the loss amounts for cyber risk are much smaller than for other operational risks.[16]

Table 4 Losses per Risk Type (in million US$)

Category	N	Mean	Std. dev.	Min.	Quantiles			VaR	TVaR	Max.
					25%	50%	75%	(95%)	(95%)	
Panel A: Cyber versus non-cyber risk										
Cyber risk	1,579	43.49	426.36	0.10	0.43	1.53	7.43	100.55	730.52	14,589
Non-cyber risk	24,962	98.52	1,154.39	0.10	1.39	5.09	24.45	271.60	1,565.81	97,687
Panel B: Cyber risk subcategories										
Actions of people	1,203	42.66	475.53	0.10	0.42	1.35	5.39	77.75	743.20	14,589
Systems and technical failure	212	45.32	141.23	0.10	0.57	4.78	26.98	232.56	485.10	1,668
Failed internal processes	108	15.12	48.96	0.10	0.36	1.32	7.45	65.62	179.91	372
External events	56	109.12	431.92	0.10	1.04	4.25	19.53	331.06	1,585.58	2,949

The cyber risk subcategories (Panel B of Table 4) show that most of the cyber risk incidents occur in the "actions of people" subcategory. Hacking attacks, physical information thefts, human failures, and all incidents where employees manipulate data are included here. It thus seems that human behavior is the main source of cyber

[14] Mean and median are close to estimations of average losses found in the literature; Ponemon Institute (2013) finds that security and data breaches result in an average financial impact of US$ 9.4 million. Average losses from the theft of data are estimated at US$ 2.1 million by KPMG (2013).

[15] The largest cyber risk case occurred at the Bank of China in February 2005 when US$ 14,589.15 million were laundered through one of its branches, which was possible because the bank's internal money-laundering controls were manipulated by employees. The largest non-cyber risk case involves the US tobacco company Philip Morris, which, in November 2001, was ordered to pay US$ 97,687.34 million in punitive damages to sick smokers.

[16] Cyber risk policies (in Switzerland) typically cover a maximum such as US$ 50 million. Actual cover limits vary. If US$ 50 million is the limit, then 92% of the cases in our sample would be covered completely by the policy.

risk, while the other categories, such as external disasters, are very rare. The average losses across the different subcategories, however, are similar.[17]

To compare the distributional characteristics of cyber risk to those of operational risk, we follow Hess (2011) and estimate the loss severity distribution (Appendix D). The estimation is conducted by means of a spliced distribution, where a generalized Pareto distribution (GPD) models the tail. The results show that the distribution of cyber risk differs considerably from the distribution of other operational risk (the plots in Figure 1). For example, the distribution of the non-cyber risk sample is much more heavily tailed than that of the cyber risk sample, explaining in part the much higher maximal losses in these categories.[18] This finding implies that when modeling operational risk, cyber risk needs to be considered separately.[19]

Why does cyber risk look different? One first obvious observation is that some cyber risks are smaller than other operational risk. We will call those risks the "cyber risks of daily life." A second obvious observation is that the cyber risks in the historical data analyzed here do not show such extreme scenarios like the historical operational risk data. We will discuss this in more detail in the context of an extreme scenario for cyber risk. At the end of this section we will identify the distinctive characteristics of cyber risk.

Table 5 separates the cyber and non-cyber risk loss data into several subcategories. The geographic separation (Panel A) shows that Northern American companies experience about twice as many (52.6%) cyber risk incidents as European firms (24.9%) and even more than twice as many as firms located on other continents. This might be due to mandatory US reporting standards, which other continents do not have in place yet. For loss severity, Asia shows the highest average loss, whereas Europe and Northern America have much smaller ones. This may be because North American and European firms are more capable of and willing to invest in risk mitigation for heavy losses,

[17] The higher mean loss for category "External events" is due to the very small sample and a very high maximal value (average without that maximal value amounts to US$ 57.50 million).

[18] The modeled VaR for non-cyber risk is more than twice as high as for cyber risk.

[19] In the operational risk literature, typically models of extreme value theory and spliced distribution are used. In light of the result that cyber risk differs significantly from other operational risk, the question arises as to whether the usual methods of modeling operational risk are appropriate for modeling cyber risk or whether other methods should be used.

resulting from a longer tradition of recognizing and managing cyber risks than Asia's.[20]

Table 5 Cyber and Non-cyber Risk Losses (in million US$)

	Cyber Risks				Non-cyber Risks			
	N	Share of cyber risk incidents	Mean	Median	N	Share of non-cyber risk incidents	Mean	Median
Panel A: Region of domicile								
Africa	24	1.52%	30.90	1.86	278	1.11%	58.72	2.59
Asia	256	16.21%	104.31	1.52	3,375	13.52%	132.95	4.04
Europe	393	24.89%	31.09	1.78	5,596	22.42%	121.01	5.49
North America	830	52.56%	33.26	1.42	14,867	59.56%	85.31	5.27
Other	76	4.81%	18.44	1.55	846	3.39%	57.44	4.47
Panel B: Industry								
Nonfinancial	381	24.13%	84.11	4.47	13,665	54.74%	114.31	7.43
Financial	1,198	75.87%	30.57	1.16	11,297	45.26%	79.40	2.92
Panel C: Relation to losses in other firms								
One firm affected	1,283	81.25%	49.21	1.56	17,748	71.10%	87.59	5.02
Multiple firms affected	296	18.75%	18.65	1.45	7,214	28.90%	125.40	5.30
Panel D: Company size by number of employees[*]								
Small	67	4.24%	19.71	1.29	732	2.93%	33.27	1.97
Medium	73	4.62%	13.35	1.09	1,193	4.78%	27.81	2.17
Large	1,375	87.08%	46.17	1.49	20,005	80.14%	112.55	5.63

[*]: Small: Fewer than 50 employees; Medium: Less than 250, Large: More than 250. The total in each size group does not add up to the total sample, since for a few incidents, the number of employees is not available.

Panel B of Table 5 separates the financial from the nonfinancial services industries. According to the results, 75.9% of all cyber risk incidents occur in the financial services industry.[21] This is not surprising since financial services firms, such as banks and insurance firms, store a significant amount of critical personal data.[22] However, the average loss resulting from cyber risk for firms in nonfinancial services industries is almost three times as high as for financial services firms. This finding might be explained by financial services firms having a higher awareness of their critical data and better protection against cyber risk. For non-cyber risks, firms in the nonfinancial

[20] Similar patterns can be observed also for the non-cyber risk sample, although companies from Europe show much higher average losses than Northern American companies.

[21] We also split the data into pre 2012 (1995-2011) and post 2012 (2012+) and analyzed if those ratios significantly changed over time. This is not the case: in group pre 2012 about 75.4% of all incidents occurred in financial services, while in the post 2012 group this were 78.7%.

[22] The market survey of potential customers in the financial services industry (Biener et al., 2015) shows that banks are especially prone to cyber risk, i.e., the respondents from the banking sector had significantly more experience with cyber risk than the respondents from other financial service sectors.

services industries also face higher average losses than firms in the financial services sector; however, the difference is not as substantial.

An important aspect of cyber risk is contagion, and thus our next separation of the data is between incidents affecting only a single firm and those affecting multiple firms (Panel C of Table 5). If just one firm is involved (81.3% of the cyber risk cases), the average loss per firm per case is more than twice as high as if more than one firm is involved. This result may appear counterintuitive; however, in the event that more than one firm is affected, cyber attacks are identified earlier and thus losses can be limited. At the same time, there may be economies of scale in solving the problems created by cyber incidents when multiple firms are involved (e.g., forensic investigation costs).

Panel D of Table 5 separates the sample based on firm size. With increasing size, the number of incidents increases; firms with more than 250 employees have more cyber losses. Interestingly, we observe a U-shaped pattern in the mean losses both for cyber and non-cyber risk.[23] It may be that smaller firms do not have the ability and resources to protect against cyber risk, while large firms have diseconomies of scale due to complexity.[24]

Another piece of evidence in this context is that firms with a CISO (Chief Information Security Officer) or equivalent have lower average costs when a breach occurs (US$ 157 per record versus US$ 236 per record for firms without strategic security leadership; see Shackelford, 2012).[25] The institutional commitment demonstrated by having a person responsible for information security thus decreases the average loss per event. The average loss per event thus depends on size, effectiveness of self-protection, and institutional commitment.

---

[23] The results are robust with regard to the size categorization. We estimated the values for a separation into Small: less than 100, Medium: less than 1,000, and Large: more than 1,000 employees and find no differences in this pattern.

[24] We also analyzed the development of cyber risks over time and found that the number of cyber risk incidents was rather small before 2000. After that point, however, the number of incidents continuously increased and in the last years accounts for a substantial part of all operational risk incidents in our database. These findings again emphasize the increasing economic importance of cyber risk in recent years. The average loss, however, has decreased over the last several years, which might indicate the increasing use of self-insurance measures that reduce the loss amount in the event of a cyber attack. Detailed results are available from the authors upon request.

[25] Shackelford (2012) only considers data breaches and no other types of events (such as, e.g., business interruption).

In Table 6 we pick up two datasets from the property and liability domain, which are often used in academic literature and compare the statistical properties with those of cyber risk and operational risk. The table presents the number of observations, mean, standard deviation, skewness, excess kurtosis, minimum and maximum, the 95% quantile (VaR), and the mean loss, if the loss is above 99% (TVaR). We consider the following datasets (collected from packages available under the R Project for Statistical Computing):

- Property (1) – Danish Fire Losses (package fExtremes): represents Danish fire losses measured in 1 million Danish kroner
- Property (2) – French Business Interruption claims data (package CASdatasets): French business interruption losses from 1985 to 2000 in 100,000 French Francs
- Liability (1) – US Indemnity Losses (package copula): contains general liability claims, given for each the indemnity payment in thousands US$
- Liability (2) – Swedish Motor Insurance TPL claims (package CASdatasets): included here are third-party automobile insurance claims from 1977; losses are given in thousands Swedish kronor.

Table 6 Empirical Comparison of Risk Data (in million US$)

Category	N	Mean	Std. dev.	Min.	Median	VaR (95%)	TVaR (95%)	Max.	Skew-ness	Excess-Kurtosis
Panel A: Absolute Numbers										
Cyber risk	1,579	43.49	426.36	0.10	1.53	100.55	730.52	14,589.00	27.12	873.33
Operational risk	24,962	98.52	1,154.39	0.10	5.09	271.60	1,565.81	97,687.00	49.95	3,388.68
Property (1) – Danish Fire	2,167	3.39	8.51	1.00	1.78	9.97	24.08	263.30	18.74	482.20
Property (2) – French Business Interruption	2,387	388.80	1,119.33	17.64	142.30	1,474.31	3,245.94	30,360.00	17.15	417.35
Liability (1) – US Indemnity	1,500	41.21	102.75	0.01	12.00	170.40	373.81	2,174.00	9.15	141.98
Liability (2) – Swedish Motor Insurance (TPL)	1,797	312.10	1,113.33	0.07	43.36	1,394.49	3,909.19	18,250.00	8.29	89.78
Panel B: LN Losses										
Cyber risk	1,579	0.76	2.06	-2.30	0.43	4.61	5.84	9.59	0.79	0.39
Operational risk	24,962	1.79	2.16	-2.30	1.63	5.60	6.61	11.49	0.38	-0.09
Property (1) – Danish Fire	2,167	0.79	0.72	0.00	0.58	2.30	2.92	5.57	1.76	4.18
Property (2) – French Business Interruption	2,387	5.08	1.21	2.87	4.96	7.30	7.86	10.32	0.54	0.02
Liability (1) – US Indemnity	1,500	2.47	1.64	-4.61	2.49	5.14	5.78	7.68	-0.15	0.32
Liability (2) – Swedish Motor Insurance (TPL)	1,797	3.77	1.98	-2.63	3.78	7.24	8.04	9.81	0.16	-0.17

The descriptive statistics in Panel A of Table 6 show that the property losses are more extreme with respect to skewness and kurtosis than the considered liability losses. For example, values for skewness and kurtosis are around 9.15 and 141.98 for the US indemnity losses; the corresponding values for the Danish fire losses are 18.74 and 482.20. Both the indemnity and the fire data are thus significantly skewed to the right and exhibit high kurtosis.[26] These characteristics are also reflected in the relatively high

[26] Tests for normality, such as the Jarque-Bera test, are rejected at very high confidence levels. See Jarque and Bera (1987) for the test.

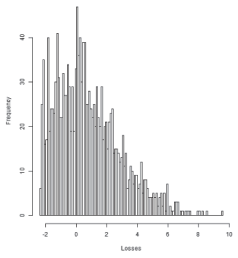
values for value at risk and tail value at risk. Comparing the property and liability data with the operational risk data shows that operational losses are much more extreme (skewness of 49.95, kurtosis of 3,388.68). This extreme behavior, especially in the tail of the distribution, is why for operational risk specific modeling approaches from extreme value theory are used (e.g., the peaks over threshold approach; see, e.g., McNeil, Frey, and Embrechts, 2015). We also see that cyber risks are not as extreme as the operational risk data, but more extreme than the property and liability datasets.

In Panel B of Table 6, we analyze the logarithm of the loss data. Consideration of logarithmic data is a widespread practice in statistics and actuarial science in order to decrease extreme values of skewness and kurtosis for modeling purposes (e.g., Bolancé et al., 2008). We still see deviations from normality with the liability loss data, but the tails are not very extreme. In addition, the Danish fire data are now also less extreme with a kurtosis value of 4.2. Figure 1 presents the histograms and normal Q-Q plots for the six datasets after taking the natural logarithm of all data values. After taking the natural logarithm, the liability loss data looks much more like the normal distribution, whereas the fire losses distribution is still skewed to the right.[27] The cyber and operational risk datasets also converge towards the normal distribution, but the graphical inspection of the pictures still emphasizes heavy right tails of both these two distributions. Cyber risk and operational risk are thus more extreme than other loss categories, which make them very difficult to model.

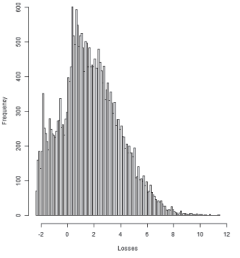
[27] One reason why the log of the Danish fire data is skewed is that the original data are truncated at 1, resulting in a minimum value of 0 for the log data. The US indemnity data are not truncated at 1 so that negative values for the log data are possible.

Figure 1 Graphical Comparison of Losses (Histogram + Q-Q Plots)

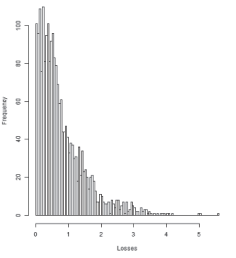
Panel A: Histogram



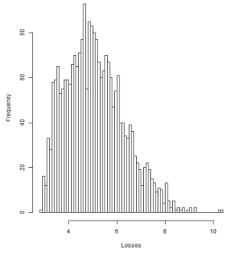
(A1) Cyber Risk



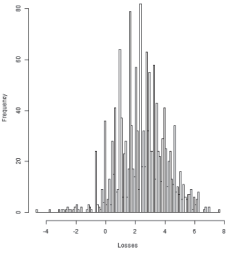
(A2) OpRisk



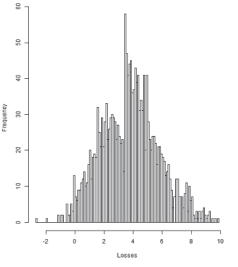
(A3) Property (1)



(A4) Property (2)

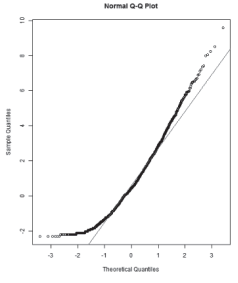


(A5) Liability (1)

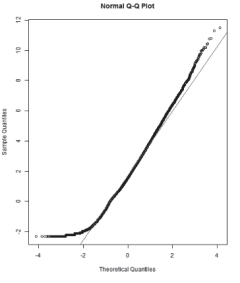


(A6) Liability (2)

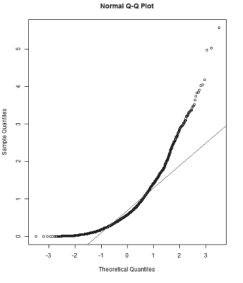
Panel B: Q-Q Plots



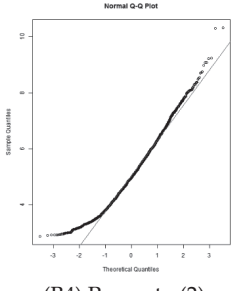
(B1) Cyber Risk



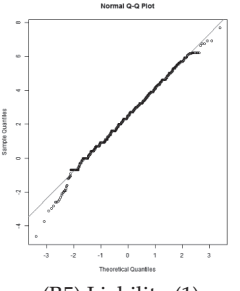
(B2) OpRisk



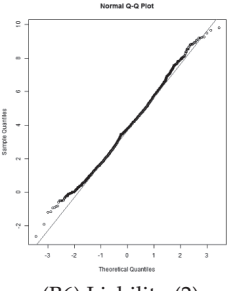
(B3) Property (1)



(B4) Property (2)



(B5) Liability (1)



(B6) Liability (2)

2.3 Market for Cyber Insurance

Commercial property and liability insurance is available in most insurance markets worldwide.[28] However, most property policies only cover damage to physical assets such as production facilities, and exclude cyber risk, as is generally the case with liability policies. Possibly in response to this situation, a specialized market providing coverage for cyber risks has emerged in recent years, most prominently in the United States.

As yet, however, market coverage is small. Moreover, outside the United States, insurance coverage for cyber risk is not well known and little used. In Europe, for example, about 25% of corporations are not even aware that this type of insurance exists and only 10% have purchased cyber risk coverage (Marsh, 2013). Figures for the United States show a similarly low average level of coverage of about 6%, but large variations between industries among the Fortune 1000 companies (Willis, 2013b).[29] According to Betterley (2015), current annual gross premiums for cyber insurance in the United States are US$ 2.75 billion and growing 26–50% on average per year. Advisen (2015) estimates the premium volume for the US market in 2015 already in the neighborhood of 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 about US$ 18 billion until 2025 (Swiss Re, 2015).

In summary the cyber insurance market is very small at present, but expected to increase significantly. The US market is much more developed than its European counterpart, partly because the US has had reporting requirements for cyberattacks in place for several years. Violations of these reporting obligations incur heavy fines. The new regulations have considerably increased the awareness of cyber risk. Now, discussions about the introduction of reporting obligations are taking place in the European Union. Thus, new regulatory approaches will be an important driver in the development of the cyber insurance market.

---

[28] Note, that the majority of the discussion on cyber insurance is referring to the commercial insurance market. 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 study focuses on the commercial insurance market.

[29] According to Willis (2013b), about 20% of all financial services companies have cyber risk coverage, whereas manufacturing (2%) and health care (1%) have the lowest share of companies covered. Another recent market survey for the United States by the Harvard Business Review Analytic Services (2013) finds that among 152 companies, market coverage is 19%.

Table 7 summarizes the market estimations for different markets. The results emphasize the high uncertainty in the cyber risk topic. There are no generally accepted sources of information and the estimations by market participants vary substantially.

Table 7 Estimations for the Cyber Insurance Market

Global

- Cyber insurance market is estimated to US$ 2 billion and expected to grow to about US$ 5 billion in the next 5 years / by 2020 (Guy Carpenter, 2015)
- Market is estimated to be about US$ 2 billion in yearly premiums worldwide, with US business accounting for approximately 90% (AGCS, 2015)
- Market is expected to grow by double-digit figures year-on-year and could reach US$ 7.5 billion by 2020 (PwC, 2015a) and US$ 20 billion in the next 10 years (AGCS, 2015)
- Predictions by Swiss Re (2015) estimate a global cyber market premium volume at up to US$ 18 billion by 2025.
- 50-60 insurer offer standalone cyber insurance worldwide; market leaders include AIG, ACE Limited, Beazley PLC, Lloyds of London, and The Chubb Corporation (Advisen, 2015).

US

- The premium volume in the US is estimated to be US$ 2.4 billion in 2015 (Advisen, 2015; Aon Benfield, 2015).
- Premium Volume in US$ million (Advisen, 2015)

	US	**Europe**
2012	1,300	46.1
2013	1,800	69.7
2014	2,100	123.0
2015	2,400	224.2
2016	NA	426.0

- Premium volume: US$ 2.75 billion (Betterley, 2015) compared to US$ 2 billion in 2014 (Marsh, 2014; Betterley, 2014) and US$ 1.3 billion in 2013 (Betterley, 2013)
- Average growth rates per year: 26-50% (Betterley, 2015)
- Penetration is estimated at 16% across all sectors with higher penetration in health care (50%), education (32%) and hospitality (26%) (Statista, 2015)
- Expected increase to 5.9 billion US$ until 2023 (Swiss Re, 2014)
- Predictions by Swiss Re (2015) estimate the US cyber market premium volume at up to US$ 8 billion (up to US$ 10 billion in the rest of the world).

Europe

- Premium volume about CHF 150 million (March, 2014)
- Volume increases by about 50-100% each year (Thomas and Finkle, 2014)
- Premium volume about US$ 224.2 million (Advisen, 2015)
- Expected gross written premiums by 2018: US$ 1.1 billion (Gould, 2013)
- Estimated volume of premiums in Switzerland: CHF 5 million; increase with factor 4 to 10 estimated in the next 5 years (Biener et al., 2015)

Owing to the new and evolving nature of the market, products and coverage change rapidly, and exclusions as well as terms and definitions vary significantly among competitors. Another distinctive aspect of cyber insurance is that the risks faced by corporations are often unique to its industry or even to the company itself, requiring a great deal of customization in policy writing. Company size, size of the customer base, web presence, and type of data collected and stored are important determinants of cyber insurance policy terms and pricing. Table 8 outlines typical cyber insurance policies.[30]

[30] See, e.g., Marsh (2012). Sometimes, reputational losses (e.g., NAIC, 2013; Ponemon Institute, 2013) and regulatory fines (e.g., Betterley, 2013; Ponemon Institute, 2013) are also covered by cyber insurance policies.

Table 8 Typical Cyber Insurance Policies

Coverage	Cause of cyber loss	Insured losses
Panel A: Third Party		
Privacy Liability	- Disclosure of confidential information collected or handled by the firm or under its care, custody, or control (e.g., due to negligence, intentional acts, loss, theft by employees)	- Legal liability (also defense and claims expenses (fines), regulatory defense costs) - Vicarious liability (when control of information is outsourced) - Crisis control (e.g., cost of notifying stakeholders, investigations, forensic and public relations expenses)
Network Security Liability	- Unintentional insertion of computer viruses causing damage to a third party - Damage to systems of a third party resulting from unauthorized access of the insured - Disturbance of authorized access by clients - Misappropriation of intellectual property	- Cost resulting from reinstatement - Cost resulting from legal proceeding
Intellectual Property and Media breaches	- Breach of software, trademark and media exposures (libel, etc.)	- Legal liability (also defense and claims expenses (fines), regulatory defense costs)
Panel B: First Party		
Crisis Management	- All hostile attacks on information and technology assets	- Costs from specialized service provider to reinstate reputation - Cost for notification of stakeholders and continuous monitoring (e.g., credit card usage)
Business Interruption	- Denial-of-service attack - Hacking	- Cost resulting from reinstatement - Loss of profit
Data Asset Protection	- Information assets are changed, corrupted, or destroyed by a computer attack - Damage or destruction of other intangible assets (e.g., software applications)	- Cost resulting from reinstatement and replacement of data - Cost resulting from reinstatement and replacement of intellectual property (e.g., software)
Cyber Extortion	- Extortion to release or transfer information or technology assets such as sensitive data - Extortion to change, damage, or destroy information or technology assets - Extortion to disturb or disrupt services	- Cost of extortion payment - Cost related to avoid extortion (investigative costs)

According to a study of Fortune 500 companies by Willis (2013a), these companies are most concerned with the loss of confidential data (68%), loss of reputation (42%), malicious acts (49%), and liability (41%). This ranking matches the findings in a study of European companies conducted by Marsh (2013). Available cyber risk policies thus seem to address the most pressing needs. However, if the available products are a good solution to business problems, why is market coverage so low? There are several answers to this question, including expensive premiums, ambiguous coverage, and the information asymmetries inherent in cyber risk, all of which will be discussed in the following section.

2.4 Insurability of Cyber Risk

Today's cyber insurance market is limited in terms of premium volume and coverage. To analyze why this is the case, Biener, Eling, and Wirfs (2015) discuss cyber risk beyond the background of the insurability criteria by Berliner (1982). The results (summarized in Table 9) outline the reasons for today's relatively small market. In the following we discuss the three most problematic aspects of insurability.

The first insurability criterion is the randomness of loss occurrence. For this criterion to be satisfied, the independence and predictability of losses needs to be given. This is not always the case for cyber risk, especially since cyber risk incidents are not always independent; thus the risk pooling might not always work appropriately. Pooling risks is additionally complicated by the fact that the risk pools for cyber risk are still small; the smaller the portfolio is, the more difficult it is to reach the full benefits of diversification. Another problem can be seen in the unpredictability of loss exposure, since losses are difficult to measure because of a lack of data. And even if there is data available, it is questionable whether or not the historical data is a meaningful indicator for the future, due to the dynamic nature of cyber risks and thus the risk of change.

Another significant problem in cyber insurance is information asymmetry. Companies that have experienced a serious cyber-attack are more likely to buy insurance (Shackelford, 2012), thus resulting in adverse selection. The insurers in the market try to alleviate adverse selection effects by screening (e.g., up-front audits), self-selection (e.g., questionnaires in the underwriting process), 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 lack of incentive to invest in self-protection measures following the purchase of insurance, if full coverage is offered. Insurers use instruments such as screening (e.g., audit) and risk sharing (e.g., deductibles, cover limits) to reduce moral hazard. Despite these manifold instruments, information asymmetries still pose a significant problem for the insurability of cyber risks. For instance, because of complex interrelations in modern IT systems, firms might be vulnerable to cyber risk even though they invested in self-protection. Thus, the benefit of self-protection investments in one company highly depends on the investments in other, connected firms. This might amplify moral hazard problems, because incentives for self-protection might be reduced even further. In addition, the lack of loss data aggravates a risk-adequate classification of policyholders, thus exacerbating the adverse section problem. This problem might become less relevant when data resources increase.

A third essential problem for the development of an insurance market are the coverage limits. The policies tend to cover only a small maximum loss (US$ 10 million to US$ 50 million, depending on the product and provider, see, for instance Biener et al., 2015; in some cases even up to US$ 100 million; see Finkle, 2015), and contain several exclusions (e.g., self-inflicted losses, accessing unsecure websites, or terrorism). Additionally, there might be indirect effects of cyber losses that cannot be measured and thus are not covered (e.g., reputational losses and their impact on stock prices). Another problematic aspect of coverage limits is the policy complexity. Given the large number of exclusions and the dynamic nature of cyber risk, there is uncertainty about what the cyber policy actually covers. Making this situation worse is that the policies in the market have no agreed-upon terminology, which makes the offerings very difficult to compare.

Table 9 Insurability of Cyber Risk

Insurability criteria	Main findings	Assessment
(1) Randomness of loss occurrence	- Correlation among risks hinders efficient pooling - Risk pools are too small and cannot be diversified; also, lack of adequate reinsurance (ENISA, 2012) - Lack of data - Changing nature of cyber risks (e.g., new standards, regulations)	*problematic*
(2) Maximum possible loss	- Maximum possible loss for cyber risk lower than for other operational risks - Insurers protect themselves against extreme losses by cover limits	*not problematic*
(3) Average loss per event	- Average loss for cyber risk lower than for other operational risks - Dependent on company size, self-protection, and institutional commitment for information security	*not problematic*
(4) Loss exposure	- Increasing number of cyber risk events - Dependent on event category (i.e., human actions dominate other event categories)	*not problematic*
(5) Information asymmetry	- Moral hazard poses a strong theoretical threat; regular risk assessments, deductibles, and cover limits help to reduce moral hazard - Adverse selection poses a strong theoretical threat; upfront risk assessments (screening) and signaling (e.g., ISO certificates) help to reduce adverse selection	*problematic*
(6) Insurance premium	- High premiums and other costs due to large uncertainties; expected to decline - Large geographic and industry variations in availability of policies - Low number of competitors; expected to increase over time - Additional costs (e.g., upfront risk assessments)	*increasingly less problematic*
(7) Cover limits	- Policies typically cover a maximum (e.g., US$ 50 million) - Policies contain exclusions (e.g., self-inflicted loss, accessing unsecure websites, terrorism) - Indirect costs (e.g., reputational effects) cannot be measured and often not covered - Product complexity can be problematic (lots of exclusions, dynamic risk nature, both for the insurance seller and buyer uncertainty regarding the actual coverage)	*problematic*
(8) Public policy	- Increase in overall industry exposure through cyber insurance is conceivable due to moral hazard incentives and high loss correlations in interrelated networks - Insurance fraud might be incentivized, since hacking attacks or physical attacks are difficult to detect and to trace back	*less problematic*
(9) Legal restrictions	- In many countries it is not allowed to insure regulatory fines - Risk of change (e.g., new legal standards and regulations) - Complexity and dynamic nature of this novel risk type might pose a potential legal threat for insurance brokers that limits their willingness to offer the product; only few specialists willing and able to sell cyber insurance - Disclosure of sensitive information	*less problematic*

As documented in Table 9, numerous problems with the insurability of cyber risk impede the development of a cyber insurance market. At the same time, we need to consider the time dimension. Today the cyber insurance market is 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 more are planning to do so. This will increase insurance capacity, competition and push prices down. Additionally, it will lead to a more uniform terminology and standardization of products. In light of our discussion it might be also important to establish standards on definitions, coverages and pre-coverage risk assessment, all of which will help to reduce some of the problems of insuring cyber risk.

2.5 Derivation of the Central Properties

As a summary of the results of this section and as a basis for the subsequent analyses, we now derive the central properties of cyber risk which make them difficult to insure (Table 10). One interesting aspect of cyber risk is that they can be both short- and long-tailed. Whereas cyber risk can often lead to direct losses (e.g., DoS-attack paralyzes the firm's homepage), there are also instances under which the loss might materialize only a few years after the actual incident (e.g., lawsuits, or hidden malware that spies on company/trade secrets for years before it is detected). In this context one difficulty is that the risk exposure can be both first-party and third-party.[31] According to Symantec (2015) almost two-thirds of attacks in 2014 were directed at small and medium-sized businesses (SMB), which might not have been interesting to the attackers in the first place, but that could give them a backdoor into other companies with more efficient security systems. Because SMBs do not often have the resources that large organizations do, they are vulnerable for liability losses with respect to the connected companies. With the increasing connectedness of market participants, this problem might become even more substantial in future.

Table 10 Central Properties of Cyber Risks

#	**Property**
1	Cyber risk result in both short-tail and long-tail losses
2	They produce first- and third-party (i.e., property and liability) losses
3	Cyber losses are not independent (correlations between cyber risk)
4	Cyber insurance market is small (relatively small insurance portfolios)
5	Uncertainty with respect to data (uncertainty loading necessary)
6	Uncertainty in modeling approaches (no actuarial standards)
7	Risk of change (historical data is not necessarily a good indicator)
8	Extreme scenario difficult to estimate (low frequency, high severity)
9	Insurance coverage limited (high deductibles, cover limits)
10	High importance of mitigation instruments (moral hazard)

The correlations between cyber incidents pose also a special characteristic of cyber risk. Independence of risks is one of the essential prerequisites to make risks insurable, but several authors acknowledge that this precondition is not satisfied (e.g., Baer and

[31] In this context property insurance is first-party insurance that indemnifies the owner or user of property for its loss, or the loss of its income-producing ability, when the loss or damage is caused by a covered peril, such as fire or explosion. Liability insurance is third-party insurance covering the insured against losses arising from injury or damage to another person or property.

Parkinson, 2007, or Haas and Hofmann, 2013). For instance, Baer and Parkinson (2007) argue that today's cyber systems are vulnerable to the same incidents, because of the similar design. Thus, the correlation of cyber incidents poses a problem for the cyber insurance industry. In addition, the pooling of losses in the insurance companies is impaired, since insurance portfolios are still rather small (Biener, Eling, and Wirfs, 2015), leading to sub-optimal levels of risk diversification.

Moreover, in contrast to other risks, cyber risks are characterized by extreme uncertainties, both with respect to the data itself and with respect to suitable modeling approaches for these risks. Without data and modeling approaches, insurance underwriting is impossible or only heuristic assessments are possible. These uncertainties then lead to extremely high premium loadings, which make policies expensive and unattractive to policyholders. The problems are even impaired, because of the risk of change that is connected to cyber risk. With the dynamic nature of cyber risk, there is doubt that the scant historical data that is available can accurately predict future development.

In this context another special property of cyber is the risk of extreme events. This poses a serious threat because worst-case scenarios cannot be estimated, and thus the economic magnitude cannot be derived. Several papers have discussed potential worst-case scenarios (e.g., WEF, 2010; Cambridge Center for Risk Studies, 2014; or Lloyd's, 2015). However, this collection of potential scenarios also shows how diverse and complex this topic is. While insurance companies can protect themselves against extreme scenarios with cover limits, policyholders might be more concerned and in need of protection against them. At the end of the day, these extreme events might jeopardize the whole economy, so the public and the government should be interested in efficient risk management solutions.

Another hallmark of cyber risk is the high importance of mitigation instruments. Modern information systems are interrelated, and thus the utility of cyber security investments depends on the investments made by the interrelated parties (see, Symantec, 2015, in which SMB were identified as gateway to larger or better protected companies). This might drive companies to minimize investments in self-protection, leading to moral hazard problems. Still, establishing minimum standards for self-protection can enhance economic welfare (Zweifel and Eisen, 2012), again emphasizing the important role and interest of the public and the government in the topic. One open question, however, is what the optimal amount of risk mitigation would be.

3 What Options for Risk Transfer do Exist?

In principle, there are five risk carriers (e.g., Smolka, 2003): risk owners, primary insurers, reinsurers, capital markets and the government (i.e., the public or the taxpayers). In Table 11 we outline potential risk transfer options that can be applied to each layer in order to manage the exposure to cyber risk. In the following sections we discuss these transfer options, and conclude with a summary of all instruments (Table 12) with their advantages and disadvantages.

Table 11 Risk Transfer Options

Layer	Risk Transfer Options		
Risk owner	Private risk pool	Industry-wide risk pool	
Primary Insurer	Conventional insurance	Insurance pool	
Reinsurer	Proportional reinsurance	Non-proportional reinsurance	Reinsurance pool
Capital markets	Insurance-linked securities		
Governments/Taxpayer	State as Primary Insurer/ Complete Coverage	Reinsurer of Last Resort	

3.1 Risk Owner

The risk owner will first install risk control activities such as self-protection and self-insurance to reduce the risk exposure. In the field of risk transfer, one option which keeps the risk at the level of the risk owners is the "private risk pool." A prominent example for such a pool in the German speaking countries is Friendsurance (2015). The premise is that a collective of risk owners pools their own risk exposure to cover small losses.[32] Group schemes with joint liability have been implemented in both developing countries, such as the mutual insurance funds model Fondos in Mexico (mutual insurance funds formed by local farmers for agricultural losses, which provide insurance only to their members; World Bank, 2013), and in developed countries through "peer-to-peer" insurance schemes, such as Hey Guevara (mutual car insurance in the United Kingdom; Guevara, 2015), and PeerCover (mutual insurance for different risks in New Zealand, e.g., saving plans for a pet's health, car insurance, comprehensive dental cover; PeerCover, 2015).

[32] Friendsurance is a special type of private risk pool, since it actually combines two risk transfer options. That is the private risk pool for small losses and insurance, in which high losses that exceed the volume of the risk pool are covered. A similar system is applied by the farmer mutual insurance funds (Fondos) in Mexico.

A second risk transfer option which keeps the risk at the level of the policyholder is the "industry-wide risk pool." The difference between the private risk pool and the industry-wide risk pool is the size. In a private risk pool the number of policyholders is limited, but the industry-wide pool consists of a large number of participants. While at first sight this looks unattractive – given moral hazard and adverse selection problems[33] – there are examples where also the industry-wide risk pool has proven beneficial. Some binding minimum standards for self-protection are necessary to establish an industry-wide risk pool.

A classic example of an industry-wide risk pool can be found as early as the Middle Ages. The craft guilds were medieval associations of workers of the same trade for mutual benefit (Renard and Terry, 2011). Every member of the guild was trained in that profession and those who reached the status of master had to pay dues to the coffer ("pool"). If one of the members faced a loss (e.g., robbery, fire, disability, death) the guild would cover the obligations. In case of death, support for widow and family, made this practice one of the first forms of life insurance (e.g., Baettie, 2015; or Renard and Terry, 2011).

[33] The advantage of the private risk pool is that the risk type and the behavior of the other pool members is observable, thereby limiting adverse selection and moral hazard. This is not the case with the industry-wide risk pool.

3.2 Primary Insurer

Another risk transfer option for the risk owner is to buy conventional insurance. Müller (1981) defines "insurance" as a device for the reduction of uncertainty of one party (the insured), through the transfer of particular risks to another party (the insurer), who offers at least partial restoration of economic losses suffered by the insured. Under conventional insurance we subsume all insurance contracts that are signed between a policyholder and a primary insurance company. With respect to cyber risk, insurance policies do exist as stand-alone products and are offered by various insurance companies (e.g., in Switzerland by AIG, Allianz, Chubb, and Zurich). In addition, some cyber risks are covered under other policies (e.g., business interruption after a hacker attack is covered by some business interruption policies).[34]

Following the logic of the previous sub-section the primary insurer might pool risks with other primary insurers. The intention behind such collaborations is to create a wider actuarial foundation for particularly high and unbalanced risks (Reichel and Schmeiser, 2015). The European Commission (2014) describes two approaches for collaboration on the primary insurer level. First, ad-hoc co-insurance agreements "represent arrangements in which each insurance company agrees *independently* to insure an agreed percentage of a given risk, each participating insurer being responsible for its share only" (European Commission, 2014, or Fundación Mapfre, 2013).

The second approach is a co-insurance pool. Under this approach, different insurance companies consolidate, and "agree to underwrite, in the name, and for the account, of all the participants, the insurance of a specific risk category" (European Commission, 2014). In general, a common entity is set up for this purpose to which all participants entrust their underwriting and management. From an economic point of view the co-insurance pool is quite similar to the ad-hoc co-insurance agreements. The main difference is that the risk is covered by all participants, not independently for a pre-defined share of the risk by only one insurer.

[34] Other variations of insurance that we do not discuss here in detail are microinsurance and takaful insurance. Microinsurance has the same principles as regular insurance (Biener and Eling, 2012) and thus does not provide a new risk transfer mechanism. Also with Islamic takaful insurance the actual risk transfer mechanism is the same as in conventional insurance. The difference lies mainly in the organization and definition of terms (e.g., the comparison of Takaful Pakistan Ltd., 2015).

The co-insurance pool has a series of advantages for its members (compared to the ad-hoc co-insurance agreement). For instance, when the members underwrite collectively, the pool's retention limit (determined by the financial capacity of the pool) is higher than the retention levels of each member individually. This might reduce the need for reinsurance for each member (Fundación Mapfre, 2013). In addition, if the pool is large enough, members can benefit from the pool's ability to influence market conditions, and limit possible deterioration in the business due to exaggerated competition (Fundación Mapfre, 2013). The latter might be a disadvantage for the economy. Probably the main disadvantage of this risk transfer option is that members are bound to the rules defined in the pool arrangement contract, which might detract from their competitiveness, especially with other companies outside the pool structure (Fundación Mapfre, 2013). For ad-hoc co-insurance agreements the latter is not problematic, since each participant can decide on how best to cover his own portion.

Important examples of co-insurance pools and ad-hoc co-insurance agreements can be found in most countries. The European Commission (2014) provides an overview of insurance pools in Europe and their scope of coverage. Its study identified 28 co-insurance pools in the European Union alone (of which 11 besides primary insurance business also write reinsurance business). Examples in the European Union are the Danish Terror Pool (European Commission, 2014), the Nederlandse Atoompol (coverage of nuclear installations in the Netherlands, European Commission, 2014), or the VOV Versicherungsgemeinschaft in Germany (collaboration of six primary providers of D&O insurance; VOV, 2015). In Switzerland the Swiss Natural Perils Pool (Schweizerischer Elementarschaden-Pool) is a "pooling of private insurance companies for better equalizing the risk associated with natural disasters and the elements" (Swiss Insurance Association, 2015). In the USA there are several examples, including the California Earthquake Authority (Insurance Information Institute (III), 2005), or the Price-Anderson Act (nuclear power; III, 2005).[35] Examples of the ad-hoc co-insurance agreement are typically not documented in studies, since most of the contracts have not been made public. An example is the Germanwings Airbus crash in the French Alps in March 2015, where Allianz was the lead underwriter in a co-insurance agreement for this plane and AIG was involved as a co-underwriter

[35] With respect to all these co-insurance solutions/ad-hoc co-insurance arrangements we have to mention that some of them are also connected to the instruments that can be applied by the state for risk transfer. Some of them are thus examples of both risk transfer layers. This might be a crucial factor, if size of such pools is discussed. If pools are defined by governmental intervention they might be mandatory, and thus capacity is higher than if the market participants connect themselves.

(Insurance Journal, 2015). Another example would be D&O insurance offered by Allianz Global Corporate & Specialty (AGCS) (2010). If D&O coverage with a cover limit of more than US$ 25 million is required, an ad-hoc co-insurance agreement is needed.[36] All these examples illustrate that for significant loss amounts going in the tens of millions of US dollars, insurance companies often are only willing to offer coverage if the risk can be shared with other market participants (whether co-insurance pools, ad-hoc co-insurance agreements or other risk transfer mechanisms discussed in the following sub-sections: reinsurance, alternative risk transfer, involvement of the government).

[36] For instance, for the emissions test manipulation scandal with Volkswagen, Zurich Insurance Group is claimed to be the lead insurer for a D&O insurance with a coverage of up to EUR 500 million (e.g., Enz, 2015).

3.3 Reinsurance

The most classical way to transfer risks for the primary insurer is to buy reinsurance. There are two basic forms of reinsurance: facultative and obligatory. The first solution is used to reinsure individual risks (e.g., a particular bridge or a building). Thus, coverage for risks that need individual treatment would be optimally covered by facultative reinsurance. It is called "facultative" because the reinsurer retains the opportunity (or the "faculty") to accept or refuse specific contracts from a portfolio. The same applies to primary insurers that are free to choose which risks they want to cover (Swiss Re, 2013). This is unlike obligatory reinsurance, where a primary insurer wants to purchase coverage for all of its policies (the whole portfolio) in a particular risk category (Swiss Re, 2013). This means, both parties are obliged to cede or accept any risk covered by the contract. Obligatory reinsurance is sometimes called "treaty" or "automatic reinsurance" (Swiss Re, 2013). Facultative reinsurance is mostly used as a complement to obligatory reinsurance, where additional risks that are not covered under obligatory reinsurance can be transferred (Swiss Re, 2013). This is why we focus here and in Section 4 on obligatory reinsurance.

Both reinsurance contracts can provide proportional or non-proportional coverage. In proportional reinsurance the primary insurer and the reinsurer share premiums and losses by a pre-defined ratio, meaning that the reinsurer's share of premiums is directly proportional to the payable losses in case of an incident (Swiss Re, 2013). Since shares are defined on premiums the actual underlying basis for claim settlement is the sum insured. This is different in the case of non-proportional reinsurance. Reinsurance products that are part of the proportional category are quota-share reinsurance and the surplus reinsurance. For a more detailed description of the contracts we refer to Munich Re (2010), Fundación Mapfre (2013) or Swiss Re (2013).

For non-proportional contracts the reinsurer covers losses that exceed the primary insurer's deductible up to an agreed cover limit.[37] Losses below the deductible have to be covered solely by the primary insurer. Most of the losses above the cover limit are also covered by the primary insurer, or transferred to the reinsurer by a facultative reinsurance contract. As indicated earlier, for non-proportional reinsurance the allocation of liabilities between the cedent and the reinsurer is based on the actual claim, not the sum insured as in proportional reinsurance. The most common examples of non-proportional reinsurance contracts are excess-of-loss reinsurance (per risk or

[37] The deductible is also called the (net) retention, excess point or priority (e.g., Swiss Re, 2013).

catastrophe excess-of-loss) and stop-loss reinsurance. For more information on those contract designs, we again refer to Munich Re (2010), Fundación Mapfre (2013), or Swiss Re (2013).

The reinsurance company itself can define reinsurance contracts with other reinsurance companies, called "retrocession." However, this is not a new risk transfer opportunity, since it is similar to the actual reinsurance contract. Another way to transfer risk for reinsurance companies is by the definition of a reinsurance pool, where a company collaborates with other reinsurance companies to assume the accepted risks. As for the insurance pools, different approaches can be defined: (1) co-reinsurance pools and (2) ad-hoc co-reinsurance agreements. These definitions are similar to those introduced for the pool solutions on the primary insurance layer.

Examples of reinsurance pools in the European Union are the German Nuclear Reactor Insurance Association (Deutsche Kernreaktor Versicherungsgemeinschaft, DKVG; European Commission, 2014), the Gestion de l'Assurance et de la Réassurance des risques Attentats et actes de Terrorisme – GAREAT (management of reinsurance of terrorism risks in France, GAREAT, 2015), or the Pool Inquinamento (co-reinsurance pool for civil and environmental liability losses; Pool Inquinamento, 2015).

3.4 Capital Markets

Risk transfer opportunities where insurance-related risks can be ceded to the capital markets have grown in importance in the last years (Swiss Re, 2013). The instruments here are called "insurance-linked securities" (ILS).[38] These are often described as an attractive investment opportunity because of their high yields and their return's low correlation to the overall economy (Ben Ammar, Braun, and Eling, 2015). For the risk ceding parties, ILS have the potential to enhance the risk-bearing capacity of the insurance industry because capital markets are involved and thus allow the insurance industry or risk owners to spread risks more efficiently and more broadly (Kunreuther, Kleindorfer, and Grossi, 2005).

ILS are typically structured as special purpose vehicles (SPV), which offer conventional reinsurance to the cedent (usually the primary insurer or reinsurer).[39] The SPV then finances itself by issuing interest-bearing notes to capital market investors and invests the proceeds in high-quality securities (e.g., government bonds) and holds them in a collateralized fund (Swiss Re, 2013). If a trigger event happens (which is defined in the reinsurance contract, such as a predefined magnitude on the Richter scale is reached at an earthquake), the SPV pays out funds to the primary insurer/reinsurer according to the reinsurance agreement signed by them. The investors' principal will then be reduced by that amount and only the remaining investments (+ coupon) are transferred back to the investor at the end of the contract period.

ILS products are used to cover losses from property and casualty (P&C) insurance as well as life insurance. Examples of P&C are catastrophe (cat) bonds, industry loss warranties (ILW), collateralized reinsurance, sidecars, cat swaps, cat futures and options, as well as contingent capital (Ben Ammar, Braun, and Eling, 2015). Most of these instruments are used to transfer risks. For life, these instruments are used mainly as a financing tool. Examples of these products are longevity and mortality bonds, embedded value securitization, and XXX/AXXX reserve securitization (Ben Ammar, Braun, and Eling, 2015). For more detailed definitions of these products and further

[38] Insurance-linked securities are mostly related with catastrophe bonds, which only describe a small part of the whole range of ILS solutions. Cat bonds however, are the most prominent and probably the most important ILS solutions (Ben Ammar, Braun, and Eling, 2015).

[39] The cedent is also called "sponsor" because it assumes the risk. The cedents are not limited to insurance and reinsurance companies; see for example the cat bond for terror risk at the 2006 FIFA World Cup in Germany.

information on insurance-linked securities in general, we refer to Ben Ammar, Braun, and Eling (2015).

3.5 Governments

The government could have several roles in risk transfer. For some risks, governmental intervention might not be necessary; however, for other risks state intervention is inevitable, since otherwise private insurance markets would not be able to function (market failure) or the economic welfare would be impaired. Examples of these kinds of risk are terrorism, natural catastrophes, and accidents in nuclear power plants. Those risk categories are the severe examples from the property and liability insurance field, which would face particular problems of market failure (e.g., Kunreuther, Hogarth, and Meszaros, 1993). However, government is also involved with health and life insurance in terms of social insurances in most European countries to achieve social outcomes.

According to OECD (2005), there are two types of governmental intervention. In the "indirect" or "implicit" intervention, a government will not offer coverage itself, but will build a market environment that cultivates the growth of the private insurance market. Since this is not an actual risk transfer option we will not discuss it here; please refer to Section 5.2. Under the "direct" or "explicit" form of involvement the government itself bears the actual risks. This category includes mixed private-public undertakings, where the private markets are responsible for most of the risks and the government may assume only designated insurance functions. In general, the extent to which the risks are shared between public and the private stakeholders can be described in two ways:[40]

1. **State as Primary Insurer/Complete Coverage:**
   This is the most extreme version of private-public enterprise, since the government takes all the insurance functions, and thus is the only risk carrier; there is no private market for those risks.[41] One example is the Swiss old-age and survivors' insurance (AHV; Alters- and Hinterlassenenversicherung). This scheme covers basic living costs in retirement and protects surviving dependents. It is compulsory for everyone in Switzerland and is provided by the Federal Social Insurance Office (FSIO; see FSIO, 2015). The basic coverage can be complemented by a second (occupational benefit plan for workers) and

[40] Under the "direct"/"explicit" approach there is also a third approach discussed for the government ("Lender of Last Resort"). However, the state will not participate in the actual risk transfer, which is why we do not discuss it. However, more information can be found in Section 5.2.

[41] There might be additional solutions from the private market (substitutes or complements), but the state provides the basic coverage.

a third layer of coverage (individual provision), which then are not covered directly by the state (but subsidized). Further examples are terrorism insurance in Israel and the Spanish Consorcio de Compensación de Seguros (CCS).[42]

2. **Reinsurer of Last Resort:**
   The government steps in for losses that are above a deductible limit at the lowest risk level and possibly losses at the intermediate risk levels by co-reinsurance (OECD, 2005). Therefore, government only covers the highest risk level while the private insurers cover the small and intermediate losses. Under this approach the government can take the advantage of the (re-)insurance industry's experience and knowledge in writing insurance business (i.e., underwriting practices, claims settlement, and their existing network) and couple it with its exclusive capacity to provide coverage for large risks (much wider diversification over the entire population, and across future generations of taxpayers possible; OECD, 2005). Examples of this approach are the Terror Risk Insurance Act (TRIA; III, 2005), Pool Re for terrorism in the UK (Pool Re, 2015), or the Japanese earthquake reinsurance program (JER, 2013).

[42] The terrorism insurance program in Israel consists of two tiers: (1) Property Tax and Compensation Fund: covers property and casualty insurance for terrorist attacks; (2) Law for the Victims of Enemy Action: covers life and health insurance in terrorism context (GAO, 2001). The Spanish CCS compensates damages caused to people and property as a result of certain natural phenomena (e.g., floods, earthquakes, volcanic eruption, or meteorites) and also of some events deriving from certain political or social occurrences (e.g., terrorism, rebellion, riot, or popular uprising). Condition for reimbursement is that the affected stakeholder has an insurance contract in one of the insurance branches that are covered under the agreement (CCS, 2015).

Table 12 Systematic Comparison of Risk Transfer Options

Layer	Option	Description	Advantage	Disadvantage	Examples of Risks Covered	Sources/References
Risk owner	Private risk pool	A collective of risk owners pool their own risk exposures to cover small losses.	• Moral hazard and adverse selection small, since the risk type and behavior of the pool members is often observable • Close connection to members and deep knowledge of their condition → also moral obligation to avoid losses • Often cheaper for risk owner, because of contribution refunds (e.g., Friendsurance, peerCover, Hey Guevara) • In some setups, reinvestments of any profits back to the community (e.g., contingency reserves; see Fondos) • Additional benefits for participants, e.g., social services, technical support in the local community	• The aggregated volume in the pool might not be sufficient to cover all losses → insurance might be necessary (e.g., Friendsurance or Fondos) • More vulnerable to cumulative risk if losses are correlated, because in general participants know each other (e.g., Friendsurance)	• Liability risks • Property risks (e.g., motor) • Legal risks • Agricultural risks	World Bank (2013), Friendsurance (2015), Guevara (2015), PeerCover (2015)
	Industry-wide risk pool	All participants in an industry pool their own risk exposure to cover losses. Differentiation from private risk pool: industry-wide pools consist of a larger number of participants.	• The risk taking capacity is much higher than in the private risk pool, because of a larger number of participants • Additional benefits for participants, e.g., social services, technical support in the local community	• Moral hazard and adverse selection problems, since risk type and behavior are not observable anymore because of high number of participants • More vulnerable to cumulative risk if losses are correlated, because participants are from the same industry and by that very similar	• Property risks (e.g., fire, robbery, etc. in the guilds) • Life and health risks (e.g., disability, life insurance in the guilds)	Baettie (2015) Renard and Terry (2011)
Primary Insurer	Conventional Insurance	Device for the reduction of uncertainty of the insured, through the transfer of particular risks to the insurer, who offers a restoration, at	• Satisfies sense of security in human beings • Puts a price tag on risk • Risk that cannot be controlled by self-protection or self-	• Sometimes relatively expensive • Every insurance contract has exclusions/cover limits → no 100% coverage possible	• Almost all risks → also insurance for cyber risk present	Müller (1981) Zweifel and Eisen (2012) Farny (2011)

		least in part, of economic losses suffered by the insured.	insurance can completely or just partially be covered • Maintains economic stability	• Claims settlement process can be slow → indemnity payments may arrive late • Moral hazard → potential riskier behavior after insurance purchase		
	Insurance Pool	Group of primary insurers which create a wider actuarial foundation for particularly high and unbalanced risks. (Two approaches: co-insurance pool and ad-hoc co-insurance arrangement)	• Risk taking capacity can be increased significantly • Improvements in risk diversification (only under the co-insurance pool) • Scale advantages because of greater collective (only under the co-insurance pool) • Improved representation of interests (only for co-insurance pools)	• Accumulation risk play an essential role • For extreme losses the capacity of the pool might still not be sufficient (e.g., cat) • Potential limitations of competition • Pressure to innovate might be reduced • Additional administration costs (compared to conventional insurance)	• Aviation risks • Natural catastrophes • Nuclear accidents • Terrorism	Fundación Mapfre (2013) European Commission (2014)
Reinsurer	Proportional reinsurance	Primary insurer and reinsurer share premiums and losses by a pre-defined ratio, i.e., the reinsurer's share of premiums is directly proportional to the payable losses in case of an incident.	• Well-suited for homogeneous portfolios of risks • Potential catalyst for young, fast-growing insurers or established companies which are new to a certain class business • Provides capital relief in light of solvency requirements • Income smoothing: (1) Protection against random fluctuations across an entire portfolio; (2) Protection against changes triggered by unexpected legal development or economic factors (e.g., inflation)	• In general inappropriate to cover extreme losses (e.g., accumulation) • Potential imbalances in the primary insurer's portfolio remain unaddressed • Potential profitability issues (insurer might cede too much and retain too little)	• General property and liability losses (e.g., motor insurance)	Munich Re (2010) Fundación Mapfre (2013) Swiss Re (2013)
	Non-proportional reinsurance	Reinsurer covers losses that exceed the primary insurer's deductible up to an agreed cover limit. Losses below	*For the cedent:* • Extreme losses in the portfolios are covered	*For the cedent:* • Coverage only for very large risks appropriate	• Losses from natural catastrophes	Munich Re (2010) Fundación Mapfre (2013) Swiss Re (2013)

		the deductible have to be covered solely by the primary insurer.	• Reduction in administrative costs (in particular compared to surplus reinsurance) *For the reinsurer:* • More information from the portfolio covered • Reinsurance premiums are set by the reinsurer • In general, upper limits of coverage are given	• Counterparty risk for large cat events where coverage is offered by only a few reinsurers • Dependence on developments in the reinsurance market (prices might vary substantially from one year to the next, because of international claims experience) *For the reinsurer:* • Ratio between premiums and liabilities accepted is very high → recovery from extreme losses might be tedious		
	Reinsurance pool	A group of reinsurers who share the premiums and losses of a risk they have written together, according to an agreement that exists between them.	• Similar reasoning as in the insurance pools applies here	• Similar reasoning as in the insurance pools applies here	• Natural catastrophes • Nuclear accidents • Terrorism	Fundación Mapfre (2013) European Commission (2014)
Capital market	Insurance-linked securities	Transfer of a specified set of risks from the sponsor (i.e., in general (re-)insurer) to capital market investors through a fully-collateralized Special Purpose Vehicle (SVP). The SPV issues interest-bearing notes of which the principal is used to pay losses if special trigger conditions are met.	*For the sponsor:* • Ability to transfer peak risks (otherwise difficult to cover through reinsurance) → increased risk-bearing capacity • Because of multi-year contracts, sponsor can uncouple from pricing cycles • Counterparty credit risk (e.g., reinsurer defaults) is limited • Simplified claims settlement process (in particular for index triggers) • Segregation of expected future income flows from the insurance portfolio (life insurance)	• Basis risk in case of index trigger • In general only for large volumes applicable (> US$ 100 million) • No transparency for investors (issuer knows risk, investor does not) → information asymmetries? • Traditional reinsurance market continuous to soften (making traditional reinsurance more competitive)	• Mostly coverage of natural catastrophes (cat bonds) • also longevity or mortality risks	Lale (2013) Swiss Re (2013) Ben Ammar, Braun, and Eling (2015)

			• Costs for protection are currently quite low *For the investor:* • Provide attractive potential for diversification (relatively high returns, independence from general economy)			
Government	"State as Primary Insurer"/"Complete Coverage"	Government undertakes all the insurance functions, and thus is the only risk carrier in the market.	• Availability of coverage for everyone guaranteed • Extreme losses are covered	•Might be expensive, in particular for extreme risk categories (e.g., terrorism) •Potential underwriting, pricing and claim management rigidities, because of inexperience •Bureaucratic excesses which could result in high operating expenses •Crowd out/replace effect of private solutions •Moral hazard possible, since incentives for private risk mitigation approaches not present	• Terrorism • Natural catastrophes • Health/Life insurance	OECD (2005)
	"Reinsurer of Last resort"	Government steps in for losses that are above a deductible limit at the lowest risk level and possibly losses at the intermediate risk levels by co-reinsurance.	•Availability of coverage for every primary insurer can be guaranteed •Extreme losses are covered •Might not be as expensive as "State as Primary Insurer" •No crowding out/replacement of private primary insurance solutions	•Solidarity over generations might be impaired •Bureaucratic excesses which could result in high operating expenses •Crowd out/replace effect of private reinsurance solutions •Moral hazard (only for the highest level, but still present)	•Terrorism •Natural catastrophe •Nuclear accidents	III (2005) OECD (2005)

4 Analysis of the Risk Transfer Options

4.1 Motivation

The idea of this section is to analyze the risk transfer options from Section 3 in light of the special properties of cyber risk derived in Section 2. Ten properties of cyber risk were identified in Section 2.5, eight of which will be modeled and analyzed in this section.[43] Table 13 outlines those aspects and explains how we integrate them into our analysis.

Table 13 Integration of the Central Properties of Cyber Risk in the Model

Special characteristics	How we integrate it into our model
1. Cyber losses are not independent	Variations of correlation in portfolios
2. Cyber insurance market is small (relatively small insurance portfolios)	Variation of portfolio size
3. Uncertainty with respect to data (uncertainty loading necessary)	Variation of uncertainty loading
4. Uncertainty in modeling approaches (no actuarial standards)	Use of different modeling approaches (e.g., for pricing)
5. Risk of change (historical data is not necessarily a good indicator)	Modeling of different scenarios
6. Extreme scenario difficult to estimate (low frequency, high severity)	Modeling of separate extreme scenario
7. Insurance coverage limited (high deductibles, cover limits)	Variation of deductibles and cover limits
8. High importance of mitigation instruments (moral hazard)	Modeling and variation of investments in self-protection

As shown in Table 13, the integration of the special characteristics is done via the systematic variations of the model parameters and the inclusion of alternative modeling approaches. Later in this section, we present variations of model parameters in order to analyze in how far an insurance pool and the intervention of the government might improve the insurability of cyber risks. The consideration of an insurance pool can be accomplished, for example, by the increase of insurance portfolio size (due to larger portfolios) and the decrease of uncertainty loadings (due to better data availability for pricing). The consideration of government interventions can be considered, for example, by analyzing different minimum standards for self-protection.

[43] The remaining two categories that are not modeled are that cyber is a mix of short- and long-tail losses and a mix of first-party and third-party losses.

4.2 Model

4.2.1 Expected Utility Framework

We use expected utility to analyze the five risk transfer options from Section 3 under different predefined scenarios. The consideration of expected utility is needed to analyze decision making under risk. Expected utility theory goes back to Gabriel Cramer and Daniel Bernoulli who proposed that a mathematical function should be used to correct the expected value depending on probability in order to account for risk aversion (Bernoulli, 1954). The incorporation of expected utility theory and risk aversion in insurance decision making has been standard in literature since the 1960s. Scholars such as Pratt (1964), Arrow (1965), and Mossin (1968) used this framework to determine optimal insurance demand for individuals. Over the years these models became more specialized and incorporate more complex contract details; for instance Cummins and Mahul (2004) analyze the individual's decisions to buy insurance coverage under the assumption of a cover limit, restricting the coverage to a maximal amount. Kunreuther, Hogarth, and Meszaros (1993) emphasize risk aversion for decision making at the company level, which is why we will incorporate the expected utility concept there.[44]

These papers examine only one of the parties in the market: supply or demand. This may lead to optimal coverage solutions for one party, although the other party would not offer or buy them. To consider both the supply and demand side, simultaneous optimization problems need to be solved which make the model more complex from the mathematical side. For example, Golubin (2014) determines the optimal insurance and reinsurance policies for the primary insurer under constraints for the policyholder and the reinsurer.

Our modeling approach falls into this category of simultaneous optimization. The idea is to consider different risk transfer options and to analyze under which of those options the cyber insurance market would be the greatest (i.e., the greatest variety of deductibles and cover limits are possible in the sense that all market participants are entering the market). The risk transfer options we consider are insurance, different

[44] The introduction of expected utility for insurance companies might be uncommon in the academic literature, since only a few scholars apply it in these cases; see, e.g., Mossin (1968), and Cummins and Mahul (2004), who apply it to discuss decisions about the optimal reinsurance coverage; or Golubin (2014) who analyzes the decisions for reinsurance and primary insurance simultaneously. However, for our approach these decisions are the important part of this analysis and by that would motivate the extension in the model.

types of reinsurance, a capital market solution and the inclusion of the government. In the following we introduce the expected utility models. We then describe the different risk transfer options on each layer and finally the scenarios we consider to analyze the risk transfer options.

In a first step, we simulate losses on each risk transfer option layer by actuarial standard approaches (e.g., Kaas, Goovaerts, Dhaene, and Denuit, 2008, pp. 17-86; for the actual loss simulation approach used in this study, we refer to Appendix E). Next, we distribute those losses under each model defined in Section 4.2.2 (e.g., how much of the risk owner's loss is covered by the risk owner him-/herself and which amount is covered by the primary insurer, which part of the loss can be distributed to the reinsurer/capital market, and which part has to be taken over by the government). The amount covered by each party is defined by the contracts signed between them. Since we are not sure a priori which contracts are feasible for the different stakeholders we simulate potential contracts and determine the appropriate cash-flows between the stakeholders for the contract under investigation. Based on the different cash flows, we evaluate if each stakeholder would be willing to enter the contract, measured by the expected utility concept. This approach will enable us to end up with one value (utility) for each contract option, which we can compare against all other options. This permits the determination of areas under which the contract could be realized, only if all parties have a higher utility with the contract than without it. For a more detailed definition of the expected utility constraints we refer to Appendix E.

For the expected utility analysis, we define utility functions for each party. For the risk owner, the primary insurer, and reinsurer we define their utility by the following mean-standard deviation utility function:

$$U(W) = E[W] - \frac{a}{2}\sqrt{Var[W]},$$

where W is the wealth on each risk layer from which value/utility is gained.[45] The utility is thus the expected wealth subtracted by its weighted standard deviation, which accounts for the riskiness of the payments. The extent to which this riskiness should be accounted for can be adjusted by the risk aversion parameter a. We apply the mean-standard deviation preference function instead of the related mean-variance-utility function – which might be more common in this context (e.g., Levy and Markowitz, 1979; Müller, Schmeiser, and Wagner, 2011; Gatzert and Schmeiser, 2012).

[45] There are other utility functions that can be used (e.g., power utility, exponential utility, etc.). We use this approach because of simplicity; however, the application of other utility functions is possible and can be found in Wirfs (2016).

According to Samuelson (1963) for independent and identically distributed claims in a portfolio, the riskiness of the portfolio increases with the number of contracts if measured by the variance. That means the mean-variance function cannot be used to model the portfolio effects which we analyze when we consider the insurance pool solutions. In contrast to the policyholders, insurers, and reinsurers, the investors use another decision making metric; they will only enter the risk transfer, if the expected performance of their investment is higher than a benchmark performance (measured by a pre-defined Sharpe Ratio). All parameters and their details are listed in Sections 4.2.2 and 4.3.1.

4.2.2 Definition of Risk Layers

We consider risk transfer solutions from all risk layers considered in Section 3 (risk owner, primary insurer, reinsurer, capital market, government). We define five models, under which we incrementally establish a market in which all layers are present.

Model #1 – "No insurance"

In the first model there is only a risk owner and no risk transfer option available and thus no insurance market. This initial model will serve as a benchmark against which the other models can be compared.

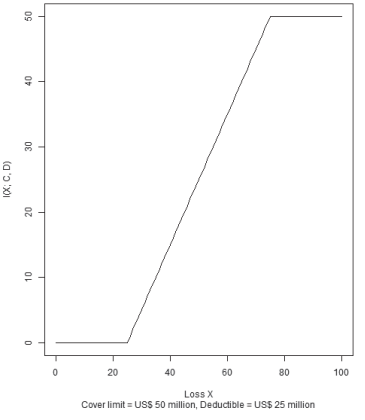
Model #2 – "Conventional Model"

For this model we assume a market with risk owners and primary insurers, but no further risk transfer layers. According to Section 2, this model is close to the current status of the cyber insurance market as we observe it today (some primary insurance coverage is available, while other risk transfer options are either very limited or non-existent). Between the two parties we define insurance contracts for cyber risks and evaluate for both parties if the coverage increases expected utility. Most of the cyber insurance contracts in the market impose cover limits (or caps). For example, according to Biener, Eling, Matt, and Wirfs (2015) cover limits in Switzerland are between CHF 10 million and CHF 50 million. Reports from insurance companies indicate that also higher cover limits are possible (e.g., Ace Ltd. plans to offer US$ 100 million cover limits; Finkle, 2015). The contracts also include deductibles to address potential moral hazard. The indemnity payment by the primary insurer can then be written as:

$$I^{PI}\left(X;C,D\right)=\min\left\{\max\left\{0,X-D\right\},C\right\},$$

where X is the random variable describing the losses on the risk owner level, C is the cover limit and D is the deductible. Thus, $I^{PI}(X; C, D)$ is a random variable and depends on the distribution of losses X. An illustration of the indemnity function $I^{PI}(X; C, D)$ for a cover limit of US$ 50 million and a deductible of US$ 25 million is shown in Figure 2. The indemnity payments by the insurer can be separated into three parts. If the loss is less than D ($X \leq D$), there is no payment and the risk owner has to cover all losses. If $D < X \leq C + D$, the insurer covers the complete loss above the deductible, while all losses above $C + D$ are only covered up to the cover limit C.

Figure 2 Visualization of the Indemnity Payment by the Primary Insurer



For taking over the amount of $I^{PI}(X; C, D)$ from the risk owner's loss, the primary insurer charges a premium. We define the premium as the expected value of the loss payment with a proportional risk loading and a fixed loading to cover costs (i.e., $P^{RO}=\left(1+\lambda^{RO}\right)\cdot E\left[I^{PI}\left(X;C,D\right)\right]+\lambda_{fixed}^{RO}$) (e.g., Mossin, 1968; Cummins and Mahul, 2004).[46] We will vary the definition of the proportional loading λ^{RO} in Section 4.5.2. In the main results presented in Section 4.3 we use a constant proportional loading, i.e., the same loading to all levels of indemnity payment I^{PI}.[47] The calibration of the loading

[46] In general, cyber insurance contracts would be priced by the different coverage blocks (Table 8) separately. The approach used here is based on the accumulated loss exposure and does not differentiated into the different coverage blocks because of reasons in data limitation.

[47] The alternative pricing approach is based on a ruin probability. The risk loading will then be estimated such that the total premium payments earned by the primary insurer over all contracts

is oriented at risk loadings for other risk categories (e.g., natural catastrophes, or general property insurances). Having estimated the premiums and the losses (after the indemnity payments), we can compute the utility for the risk owner and compare those values with the utility of the "No insurance"-model.

At the primary insurer layer the premium payments from each policyholder can be counted as a cash-inflow. However, the insurer covers the stochastic amount of $I_i = I^{PI}(X_i; C, D)$ in each contract i. Therefore, the payments that have to be made by the primary insurer in total are given as follows:

$$L^{PI} = \sum_{i=1}^{n^{PI}} I_i ,$$

where I_i is the random indemnity payment of contract i and n^{PI} is the size of the primary insurer's cyber insurance portfolio. The losses arising in this way in the primary insurer's portfolio can be modelled again with an own distribution. We simulate those losses based on the distributional assumptions for the risk owner. The loss distribution of L^{PI} (simulated losses) then can be used in the evaluation of the primary insurer's utility, where the expected losses and their standard deviation are the input factors. Again, we compute the utility values for every *(C, D)*-combination and compare them with a reference utility, in this case the utility of not offering insurance. If the utility of a *(C, D)*-combination is greater than that benchmark, we declare it as a feasible contract design for the primary insurer. Doing so will provide us with areas in which contract designs are acceptable for the primary insurer and others in which they are not. The same areas are computed for the risk owner. Only the *(C, D)*-combinations which are present in both sets produce solutions in which a cyber insurance market can be realized.

Model #3 – "Conventional Model with Reinsurance"

In Model #3 we extend Model #2 by a reinsurance market. The implementation is done by the definition of a reinsurance company that offers reinsurance to the primary insurers. We consider proportional and non-proportional reinsurance contracts. For the actual implementation we assume a (non-proportional) excess-of-loss reinsurance contract in the reference model (Section 4.3.2). We also illustrate the results with a surplus reinsurance contract (proportional) in Section 4.5.1.

---

can cover a specific amount of the expected portfolio loss (e.g., 95%). By that assumption we will derive different proportional loadings for all different indemnity payment constellations described in I^{PI}.

Excess-of-loss reinsurance contract

For the excess-of-loss reinsurance we assume the primary insurer has to pay all losses up to the retention level $R_{Excess\text{-}of\text{-}Loss}$; all losses above that benchmark are covered by the reinsurance company up to a cover limit of $C_{Excess\text{-}of\text{-}Loss}$. We will vary the values of $R_{Excess\text{-}of\text{-}Loss}$ and $C_{Excess\text{-}of\text{-}Loss}$ and evaluate the amount that is most beneficial to all market participants (i.e., which maximizes the overall solution set). Premiums for this contract are defined as in the "Conventional Model" for the risk owner-primary insurer-relationship, i.e., $P^{PI} = \left(1+\lambda^{PI}\right) \cdot E\left[I^{RE}\right] + \lambda_{fixed}^{PI}$, where I^{RE} is the stochastic indemnity payment by the reinsurer, and therefore the expected loss for the reinsurer per reinsurance contract. As before, we will analyze two approaches to the definition of the proportional risk loading λ^{PI} (i.e., constant proportional and risk-adjusted proportional loading factors, similar to the definitions for the primary insurer; see Section 4.5.2 for the results).

Surplus reinsurance contract

For the surplus reinsurance contracts, premiums and losses are shared by a fixed ratio. The surplus reinsurance contract has the advantage that it can be individualized to different risks in one insurance portfolio of one line of business (LoB) or over different LoBs. For instance, for every contract in an insurance portfolio of one LoB the reinsurance contract can be set up differently – for every contract a different insured sum can be defined, depending on the risk type, size, and the company's overall risk appetite – while the general setup of the contract stays the same. This balances a primary insurer's portfolio more effectively than under other reinsurance contracts (e.g., quota-share reinsurance). Since in our setup we look at only one risk category and the individual contracts in that portfolio are similar (we assume identical contracts), this opportunity to customize per contract might not be fully used in the setup of our model. However, we can differentiate by insured sum and thus interpret cyber insurance as a single risk category in an overall insurance business portfolio for which the actual surplus reinsurance contract was defined.

The contract under consideration is defined by the following three key figures:

- **Retention** (also called "line" or "deductible"): describes the amount of primary insurer loss, if not exceeded, that has to be covered solely by the primary insurer.
- **Multiple** of the line: defines the maximal amount the reinsurer will cover (e.g., under a three-line surplus, the reinsurer covers at least three times the retention, so if the retention is US$ 500 million, the reinsurer covers a maximum of US$

1,500 million, after losses exceeded the retention); the multiple of the line has a link with the above defined cap or cover limit in the excess-of-loss reinsurance.

- **Sum insured**: represents the amount of the risk for which reinsurance should be bought.

Under assumptions for all three values the premiums and the portions of loss to cover by each party can be determined. If the insured sum is smaller than the line, the primary insurer covers all losses for that risk. If the insured sum chosen to be between the line of the primary insurer and the maximal amount the reinsurer will cover (+ the line of the primary insurer), the primary insurer covers the ratio of line to sum insured, while the reinsurer covers the remainder.[48] If the insured sum is higher than the maximal amount the reinsurer will cover (+ the line of the primary insurer), the primary insurer covers its retention, defined as before as ratio of line to sum insured. In addition, the reinsurer covers the maximal amount possible under the contract (i.e., the ratio of multiple to sum insured). Then, there is a part left that exceeds the multiple plus line (is the ratio of sum insured minus the amount covered by the primary insurer and the reinsurer to sum insured), which then can be covered either by the primary insurer, or covered by an additional reinsurance contract (e.g., facultative reinsurance).[49] To be defined a feasible reinsurance contract in the analyses we will vary the contract parameters and identify that solution under which the solutions sets become biggest in the evaluations of Section 4.5.1.

Model #4 – "Conventional Model with Reinsurance and Capital Markets"

To the implementation of a reinsurance market we add capital market solutions to the model. There are two ways to implement this model: (1) a primary insurer issues the cyber cat bond (and no reinsurer is in place); and (2) a reinsurer is in place and issues the cyber cat bond. We will call case (1) the "Conventional Model with Capital Markets" and case (2) the "Conventional Model with Reinsurance and Capital

[48] For instance, under a three-line surplus with a line of US$ 500 million, and an insured sum of US$ 1,000 million, the primary insurer covers 50% (= US$ 500 million/US$ 1,000 million = 50%). If the insured sum is only US$ 800 million the primary insurer covers 62.5% (= US$ 500 million/US$ 800 million = 62.5%), and the reinsure covers the remaining 37.5%.

[49] In the example above, assume that the insured sum is US$ 2,500 million, then the primary insurer covers 20% (= US$ 500 million/US$ 2,500 million = 20%), the reinsurer covers 60% (= US$ 1,500 million/US$ 2,500 million = 60%), and the remainder is 20% (= (2,500 – (500 + 1,500))/2,500 = 20%). In this example, if the remainder is covered by the primary insurer as well, the primary insurer's share increases to 40%.

Markets." In the following model description we will focus on case (1). Case (2) is modelled analogue.

We assume a primary insurance company that issues a "cyber risk cat bond." We follow Kunreuther, Kleindorfer, and Grossi (2005), who discuss the capital market as an alternative to reinsurance for natural catastrophes. The cat bond consists of a predefined "attachment point" that needs to be breached by an underlying reference variable or "trigger" to make the cat bond pay the indemnity to the sponsor and thereby reduce the investor's principal at maturity. Ben Ammar, Braun, and Eling (2015) discuss six trigger types, of which we will apply the indemnity trigger. Under this trigger the reference variable is the incurred loss in the insurance company that must exceed the attachment point to make the bond pay. The contract defined between the two parties (here the primary insurer and the special purpose vehicle) is thus similar to the excess-of-loss reinsurance contract we defined in the "Conventional Model with Reinsurance" ("attachment point" vs. "retention").

Compared to reinsurers, the investor on the capital market has a different decision making criterion. That is, the investor expects a minimum performance for the investment as defined by a minimum value for the Sharpe Ratio. The Sharpe Ratio is a measure of the performance of an investment and is defined as the mean of excess returns (i.e., the expected return of an investment above the risk-free rate) over the investment's standard deviation (e.g., Cochrane, 2005). Only if the Sharpe Ratio of the investment is higher than the minimum performance the investor expects, the investor enters the arrangement.

We consider a cat bond with face value B and a rate of return for the zero-coupon catastrophe bond of $r^{Zero\text{-}Coupon}$. Thus, the investor makes an initial payment to the SPV of

$$\frac{B}{\left(1+r^{Zero-Coupon}\right)},$$

at the beginning of the contract period. At maturity the investor will receive the face value B reduced by the potential indemnity payment to the sponsor. This payout is defined as

$$PO^{Sponsor} = \min\left\{\max\left\{0; L^{PI} - AP\right\}; K\right\},$$

where L^{PI} represents the aggregated loss of the primary insurance company, AP defines the attachment point, and K $(\leq B)$ is the maximum payout from the catastrophe

bond (similar to the cover limit in the primary insurance contract).[50] For simplicity we assume the maximal payout K to be the face value (i.e., the investor can lose the whole investment). The primary insurer pays a premium of $r^{Zero\text{-}Coupon} \; x \; B$ to cover the interest for the zero-coupon catastrophe bond, in return it receives the payment $PO^{Sponsor}$ if the aggregated loss triggered AP. All definitions made so far are connected to the primary insurance company issuing the cyber cat bond. We will also analyze the effect of the cat bond if it covers losses from a reinsurance company (i.e., reinsurer is the issuer). The model for this second case can be described analogously.

Model #5 – "Collaborative Model":

In the final model, we extend the previous models by the government. One approach would be to incorporate the government as "State as a Primary Insurer" or as "Reinsurer of Last Resort." The incorporation of the state (both options) can be seen as a huge primary insurer/reinsurer. By variation of parameters, changes to incorporate one single primary insurer/reinsurer could be made. There are several other ways for the state to engage in the cyber insurance market; however, they are not directly related to the government assuming the risk. We will implement two of those "implicit" solutions: (1) we assume the state establishes a (mandatory) (re-)insurance risk pool; and (2) we suggest that the government requires a particular level of self-protection. More information on these setups can be found in Section 4.6.

4.2.3 Definition of Scenarios

We analyze the risk layers under four scenarios. Within the scenarios we will change the assumption on the potential losses by an increase in loss severity. For the definitions of Scenarios #1-#3 we rely on the empirical results presented in Section 2.2. Scenario #4 considers a "Black Swan" as discussed in NAS (2008), WEF (2010), CSRS (2014), or Lloyd's (2015).

Scenario #1 – "Base"-Scenario

The base-scenario (Scenario #1) is estimated by the total dataset (cyber risk incidents selected from SAS OpRisk Global data) available in Section 2.2. In the loss modeling approach we will fit a probability distribution to the data and use these findings to

[50] Note, that Kunreuther, Kleindorfer, and Grossi (2005) also include a co-insurance payment which has to be paid by the bondholder in excess of the attachment point AP. We construct this example as close to the reinsurance model as possible, which is why we skip this part in the analysis.

generate random numbers. Main indicators for the model will then be the mean and standard deviation of the generated losses. Table 14 shows the descriptive statistics of the whole sample and indicates the severity of that scenario.

Table 14 Descriptive Summary of Scenarios #1 – #4

	Scenario #1	**Scenario #2**	**Scenario #3**	**Scenario #4**
No. of observations	1,579	795	158	1
Average	43.49	85.82	397.80	500.00
Standard deviation	426.36	598.05	1,298.59	1,500.00
Minimum	0.10	1.53	38.23	0.00
25% Quantile	0.43	3.07	63.43	0.00
Median	1.53	7.37	101.10	0.00
75% Quantile	7.43	25.05	268.40	0.00
Maximum	14,590.00	14,590.00	14,590.00	5,000
Scenario description	Complete data	Upper 50% of the data	Upper 10% of the data	WEF (2010)

In Scenario #1 standard cover limits of US$ 10 million to US$ 50 million (Biener, Eling, Matt, and Wirfs, 2015) or US$ 100 million (e.g., Finkle, 2015) would be enough to cover most of the cyber losses. For example, 92% of all incidents in our dataset would be covered under a cover limit of US$ 50 million. Scenario #1 therefore can be interpreted as the cyber risks of "daily life" since the emphasis in this scenario is on the body of the distribution. In the following scenarios we will go into the tail of the distribution to analyze more extreme outcomes.

Scenarios #2 – "Intermediate"-Scenario

In Scenario #2 we follow Betterley (2015) who shows that the severity of losses might increase over time. We thus assume that future cyber risk losses can be described by the upper 50% of our dataset. The descriptive information for this scenario (Table 14) show that the average losses almost doubled, and the standard deviation increased by less than a half. Under this scenario, coverage limits of US$ 50 million might fall short of covering some of the losses (only 83% of the losses are covered by this cover limit), which will make it more difficult to establish an insurance market.

Scenarios #3 – "Worst-Case"-Scenario

Scenario #3 is a worst-case scenario in that we look into the actual tail of our data. That is, we consider only the worst 10% of all historical cases to generate potential losses from cyber risk. This results in a much higher mean loss and much higher standard deviation of losses (Table 14). For this scenario, average losses are almost nine times higher and the standard deviation almost three times higher than in Scenario #1. In this case, standard cover limits like US$ 50 million will not be sufficient (only 15% of the losses in our data are covered by this cover limit) and the establishment of an insurance market might be very difficult.

Scenario #4 – "Black Swan"-Scenario

In Scenario #4 we analyze a scenario which goes beyond what can be observed in historical data. We look at a cyber-catastrophe such as the long-term breakdown of the internet and its impact on the different layers. To integrate this "black swan scenario" we concentrate on four studies:

1. The National Academy of Sciences (NAS) (2008) estimates the catastrophic damage to society from a geomagnetic storm (similar to the 1859 Carrington Event) at about US$ 1 to US$ 2 trillion in social and economic costs a year. In addition, the NAS claims that the recovery from such an event can take 4 to 10 years.

2. According to the WEF (2010) a comprehensive and timely restricted critical information infrastructure breakdown generates costs of about US$ 250 billion to US$ 1 trillion. The probability that such a major event will occur is estimated at 10 – 20% over a 10-year time horizon.

3. The scenario presented by the Cambridge Center for Risk Studies (CCRS) (2014) explores the corruption of the software of a fictional market-leading relational database vendor by a malicious insider. Because of the company's important position in the market, failures integrated in software updates spread quickly and are active in companies around the globe (the losses are thus extremely correlated). It is slowly developing in the systems (e.g., also corrupts back-up systems) and remains undetected for a long time. The global macro-economic impact is estimated as a loss to global GDP output over 5 years of between US$ 4.5 and US$ 15 trillion depending on the scenario variant. In the worst-case

scenario the damage caused is predicted to be as severe as that of the 2007 to 2012 financial crisis.

4. Lloyd's (2015) predicts an incident with a total impact to the US economy at US$ 243 billion, increasing to more than US$ 1 trillion in the most extreme version. The scenario assumed malware that infects electricity generator control rooms and causes blackouts, leaving 93 million people in 15 US states (including New York City and Washington DC) without electricity for at least 24 hours. The insured losses are estimated at US$ 21.4 billion and US$ 71.1 billion in the most extreme event.

We use WEF (2010) and Lloyd's (2015) to derive our potential "Black Swan" event. The total costs discussed in both references are similar (US$ 250 billion vs. US$ 243 billion). In addition, they describe a similar event: time-restricted breakdown of critical information infrastructure. WEF (2010) has the advantage that there is also a probability of loss occurrence being defined. Thus, we expect a "black swan" to produce an aggregated loss of US$ 250 billion with a probability of occurrence of 10% (for a more conservative version of the scenario, see WEF, 2010). To stay in our old setup we consider one primary insurer who would suffer a loss of US$ 250 billion which is equally distributed across all risk owners and which occurs with a probability of 10%. In this scenario we assume a correlation in the primary insurer's portfolio of one that is every risk owner has a loss leading to the aggregate value of US$ 250 billion (Appendix E). In addition, the high correlation assumption in this model can be connected to the NAS (2008) and CCRS (2014) studies. The empirical comparison of the Scenario #4 with the previous three shows that average losses and their standard deviation further increase (Table 14). Clearly a standard cover limit of US$ 50 million will not be sufficient; even the incorporation of the reinsurance-layer might not be sufficient. In this context we have to discuss other layers of risk transfer (capital markets and government). The role of the government in "Black Swan"-events will be discussed in Section 5.2.

4.3 Results in the Reference Model

4.3.1 Parameter Summary for the Reference Model

In Table 15 we present the parameters used in the reference model. These parameters will then be varied in subsequent robustness analyses to test the sensitivity of the results with respect to the chosen parameter.

Table 15 Parameter Definitions in the Reference Model

Parameter	Value	Description	Motivation
X	Random variable	Random variable describing the losses at the risk owner level. The distribution function of losses is fitted on a cyber risk dataset by a log-normal distribution. With probability *p* an incident occurs and then is distributed as described in *X*, and with a probability of *(1-p)* no loss occurs[51]	Standard model in actuarial science (e.g., Kaas et al., 2008, p. 18). Since distributional assumptions for cyber risk are essential, we also analyze the results with respect to other distributional assumptions (Section 4.4.3). We use a log-normal distribution since we were able to observe particular good fits for this data sample (Eling and Wirfs, 2016). In addition, Edwards, Hofmeyr, and Forrest (2015) used a data breach sample and identified the log-normal with the best fit as well.
p	0.1	Loss probability	Based on WEF (2010). Sensitivity analyses in Section 4.4.3.
λ^{RO}	0.5	Risk loading on risk owner premium, paid to primary insurer	Based on historical loss ratios and expert opinions: general property and liability contracts often use a loading of 0.3. An additional uncertainty loading is necessary for new types of risk so that a loading of 0.2 is added as an additional buffer.[52]
λ^{PI}	0.5	Risk loading on the primary insurer premium, paid to the reinsurance company	Based on historical loss ratios and expert opinions, see also λ^{RO}.
$\lambda^{RO\text{-}fixed}$	US$ 1.0m	Fixed loading on the premium to cover costs	Based on historical expense ratios and expert opinions. Results for varying fixed loading presented in Section 4.4.3.
$\lambda^{PI\text{-}fixed}$	US$ 3.0m	Fixed loading on the reinsurance premium to cover costs	Based on historical expense ratios and expert opinions. Results for varying fixed loading presented in Section 4.4.3.
α^{RO}	6.0	Risk aversion parameter in the mean-standard deviation-utility function of the risk owner	A parameter greater than zero represents risk aversion. The motivation for this parameter is given by the assumptions made in Müller, Schmeiser, and Wagner (2011). The effect of this parameters size will be analyzed in Section 4.4.3.
α^{PI}	5.0	Risk aversion parameter in the mean-standard-deviation-utility function of the primary insurer	We define $a^{PI} < a^{RO}$, because the diversification effects possible in primary insurance make them less risk-averse than risk owners. The effect of this parameter will be analyzed in the sensitivity analyses of Section 4.4.3.
α^{RE}	4.0	Risk aversion parameter in the mean-standard deviation-utility function of the reinsurer	We define $a^{RE} < a^{PI}$, because the further diversification effects possible in reinsurance make them less risk-averse than primary insurers. The effect of this parameter will be analyzed in the sensitivity analyses of Section 4.4.3.
n^{PI}	50	Number of contracts in the primary insurer portfolio	Based on expert opinions. In Section 4.4.2 the effect of portfolio sizes will be analyzed separately.
n^{RE}	10	Number of contracts in the reinsurer portfolio	Based on expert opinions. In Section 4.4.2 the effect of portfolio sizes will be analyzed separately.

The parameters defined in Table 15 are the basic parameters necessary for the evaluations in the "No insurance" model, the "Conventional Model" and the

[51] From these distributional assumptions, losses for the primary insurer's and reinsurer's portfolios can be generated (e.g., individual risk model in Kaas et al., 2008, p. 17, and Appendix E).

[52] We use the inverse of the loss ratio (minus one) to estimate the necessary risk loading. The average loss ratio for the top 50 property and casualty markets in the world was 73% from 2010 to 2014, resulting in a loading of 0.36 (Aon Benfield, 2014). We will estimate robustness in pricing approaches for λ^{RO} and λ^{PI} in Section 4.5.2.

"Conventional Model with Reinsurance." For the "Conventional Model with Reinsurance and Capital Markets" several new assumptions on parameters have to be made. The model itself is explained in Section 4.2.2. The parameters necessary for the two versions of this model (i.e., the "Conventional Model with Capital Markets" and "Conventional Model with Reinsurance and Capital Markets") are summarized in Table 16.

Table 16 Parameter Definitions in the "Conventional Model with Capital Markets"

Parameter name	Supposed value	Description	Motivation
Panel A: Model with a Cyber Cat bond issued by the Primary Insurer			
B		Face value of the cyber risk catastrophe bond	We test face values between US$ 10 million and US$ 1000 million.
AP	US$ 80 million	Attachment point of the cyber risk catastrophe bond – indicating the amount which must be exceeded before the bond pays an indemnity	Since we define this model as an alternative to the reinsurance contract, we assume that the amount that has to be covered by the primary insurer is equal under the "Conventional Model with Reinsurance" and the "Conventional Model with Capital Markets."
K	$= B$	Maximal payment from the cyber risk catastrophe bond	This parameter is similar to a cover limit in the reinsurance contract. In case the loss above the AP exceeds K all initial payments of the investor are used to cover the losses (worst case for investor).
$r^{Zero\text{-}Coupon}$	3%	Rate of return for the zero-coupon catastrophe bond	We motivate this value by the average over USA 10-year zero-coupon yields for the last ten years (which is approximately 3.2%).
r_f	1%	Risk-free interest rate (necessary for the computation of the Sharpe Ratio)	Might be a bit high in the current low-interest environment and might be up to discussion. However, the parameter will only be used in the computation of the Sharp Ratio where it – if it is too high – leads to a very conservative investor's decision criterion.
Sharpe Ratio	0.6	The Sharpe Ratio that must be exceeded by the investment such that the investor will enter the agreement	Kunreuther, Kleindorfer, and Grossi (2005) assume a Sharpe Ratio of 0.6 for their analysis of a cat bond. This value is based on historical data. For offering a cyber cat bond we assume that the investors will require at least the same benchmark as for natural catastrophe bonds. Because of the innovativeness of the topic we could also add an addition security premium.
Panel B: Model with a Cyber Cat bond issued by the Reinsurer			
B		Face value of the cyber risk catastrophe bond	This parameter is up to variation. We test face values between US$ 10 million and US$ 5,000 million.
AP	US$ 50 million	Attachment point of the cyber risk catastrophe bond – indicating the amount which must be exceeded before the bond pays an indemnity	This value was up to variation as well, since the introduction of a risk transfer mechanism for the reinsurer was not in place before. We choose the one that generated the biggest effect on the overall solutions in the reference model.
K	$= B$	Maximal payment from the cyber risk catastrophe bond	This parameter is similar to a cover limit in the reinsurance contract. In case the loss above the AP exceeds K all initial payments of the investor are used to cover the losses (worst case for investor).
K, $r^{Zero\text{-}Coupon}$, r_f, *Sharpe Ratio*		Are chosen as in the first model	These parameter should be independent of the modeling approach analyzed.

4.3.2 Reference Model

We first present the results for Scenario #1 for all models: (1) "No insurance," (2) "Conventional Model," (3) "Conventional Model with Reinsurance," and (4) "Conventional Model with Reinsurance and Capital Markets." We will then present the results for Scenarios #2 and #3 under this reference model, in comparison to the results in Scenario #1 in Section 4.3.3. We will also show the effect of the "Black Swan" scenario (Scenario #4). The results of governmental intervention, established in the "Collaborative Model," are presented in Section 4.6.

"No insurance":
In the "No insurance" case, we assume that the risk owner is able to cover all potential losses. Since this might be not realistic (we provide a more detailed analysis where we relax this assumption by introducing a further constraint on the ruin probability of the individual, see Section 4.5.4), but it provides us with a benchmark for the subsequent analyses. For a risk aversion parameter $a^{RO} = 6.0$ and the losses described by the random variable X the utility of the risk owner is

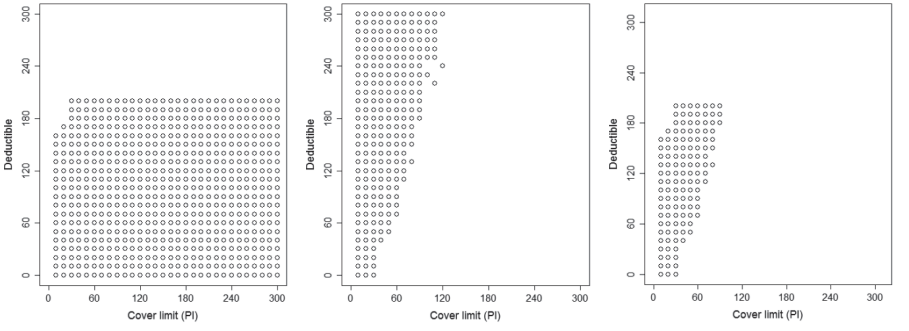
$$U^{RO}_{No\,Insurance} = -42.54\,.$$

Only if the risk owner's utility in the following models is greater than $U^{RO}_{No\,Insurance}$, the risk owner will buy insurance.

"Conventional Model":
This model adds a primary insurer that offers cyber insurance contracts with deductibles D and cover limits C. To identify feasible contracts (i.e., those (C, D)-combinations that increase the utility for both the risk owner and primary insurer), we vary deductibles and cover limits. The cover limit and deductible values in the reference model will vary from US$ 0 to 300 million. For the risk owner, all contract specifications are beneficial in which the utility with insurance is greater than $U^{RO}_{No\,Insurance}$. For the primary insurer, all contracts are offered under which the coverage of such insurance contracts produces a higher utility than the utility if no insurance would be offered. In Figure 3(a) and (b) we plot the feasible contracts with respect to the cover limit and the deductible. The indicated areas present contracts which are beneficial for the risk owner (Figure 3(a)) and the primary insurer (Figure 3(b)). We call those areas "solution sets." Finally, in Figure 3(c) we present the overlap which shows all (C, D)-combinations (i.e., contract specification) that produce higher utility

for both parties than their reference value. Thus, only for those overlapped solutions can an insurance market be realized.

Figure 3 Solution Sets for the "Conventional Model" – Scenario #1



(a) Risk Owner (b) Primary Insurer (c) Overlap

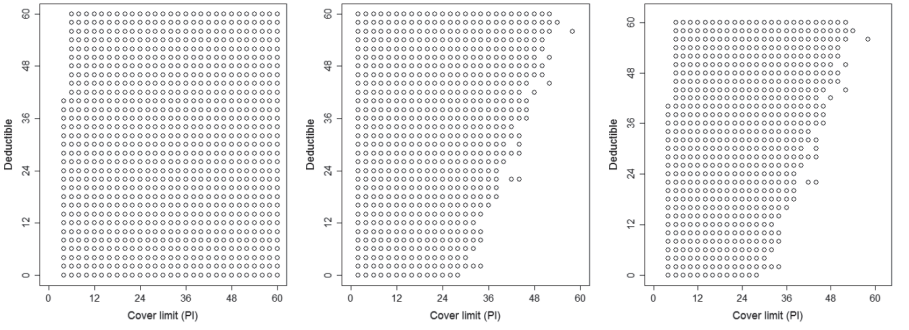
Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

For the risk owner, contracts with high deductibles do not increase the expected utility compared to the no-insurance case. If deductibles are higher than about US$ 200 million, the risk owner has to cover most of the potential losses on its own. These extremely high losses (above US$ 200 million) however, are very unlikely, and so insurance for this particular risk might be too expensive. Primary insurers are not willing to enter into an insurance contract if cover limits are high. The lower the deductible and the higher the cover limit, the higher the loss the insurer has to cover. In addition, if the deductible is very low, moral hazard problems might occur. Thus, a cyber insurance market with reasonable deductibles would only be possible with small cover limits and thus small levels of coverage (Figure 3(c)).[53] Higher cover limits are only possible, if the deductibles are also very high (between US$ 180 million and US$ 200 million in our scenario). The results presented in Figure 3 accurately reflect the situation in the cyber insurance market where only small coverages (e.g., with a maximum of US$ 50 million) are offered.

To show that the effects observed in Figure 3 already exist on very low levels for cover limits and deductibles, we show a close-up of the lower left corner of the previous analysis (Figure 4). Deductibles and cover limits range from US$ 0 to 60 million.

[53] For example, in this base scenario the insurance company is willing to offer only US$ 30 million of coverage, if the policyholder does not want a deductible. Only if the risk owner would accept a deductible of US$ 40 million, then the insurer expands its cover from US$ 30 million to US$ 40 million, clearly illustrating the limits of insurability.

Figure 4 Excerpt of Solution Sets for the "Conventional Model" – Scenario #1



(a) Risk Owner (b) Primary Insurer (c) Overlap

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 2 million.

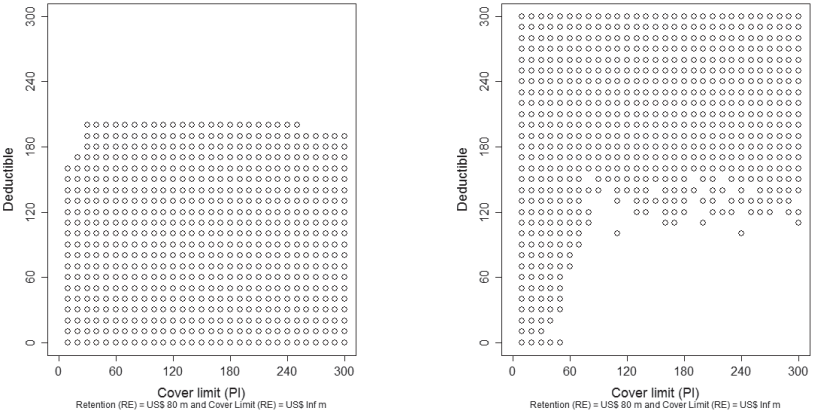
We can see that the primary insurer is not willing to offer high cover limits if the deductibles are low. The more fine-grained analysis shows that the actual cover limit for no-deductible contracts is at US$ 28 million, increasing with deductibles. Furthermore, we can observe an additional effect for the risk owner much better in this close-up analysis. For extremely small cover limits (e.g., US$ 2 million) the risk owner will not accept any contracts, independent from the deductible. This minimal coverage required increases with deductibles. The risk owner thus claims a minimal cover limit to accept insurance.

"Conventional Model with Reinsurance":

The third model adds a reinsurance company as an additional risk transfer layer, i.e., the primary insurer can transfer part of its business to the reinsurer. In Figure 5 we consider an excess-of-loss reinsurance contract with a retention of US$ 80 million.[54] The additional solution set for the reinsurer is given in Figure 5(c), the new overlap in Figure 5(d).

[54] For the reference model, we also assume that the contract does not have a cover limit on the reinsurance coverage. The analysis of the effect of cover limits for reinsurance are discussed in Section 4.5.1.

Figure 5 Solution Sets for the "Conventional Model with Reinsurance" – Scenario #1



(a) Risk Owner (b) Primary Insurer

(c) Reinsurer (d) Overlap

Note: The dotted areas in part (d) represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with reinsurance" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

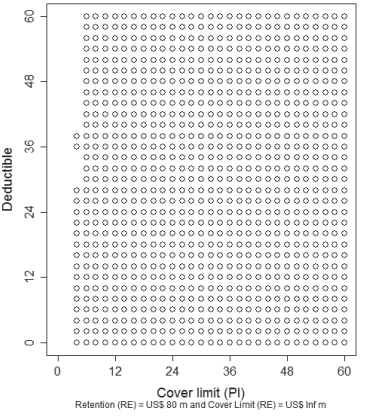
With the inclusion of reinsurance, the solution sets for the risk owner do not change and the upper level for the deductible stays the same (about US$ 200 million). However, with reinsurance the primary insurer is willing to accept insurance policies with higher cover limits for relatively high deductibles (Figure 5(b)). In addition, to the contracts offered under the "Conventional Model" the primary insurer would now offer also contracts with cover limits up to US$ 300 million for deductibles higher than

about US$ 150 million. But the reinsurer would not provide reinsurance contracts for these kind of primary insurance contracts. This might be because the aggregated primary insurer's loss under those contract specifications becomes large and the reinsurer would have to cover a severe loss from the primary insurer's portfolio. This is similar to the primary insurer in the "Conventional Model," who was not willing to offer cyber policies to the risk owner, in which the potential losses from each insurance contract were high.

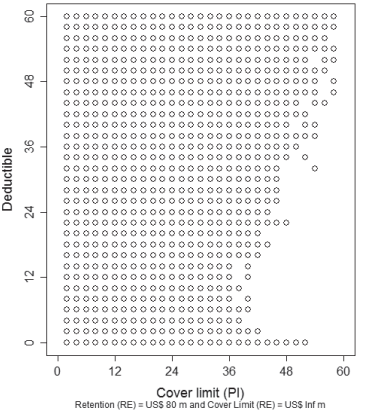
Figure 5(d) shows that with reinsurance the area of feasible cyber insurance policy designs can be increased, especially since it increases the possibilities for the primary insurer. The size of this increase depends on the retention level in the reinsurance contract. If retention levels are low, some feasible solutions under the "Conventional Model" are not possible because these contracts are unprofitable for the reinsurance company. If retention levels are too large, some valid contracts under the "Conventional Model" are not offered because the primary insurer will not buy reinsurance for the given risk because it is too expensive.

As for the "Conventional Model" we also show an excerpt of the lower left corner of the analysis in Figure 5. The results for this close-up are presented in Figure 6.

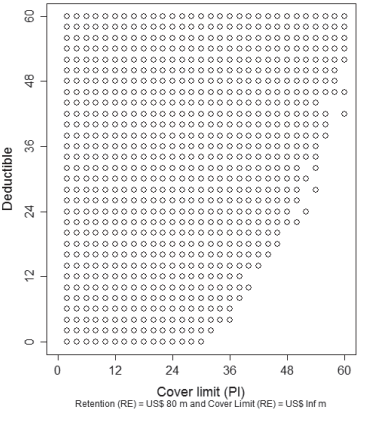
Figure 6 Excerpt of Solution Sets for the "Conventional Model with Reinsurance" – Scenario #1



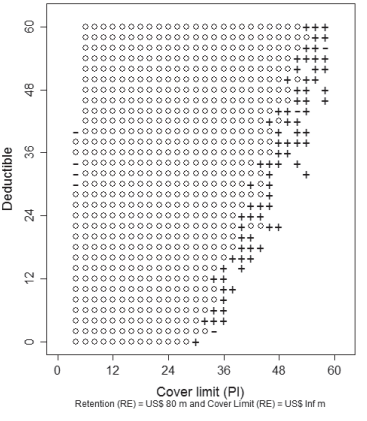
(a) Risk Owner



(b) Primary Insurer



(c) Reinsurer



(d) Overlap

Note: The dotted areas in part (d) represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Reinsurance" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 2 million.

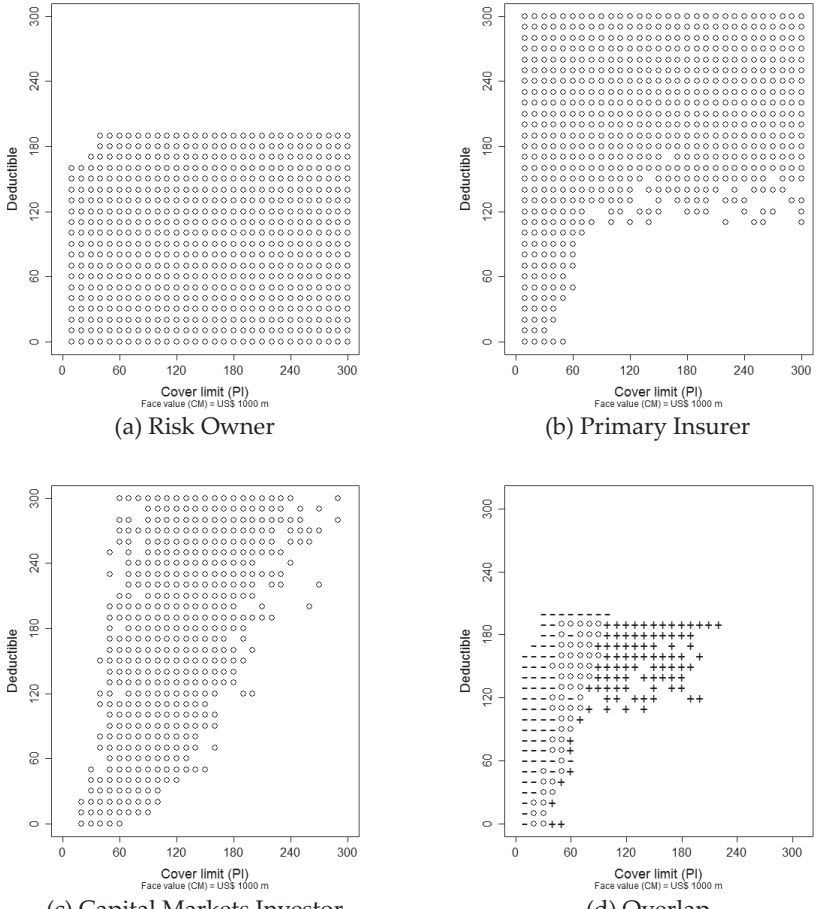
The increases in the solution set with reinsurance in place (i.e., more feasible contracts with reinsurance) can be seen more clearly in this fine-grained analysis. Figure 6(d) shows this on the right edge of the solution set. This means with the introduction of a reinsurance contract the primary insurer will be able to offer contracts with higher cover limits (per deductible) than in the "Conventional Model."

"Conventional Model with Capital Markets":

First we analyze the effect of a capital market solution if the primary insurer issues the cyber cat bond. Under this model we neglect the reinsurance layer (i.e., we use the capital market solution as a form of reinsurance). Because of the cyber cat bond's definition, we will always have a deductible (or "attachment point") and a cover limit (denoted here by $K \leq B$). Thus, comparability of the results presented here with the reinsurance contract discussion in the "Conventional Model with Reinsurance" might be limited.[55] To ensure at least some kind of comparability, we choose a cyber cat bond with a large face value B (US$ 1,000 million) and a small attachment point AP (US$ 80 million). This means we have the same retention/attachment point level in both models, but still – however, very high now – a cover limit/face value in the "Conventional Model with Capital Markets." To make both models equivalent from the risk transfer contract specification, we would have to choose a face value of infinity, which would make the contract too expensive for both parties. The results for the analysis are presented in Figure 7.

[55] In this context also see the analyses of reinsurance contracts with a cover limit in Section 4.5.1.

Figure 7 Solution Sets for the "Conventional Model with Capital Markets" – Scenario #1



(a) Risk Owner (b) Primary Insurer

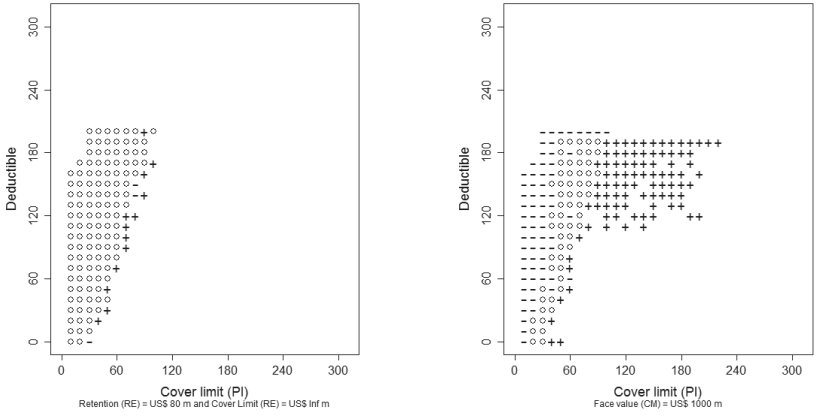
(c) Capital Markets Investor (d) Overlap

Note: The dotted areas in part (d) represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Capital Markets." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Capital Markets" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

Under the assumption adopted in Table 16, the analysis shows that the introduction of a cyber catastrophe bond leads to a decrease in the solution set for small cover limits (Figure 7(d) at the left edge of the solution set). This is because under very small cover limits the primary insurer's aggregated loss is small and might not trigger a payment from the cyber cat bond. Thus, the expected investor's return will be close to the return

of the zero-coupon, the variance of this return will be low, which then leads to a Sharpe Ratio not higher than the benchmark *SR*. In Figure 7(c) we can see that those contract specifications on the primary insurance-risk owner-level are not beneficial for the investors. In the case when cover limits are high and deductibles are low in the primary insurance contract, the primary insurer's aggregated loss is high, which then triggers a payment by the cyber cat bond. If the aggregated loss is too high, the investor's initial payment will be significantly reduced. Under those conditions, the potential loss of the initial payment cannot be compensated by higher returns and volatility of the investment (Figure 7(c)). This effect is similar to the effect observed for the reinsurance contract in Figure 5(c). The solution sets for the risk owner and the primary insurer look also quite similar to the ones in the "Conventional Model with Reinsurance." Beside the decrease in the solution set (overlap) for small cover limits, the introduction of the cyber cat bond enables contracts for medium-high cover limits (about US$ 70 million to US$ 200 million) and medium-high deductibles (about US$ 100 million to US$ 200 million). The increase in the solution set (Figure 7(d)) seems to be higher than in the model with reinsurance. For a comparison of the two models, see Figure 8.

Figure 8 Comparison of Solution Sets for Reinsurance and Capital Market Solutions in Scenario #1 – Overlaps

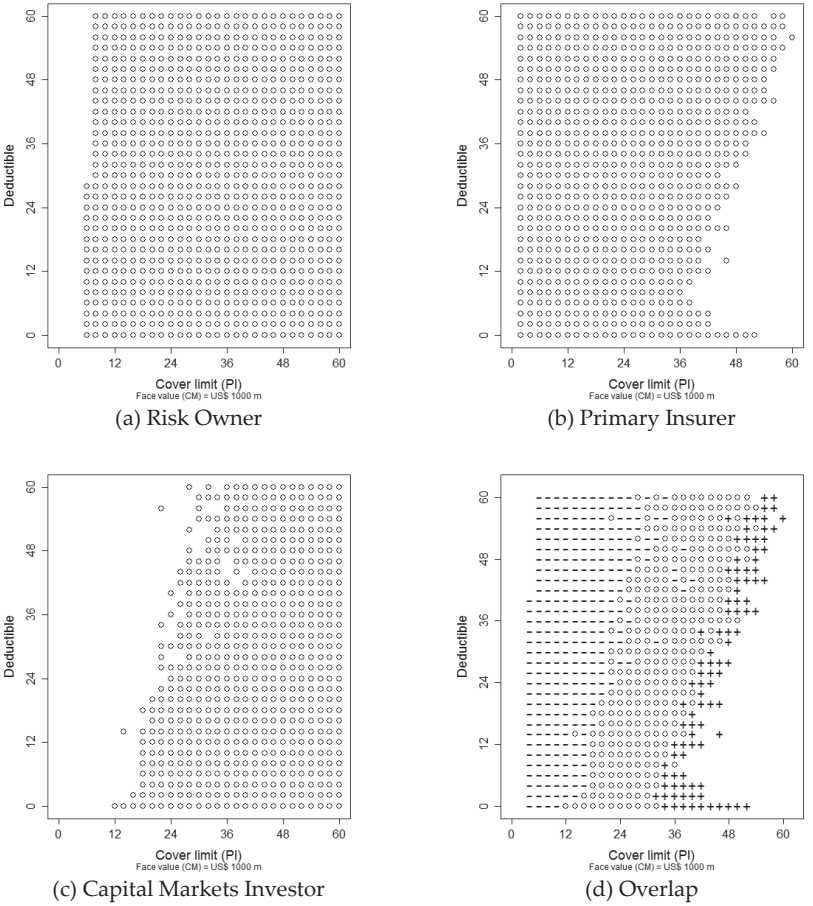


(a) "Reinsurance" (b) "Capital Markets"

Note: The dotted areas represent the solutions which are common under the "Conventional Model" and the (a) "Conventional Model with Reinsurance," (b) "Conventional Model with Capital Markets." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the (a) "Conventional Model with Reinsurance," (b) "Conventional Model with Capital Markets" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

Comparing the results from Figure 8, we have to conclude that under the assumptions made for the reference model the catastrophe cyber bond's effect on the insurability of cyber risk is higher on medium-sized deductibles and cover limits; however, there is a good effect for small cover limits, under which the reinsurance contract would be better. For completeness reasons, we also look at a close up of the results in the "Conventional Model with Capital Markets" in Figure 9.

Figure 9 Excerpt of Solution Sets for the "Conventional Model with Capital Markets" – Scenario #1



(a) Risk Owner (b) Primary Insurer

(c) Capital Markets Investor (d) Overlap

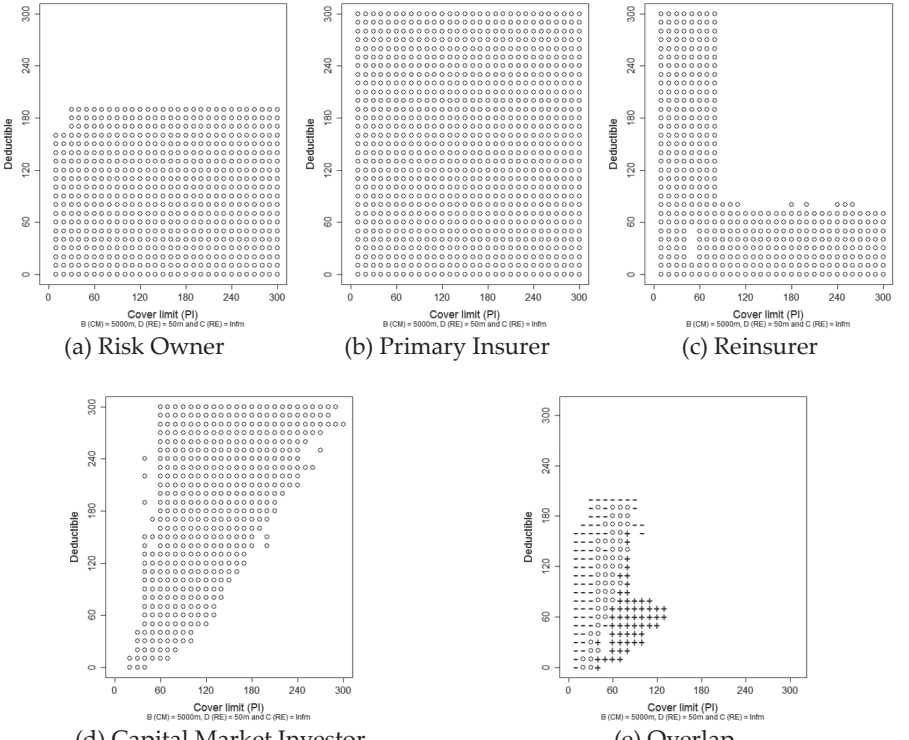
Note: The dotted areas in part (d) represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Capital Markets." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Capital Markets" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 2 million.

The effects presented in the overall setup (Figure 7) can also be observed in the close-up analysis. On the one hand, the introduction of a cyber cat bond will enable the primary insurer to offer higher cover limits (per deductible). On the other hand the cyber cat bond solution is not beneficial for primary insurance contracts with low cover limits (less than US$ 18 to 26 million).

"Conventional Model with Reinsurance and Capital Markets":
This model extends the "Conventional Model with Reinsurance" by a cyber cat bond that is issued by the reinsurance company. Thus, the reinsurer is able to transfer parts of its risk to the capital market. We assume that the reinsurer is thus willing to cover more losses from the primary insurance companies as in the model without this back-up system. Only if the aggregated loss in the reinsurance company increases, a risk transfer solution for the reinsurer makes sense. The more complex these models become the more opportunities there are to define the different contracts. For simplicity, we assume for this reference model a reinsurance contract with a deductible of US$ 50 million and no cover limit. The latter is done for two reasons: (1) to provide comparability with the original model ("Conventional Model with Reinsurance"); and (2) to increase the reinsurance company's risk exposure, such that the risk transfer to a cyber cat bond should be most attractive. The definition of an optimal cyber cat bond (not necessarily most attractive for the reinsurer, but for the overall market solution) is a task in itself. For this instrument we could vary the attachment point and the face value (respectively, the maximal payout of the bond if $K \neq B$). For simplicity we will also choose values in advance, even if they might not be the optimal contract specifications. However, the results will make the relationships in this model clear.

Therefore, we define a cyber cat bond with an attachment point of US$ 50 million and a face value B of US$ 5,000 million. Since the face value and by that the maximal possible loss for the investor is relatively high ($K = B$; see Table 16), the cyber cat bond functions similar to a reinsurance contract for the reinsurer with an extensive cover limit. The results for the analysis in the "Conventional Model with Reinsurance and Capital Markets" is given in Figure 10.

Figure 10 Solution Sets for the "Conventional Model with Reinsurance and Capital Markets" – Scenario #1



(a) Risk Owner (b) Primary Insurer (c) Reinsurer

(d) Capital Market Investor (e) Overlap

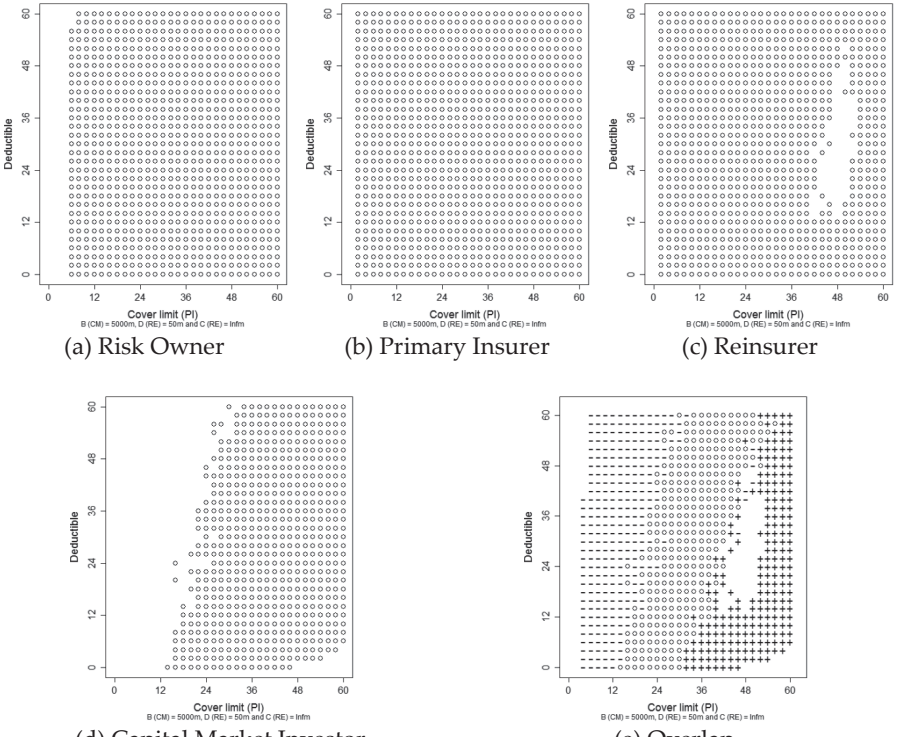
Note: The dotted areas in part (e) represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance and Capital Markets." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Reinsurance and Capital Markets" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

At first glance, the results for the "Conventional Model with Reinsurance and Capital Markets" indicate no change for the risk owner's solution set. However, minor changes can be identified at the upper bound of the solution set. Now, the risk owner will no longer accept insurance contracts with deductibles of US$ 200 million (Figure 10(e) at the upper bound of the solution set). According to Cummins and Mahul (2004) the risk owner will do so only if the costs are lower for the insurance policy. Thus, a system with a cyber cat bond issued by the reinsurer seems less expensive for the risk owner than a system without a capital market solution in place.

The introduction is also beneficial for the primary insurance company, which is now able to offer the whole range of deductible and cover limit combinations considered in the insurance contracts under the reference model. Compared with the "Conventional Model with Reinsurance" the reinsurer will offer reinsurance contracts if deductibles in the insurance contracts are low and cover limits are high. In Figure 5(c) we observed that those primary insurance contract combinations were not acceptable for the reinsurer without a capital market solution backup. The introduction of the capital market solution will thus also have a positive effect on the reinsurance industry. Finally, the solution set will show a similar results as for the "Conventional Model with Capital Markets." Although, some primary insurance contracts with low cover limits and medium deductibles will no longer be offered with a capital market as backup, contracts with medium high cover limits and low deductibles become feasible solutions.

As before, we present the results with a focus on small deductibles and cover limits in the primary insurance contract (Figure 11). The results underline the findings from Figure 10.

Figure 11 Excerpt of Solution Sets for the "Conventional Model with Reinsurance and Capital Markets" – Scenario #1



(a) Risk Owner (b) Primary Insurer (c) Reinsurer

(d) Capital Market Investor (e) Overlap

Note: The dotted areas in part (e) represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance and Capital Markets." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Reinsurance and Capital Markets" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 2 million.

4.3.3 Scenario Analysis in the Reference Model

A central property of cyber risk is the presence of a high risk of change (Section 2.5). The analyses done in the previous section are therefore very static and do not incorporate the opportunity for significant changes in the risk. This will be analyzed in this part of the study by a scenario analysis. We will test the impact of different scenarios for the loss characteristics in the distributions given in Section 4.3.2. A detailed definition of the four scenarios we apply is given in Section 4.2.3. We start with the estimation of the "No insurance" model.

"No insurance":

We now focus on the comparison of the scenarios and how the changes in severity of losses change our results. The utility of the "No insurance" model under the different scenarios is given in Table 17. The utility decreases when scenarios become more severe (Scenario #1 to #4). This is because the utility function subtracts the losses' standard deviation and expected value from the initial capital, which both increase with the scenarios (Table 14) while the initial capital is constant.

Table 17 Reference Utility Values from the "No insurance" Model

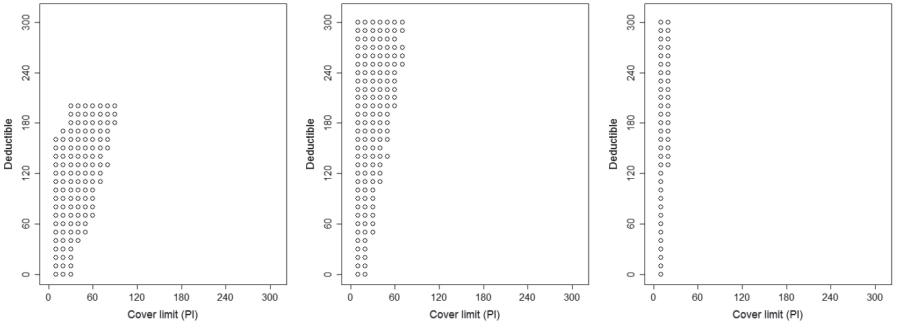
	Utility of model "No insurance"
Scenario #1	-42.54
Scenario #2	-109.56
Scenario #3	-359.11
Scenario #4	-5,000.00

Since Scenarios #2 and #3 are also based on the data as Scenario #1 (reference model), we will compare those three scenarios in the next section. We will look at Scenario #4 separately and then in more detail.

"Conventional Model":

In the following we will only show the overlapped solution sets. A description of the effects in each single stakeholder's solution sets was discussed in Section 4.3.2. More detailed analyses of the results are available upon request. The results of the "Conventional Model" are presented in Figure 12.

Figure 12 Comparison of Solution Sets in the "Conventional Model" across Scenarios #1 to #3 – Overlaps



(a) Scenario #1 (b) Scenario #2 (c) Scenario #3

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

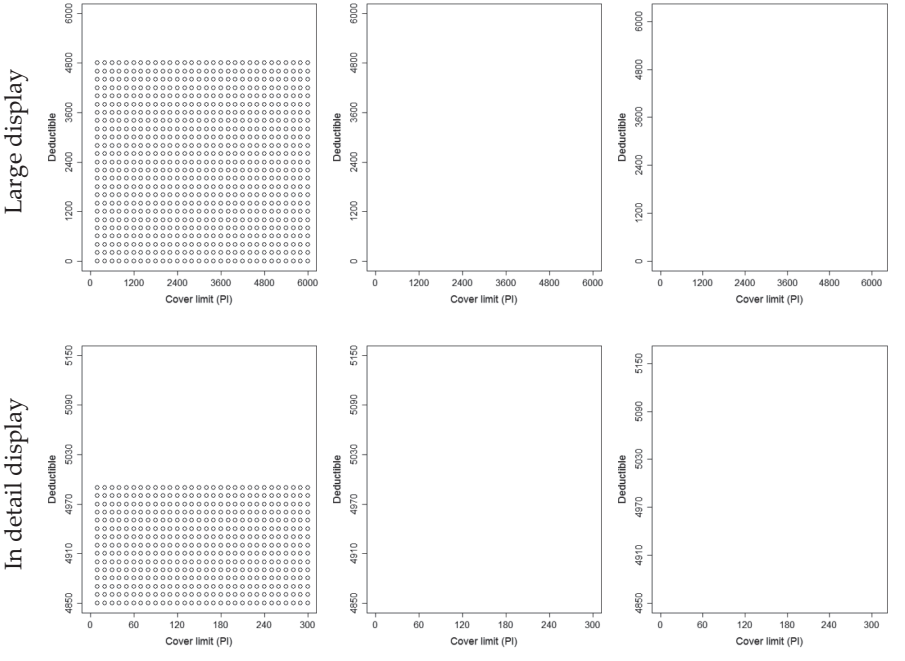
When losses become more severe, the solution sets vary substantially. We observe that with an increase in the loss severity (going from Scenario #1 to #3) high deductible levels for small cover limits become attractive, which were not before (upper left corners of Figure 12(b) and (c)). This is due to an increased willingness of the risk owner to accept deductibles to receive coverage even if cover limits are low. While under Scenario #1 the risk owner was willing to accept at most deductibles up to about US$ 200 million, this increased to more than US$ 300 million in Scenario #2 and #3.[56] The results presented here are in line with findings from Cummins and Mahul (2004).

The scenario analysis of the "Conventional Model" shows a second effect. The offered cover limits decreased significantly with the scenarios. Under Scenario #3 only cover limits of about US$ 20 million are feasible, from the originally about US$ 90 million in Scenario #1 (Figure 12(a) for deductibles of US$ 180 to 200 million). This is due to the primary insurer's unwillingness to accept those contracts under severe scenarios. The results from the scenario analysis prove that a cyber risk development under which the losses become more severe makes an insurance market for cyber risk unattractive, both for risk owners and primary insurers. Even under Scenario #3 an effective insurance market, as we can observe it in the real market right now, could not be realized.

[56] Note, that we only show contracts with deductibles up to US$ 300 million to guarantee comparability with the reference model of Section 4.3.2. The feasible deductibles are probably much higher than the US$ 300 million value mentioned here.

In the following we will analyze the effect of an even worse scenario, i.e., the "Black Swan"-event. Under Scenario #4 we assume that the risk owner faces a loss of US$ 5 billion (US$ 250 billion/number of contracts in the primary insurer's portfolio (50 under the reference model)), which will occur with a probability of 10%. If a loss occurs, all contracts in the primary insurer's portfolio generate a loss of US$ 5 billion, exposing the primary insurer's portfolio to an aggregated loss of US$ 250 billion (the correlation is thus one). The results for Scenario #4 in the "Conventional Model" are presented in Figure 13.

Figure 13 Solution Sets for the "Conventional Model" – Scenario #4



(a) Risk Owner (b) Primary Insurer (c) Overlap

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 200 million upper row; bins of US$ 10 million lower row.

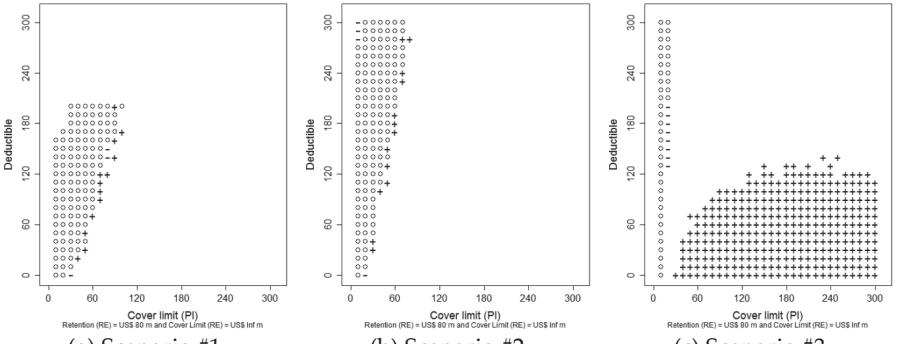
The risk owner is only willing to accept contracts in which the deductibles are smaller than US$ 5 billion (Figure 13(a), in particular detailed display, lower row). This is because, there are only losses up to this benchmark possible for the risk owner, so accepting deductibles higher than that would mean they would have to cover the loss

completely by themselves.[57] The primary insurer is not willing to offer insurance contracts for any considered contract design. If deductibles are higher than US$ 5 billion, no portion of the loss is paid by the primary insurer in case of loss occurrence. Consequently, there are not premiums earned either, since the expected loss is zero. If deductibles are smaller than US$ 5 billion, the primary insurer has to face the worst loss possible in case of an incident (because of high correlation), although premiums were computed on the expected loss per contract. Thus, premiums earned will not cover the losses that might occur, which is why the primary insurer will not cover anything. No feasible solution in this model is possible under Scenario #4.

"Conventional Model with Reinsurance":

The comparison of overlaps for the "Conventional Model with Reinsurance" is presented in Figure 14.

Figure 14 Comparison of Solution Sets in the "Conventional Model with Reinsurance" across Scenarios #1 to #3 – Overlaps



(a) Scenario #1 (b) Scenario #2 (c) Scenario #3

Note: The dotted areas represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Reinsurance" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

Again, the introduction of a reinsurance contract increases the potential solution sets as in the reference model. In particular for the third scenario the introduction of a reinsurance contract can significantly increase the solution set for high cover limits and small deductibles. This effect in Scenario #3 is surprising, since contracts with low

[57] The net premium for instances with deductibles above US$ 5 billion is zero, since the expected loss to pay by the primary insurer is zero. However, if choosing the insurance contract, the risk owner would still have to pay the fixed risk loading to cover costs (e.g., administration).

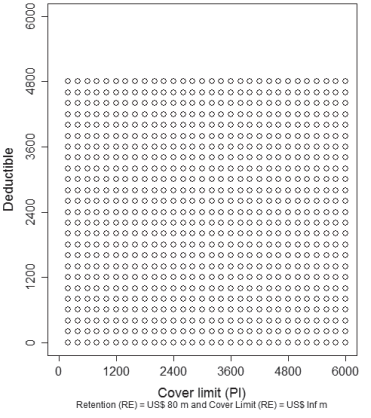
deductibles and high cover limits in the primary insurance contract were avoided by the primary insurer and the reinsurer in Scenario #1. This was due to generating high aggregated losses for the primary insurance company. Latter should apply in particular for Scenario #3, where losses become more severe. However, why does the same reinsurance contract provide so much more solutions in Scenario #3 than in Scenario #1?

An explanation for this result could be as follows: the excess-of-loss reinsurance contract that is used in the reference model, is an instrument primarily utilized to cover extreme losses in the primary insurer's portfolio. The setup used to model the losses in the scenario analysis generates losses with a high diversity in severity for Scenario #1. Thus, only in few cases extreme losses could lead to an extreme aggregated primary insurer loss that requested reinsurance for the given premium. However, in Scenario #3 only extreme losses were generated that almost all lead to an aggregated primary insurer loss that exceeded the retention of the reinsurance. The explanation could thus be that the excess-of-loss reinsurance contract is too expensive for non-extreme primary insurer losses and only became profitable when the losses in the primary insurance portfolio significantly increased. The latter is particularly true for low deductibles and high cover limits in the primary insurance contracts.

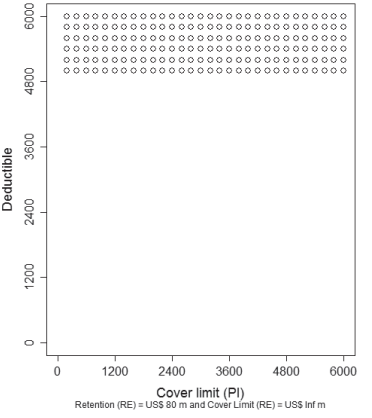
In the "Conventional Model with Reinsurance" there is no feasible solution in scenario #4 (see Figure 15 for an example with even higher retention levels in the primary insurance contracts than in the reference model). By introducing a reinsurance contract (equal to the one in the reference model) the solution set for the primary insurer can be increased; however, the reinsurance company is not willing to offer reinsurance for those primary insurance contracts. Even though the reinsurer would offer reinsurance to the primary insurer, no overall solution could be generated because the risk owner's and primary insurer's solution sets do not overlap (similar discussion as in the "Conventional Model").[58] The detailed analysis comparable to the scale given in Figure 13 (second row) does not show any overlaps either.

[58] In comparison with the surprising results for Scenario #3 under this model, losses in Scenario #4 are too high because of correlation to be beneficial for the reinsurer.

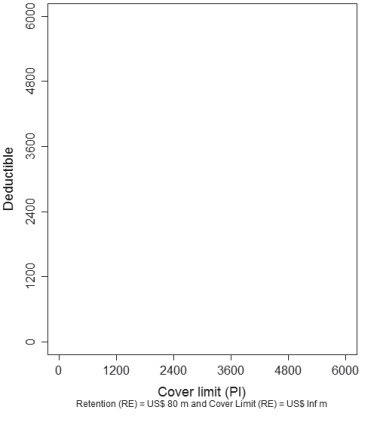
Figure 15 Solution Sets for the "Conventional Model with Reinsurance" – Scenario #4



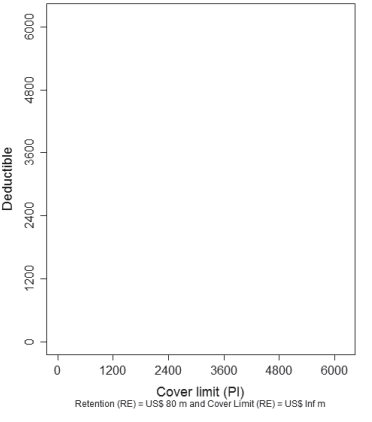
(a) Risk Owner



(b) Primary Insurer



(c) Reinsurer



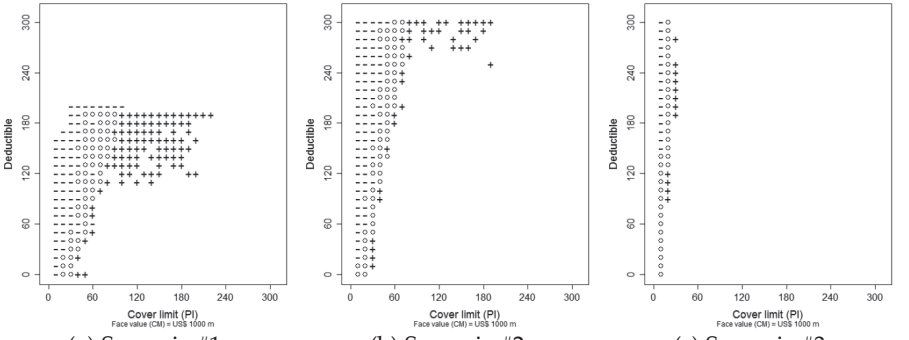
(d) Overlap

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 200 million.

"Conventional Model with Capital Markets":

In the following model we replace the reinsurance company by the capital market solution. In the reference model we identified a positive effect of the cyber cat bond on the size of the overlapped solution set (Figure 16(a)). Similar effects can be observed for Scenarios #2 and #3, although the effect is not that significant as in Scenario #1. For Scenario #3 this effect is not as significant as the increases generated by the introduction of a reinsurance contract (compare Figure 14).

Figure 16 Comparison of Solution Sets in the "Conventional Model with Capital Markets" across Scenarios #1 to #3 – Overlaps

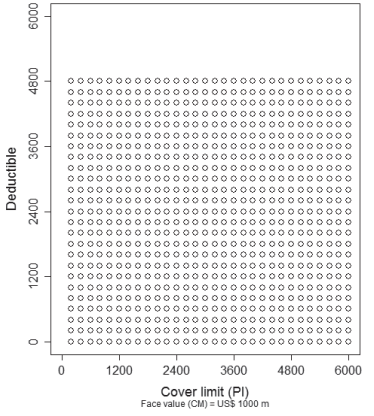


(a) Scenario #1 (b) Scenario #2 (c) Scenario #3

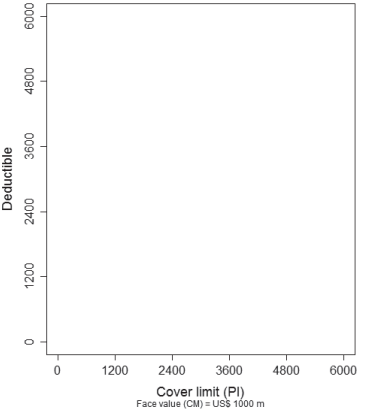
Note: The dotted areas represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Capital Markets." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Capital Markets" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

Looking at the effect of a cyber cat bond issued by the primary insurer in case of an extreme scenario (#4), no feasible solution is possible (Figure 17). This is in line with the previous models for Scenario #4. The risk owner still asks for cyber insurance coverage with deductibles less than US$ 5 billion, the primary insurer – and the capital market investor – are not offering any contract. Under the "Conventional Model with Reinsurance" the solution set of the primary insurer could be increased, but for the cyber cat bond this is not possible. That might be because of the expensive premiums necessary for cyber cat bonds under risks defined in the more severe scenarios. For instance, while the reinsurance contract under the "Conventional Model with Reinsurance" is priced based on the expected indemnity payment by the reinsurer, the cyber cat bond's price is based on the face value, which is independent from the risk. Thus, the costs for the cyber cat bond are equal for any risk underwritten by the primary insurer, and by that might not be profitable for all underlying risks. Nevertheless, no feasible solution in the overlap can be generated under the "Conventional Model with Reinsurance" and/or the "Conventional Model with Capital Markets."

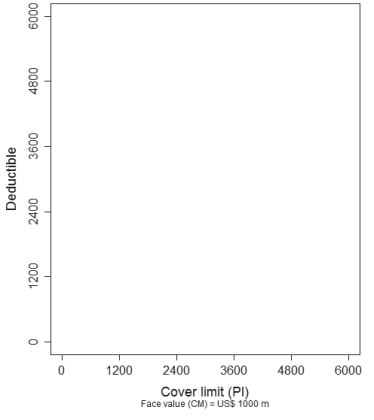
Figure 17 Solution Sets for the "Conventional Model with Capital Markets" – Scenario #4



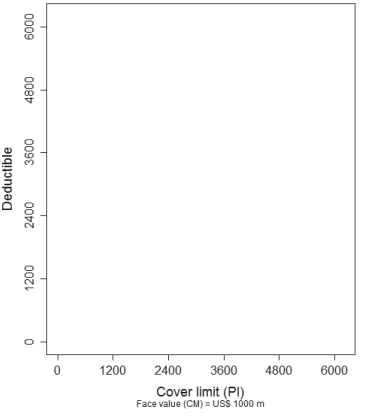
(a) Risk Owner



(b) Primary Insurer



(c) Capital Market Investor



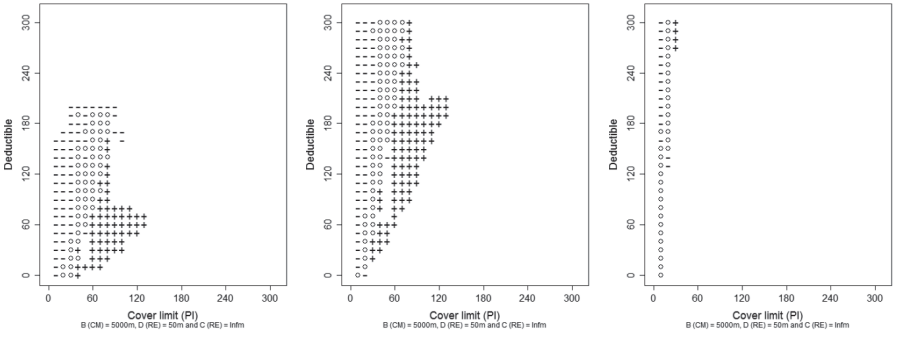
(d) Overlap

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 200 million.

"Conventional Model with Reinsurance and Capital Markets":

Finally, we present the results for the scenario analysis for the last model in the reference (Figure 18).

Figure 18 Comparison of Solution Sets in the "Conventional Model with Reinsurance and Capital Markets" across Scenarios #1 to #3 – Overlaps



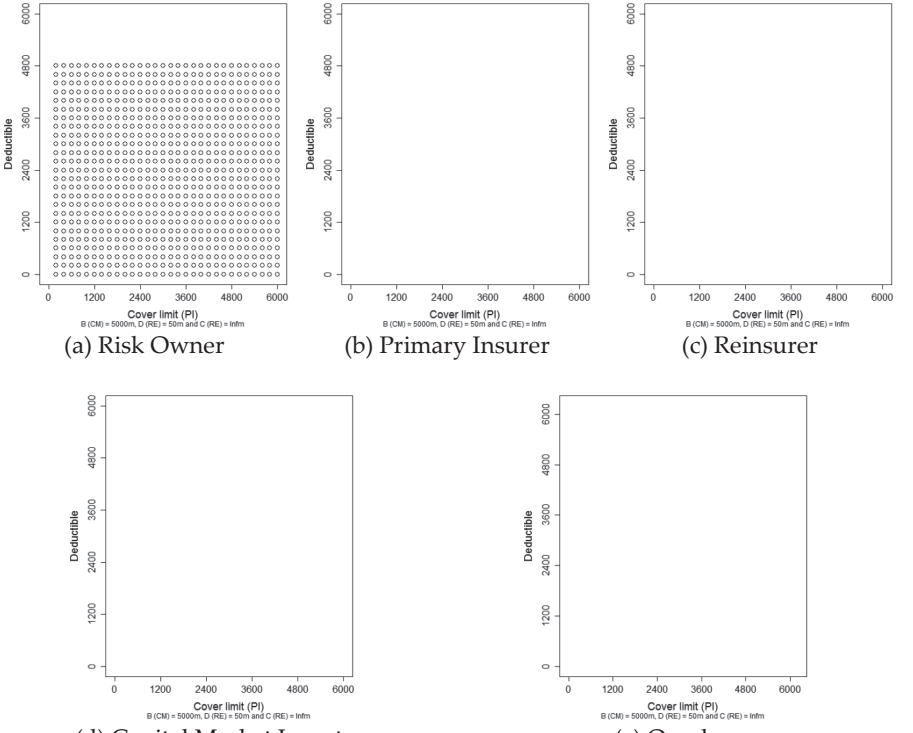
(a) Scenario #1 (b) Scenario #2 (c) Scenario #3

Note: The dotted areas represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance and Capital Markets." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Reinsurance and Capital Markets" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

In the previous model of the scenario analysis, we did not observe a significant improvement by the introduction of a cyber cat bond (issued by the primary insurer) on the solution sets of the "Conventional Model." This will not change under the "Conventional Model with Reinsurance and Capital Markets" (i.e., a reinsurer that issues the bond). For instance, in Scenario #3 almost no further feasible solution is added. Thus, the implementation of cyber cat bonds can contribute to the development of the cyber insurance market only if losses do not change significantly. If losses become greater, a cyber cat bond does not seem to be a feasible instrument.

As before, we also look at Scenario #4 for this model (Figure 19). The results are the same in the "Conventional Model with Capital Markets". The risk owner asks for contract designs that no one is willing to offer. Under none of the considered risk transfer models is the development of an insurance market in a "Black Swan" event possible. Thus, for such scenarios government might have to step in to improve insurability.

Figure 19 Solution Sets for the "Conventional Model with Reinsurance and Capital Markets" – Scenario #4



(a) Risk Owner (b) Primary Insurer (c) Reinsurer

(d) Capital Market Investor (e) Overlap

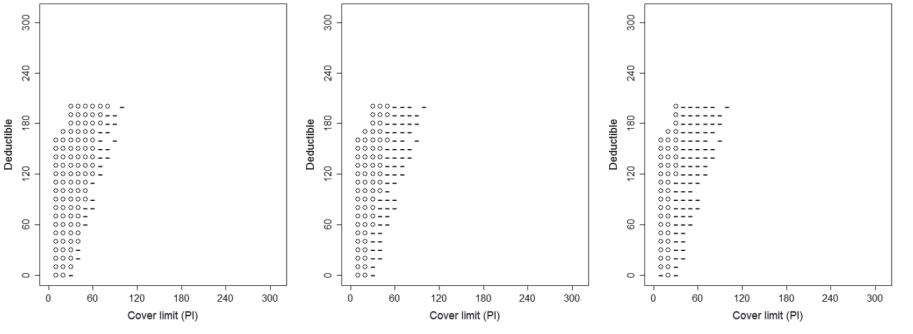
Note: Axes are labeled in US$ 1 million; axes: bins of US$ 200 million.

4.4 Sensitivity in the Reference Model

4.4.1 Correlation in the Portfolio

The results presented so far are based on the assumption that the losses in a portfolio are independent. In this section we consider the more realistic case that cyber losses in the primary insurer portfolios are correlated (e.g., Baer and Parkinson, 2007).[59] The approach used to simulate correlated losses in the primary insurer's portfolio is provided by Cossette, Gaillardetz, Marceau, and Rioux (2002). Figure 20 shows the results for three correlation assumptions (Low: $q = 0.05$, Medium: $q = 0.2$, and High: $q = 0.5$) in comparison to the basic results (no correlation at all, $q = 0.0$).

Figure 20 Solution Sets for Correlated Portfolios in Scenario #1 of the "Conventional Model" – Overlap



(a) $q = 0.05$ (Low) (b) $q = 0.2$ (Medium) (c) $q = 0.5$ (High)

Note: The dotted areas represent the solutions which are common under the "Conventional Model" without correlation and the "Conventional Model" with correlation. Areas indicated by a "-" identify those solutions by which the solution sets in the "Conventional Model" with correlation are smaller compared to the "Conventional Model" without correlation. Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

Insurance is based on the law of large numbers, which states that if more mutually independent risks are clustered together, the more likely the average aggregated loss of this portfolio converges to the expected loss, thus decreasing variance and resulting in decreasing security levels. This mathematical proposition holds only if the losses are independent. Correlation between the losses in the portfolio decreases the solution sets compared to the independent case. This is due to a decrease in the primary

[59] Similar analyses can be also conducted for correlations in the reinsurer's portfolio. The results are similar to the observations for the primary insurer and are available upon request from the authors.

insurer's solution set. Since the aggregated loss of the primary insurer increases with increasing correlation, the insurer should protect the own company by raising deductibles and reducing cover limits.[60] In Figure 20 we observe that the latter is especially the case in our analysis (solution set decreases at the right border, meaning lower cover limits). This analysis shows that correlation in the primary insurer's portfolio has a massive influence on the potential contract designs that can be offered. Thus – if correlation is too high – the development of an adequate market for cyber risk is hampered.

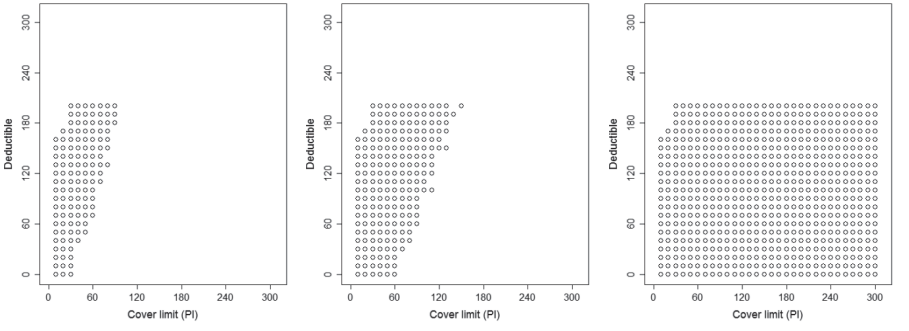
4.4.2 Size of Portfolios

According to the law of large numbers, with an increasing portfolio the average loss of the portfolio will converge to the expected loss (if risks in the portfolio are independent; see discussion in the previous section). Thus, the larger the portfolio the lower the portfolio's variance (per contract), and by that the lower the security loadings needed in the contracts. However, cyber risks are stated to be correlated (e.g., Baer and Parkinson, 2007), and therefore large portfolios exhibit potential problems with accumulation. The effect of pool size is therefore analyzed in this section.

We vary the size of the primary insurer's portfolios from 50 (Low) policyholders (reference for primary insurance portfolios in Section 4.3.2), to 100 (Medium) and 500 (High). The results for this analysis are presented in Figure 21. Furthermore, we investigate the effects of reinsurer's portfolio size on the development of primary insurance contracts. We apply portfolio sizes of 10 (Low) (reference for reinsurance portfolios in Section 4.3.2), 20 (Medium), and 100 (High), with the assumption that a regular primary insurance portfolio consists of 50 contracts. The results for reinsurance are shown in Figure 22.

[60] The primary insurer might also buy reinsurance or sell portions of its risk at the capital market. However, this should not be part of this model, and we already addressed these effects in the "Conventional Model with Reinsurance" and the "Conventional Model with Reinsurance and Capital Markets" on the previous pages. The results for these special cases can be made available upon request.

Figure 21 Comparison of Solution Sets for Different Portfolio Sizes in the "Conventional Model" in Scenario #1 – Overlap

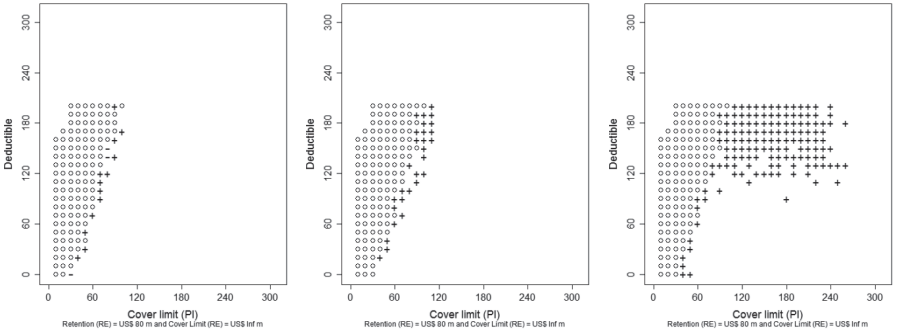


(a) Small (50 policies) (b) Medium (100 policies) (c) Large (500 policies)

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

By varying the size of the primary insurer portfolio, we observe that with an increasing number of policies the solution sets become bigger. The more contracts are pooled at the primary insurer level, the more contracts with smaller deductibles and higher cover limits can be offered by the primary insurer. For the case with 500 insurance contracts in the portfolio the overlapped solution set is close to the one of the risk owner, which indicates that the primary insurer is willing to offer almost all contracts desired by the risk owner. This is a first indication that an insurance pool on the primary insurance layer could improve the insurability of cyber risks.

Figure 22 Comparison of Solution Sets for Different Portfolio Sizes in the "Conventional Model with Reinsurance" in Scenario #1 – Overlap



(a) Small (10 policies) (b) Medium (20 policies) (c) Large (100 policies)

Note: The dotted areas represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Reinsurance" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

Looking at the reinsurance portfolios, we yield similar results as for the primary insurer, although, the effect (i.e., the increase in the solutions sets) is not that significant as for the primary insurer. Nevertheless, the development of a cyber insurance market can benefit from an efficient pooling in the reinsurance market (e.g., by a (re-)insurance pool).

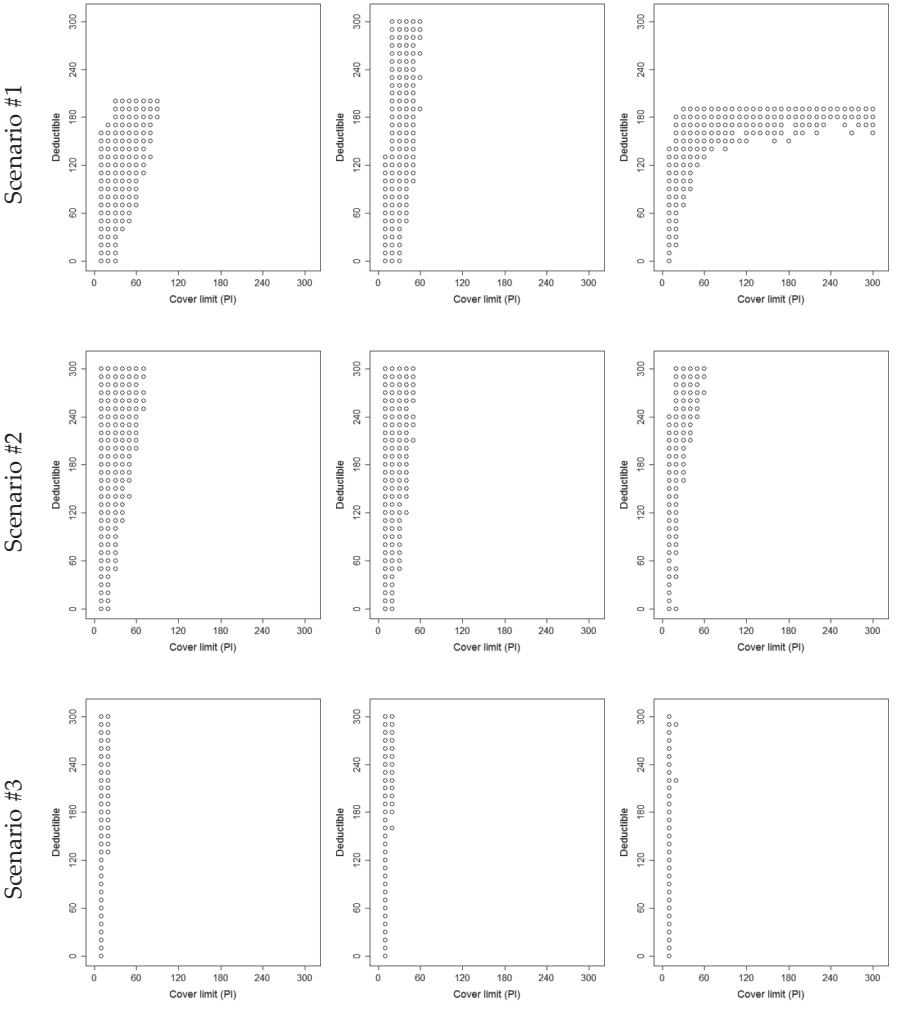
4.4.3 Additional Parameter Variations

Loss Distribution:

In Figure 23 we vary the loss distribution that was used to simulate the losses on the risk owner-level. Eling and Wirfs (2016) analyze the adequacy of loss distributions for cyber risks in more detail. Based on their findings we evaluate the results under the log-normal (reference model from Section 4.3) and the generalized Pareto distribution (GPD). Both distributional assumptions proved to be good fits for cyber risks. In addition, we will show the results with respect to the exponential distribution. The latter showed relatively poor results in the loss modeling approach (Eling and Wirfs, 2016). This will underline that the uncertainty problem with respect to modeling (e.g., how to model cyber losses) is an important issue for cyber risk. We will not analyze the results for Scenario #4, since those results are not based on the actual loss distribution estimated from our cyber risk dataset. For simplicity, we show only the

robustness for the risk owner-primary insurance-relationship (meaning the "Conventional Model"). Results for the other models are similar.

Figure 23 Variation of the Loss Distribution in the "Conventional Model" – Overlap



(a) Log-normal distribution (reference) (b) GPD (c) Exponential distribution

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

The results for the exponential distribution significantly deviate from the results for log-normal and GPD, in particular for Scenario #1. This might be because the latter two

distributions model losses with heavier tails better (e.g., McNeil, Frey, and Embrechts, 2015) and we identified cyber losses to have heavy tails (Eling and Wirfs, 2016). This result shows the impact of the uncertainty in modeling approaches (no actuarial standards) that are present in cyber risk. It thus emphasizes more (and in detail) actuarial analyses for cyber risks. However, the development of solution sets over the different scenarios is similar for all distributions: with increasing severity of losses, solution sets become extremely small and customized contracts (e.g., with small deductibles and high cover limits) are unavailable.

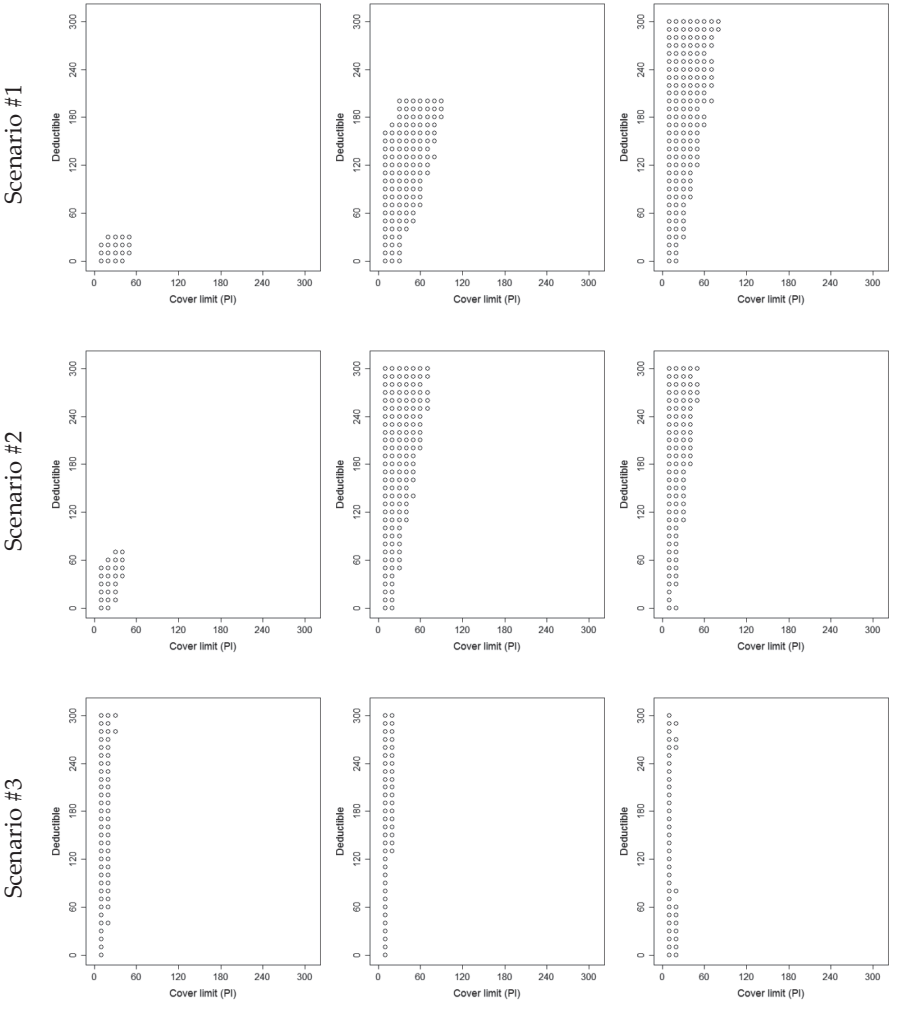
Loss Probability:

A second crucial assumption in the reference model is the loss probability. In the reference model we chose a $p = 10\%$ probability of loss occurrence on the risk owner level. In Figure 24 we present the results for a loss probability of $p = 5\%$, $p = 10\%$ (the reference case) and $p = 20\%$. With an increasing probability of loss occurrence the solution sets seem to be stretched upwards. This can be explained as follows: if the probability is relatively high, so is the expected risk owner's loss. To compensate for the higher loss, the risk owner should wish for insurance contracts with a higher cover limit (given a fixed deductible). However, if the risk owner's expected loss increases (because the probability of occurrence increases), the primary insurer's aggregated loss also rises. The primary insurer should thus reduce cover limits and increase deductibles. That is what we saw in the scenario analysis for more severe losses (Section 4.3.3), where the primary insurer reduced cover limits. This effect is observable on the horizontal axis of Figure 24 (from (a) to (c)). For instance, in Scenario #1 we observe the isolated effect of increasing loss probabilities. With a loss probability of 5%, cover limits of about US$ 50 million were possible solutions for small deductibles (about up to US$ 30 million). With an increase of the loss probability to 10% and 20% the cover limits reduce for exactly these small deductibles (cover limits of US$ 30 million for $p = 10\%$, and only US$ 20 million for $p = 20\%$). Therefore, if the primary insurer does not fulfill the risk owner's desire for higher cover limits, the risk owner's only way to receive the higher cover limits is to accept higher deductibles. This is the effect that can be observed in Figure 24(b) and (c) of Scenario #1 where cover limits of about US$ 50 million become feasible solutions only if deductibles rise higher than US$ 50 million and US$ 120 million.

The main result from this analysis is that an increase in the probability of loss occurrence will lead risk owners to accept higher deductibles for the same amount of

coverage. From a customer perspective this cannot be desirable.[61] For Scenario #4 no results are presented, because independent of the probability of loss occurrence, all models would not provide feasible solutions as observed in the reference model.

Figure 24 Variation of the Loss Probability in the "Conventional Model" – Overlap



(a) p = 5% (b) *p = 10%* (reference) *(c) p = 20%*

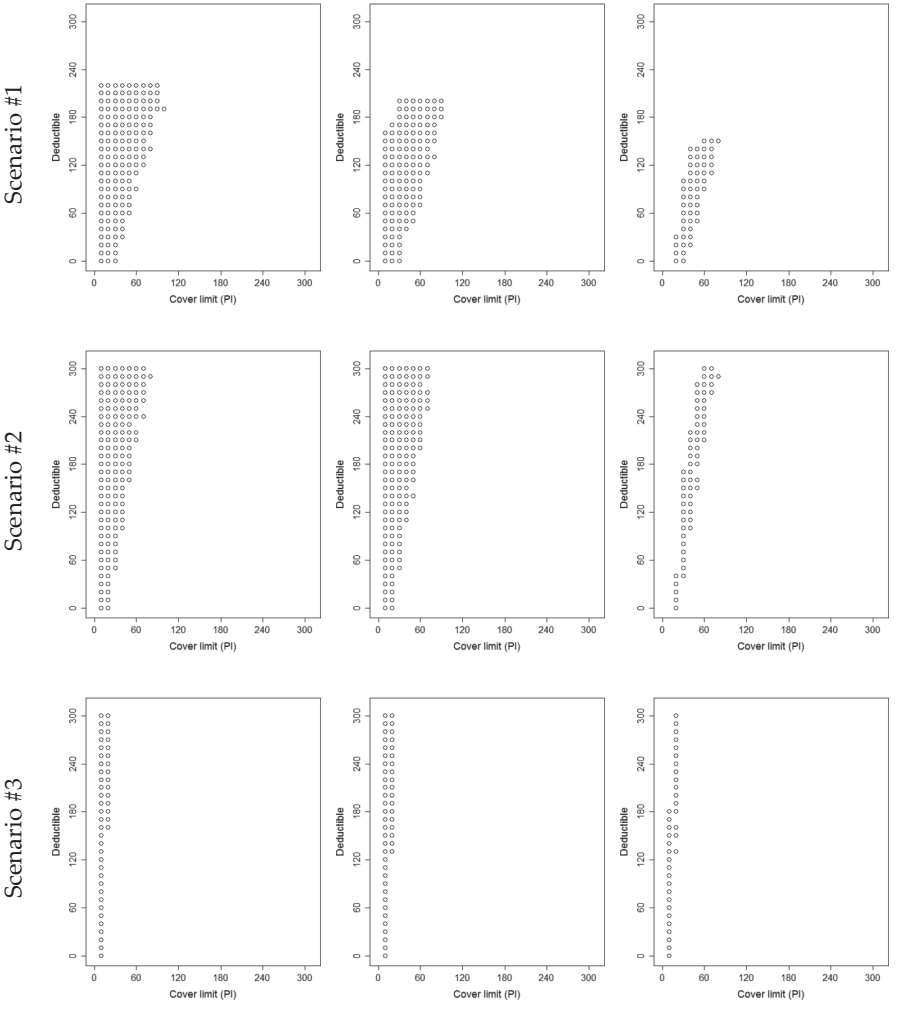
Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

[61] Remember, that an increase in the loss severity (e.g., by going from Scenario #1 to #3) has the same effect. This can be observed very well on the vertical axes of Figure 24.

Fixed Risk Loading:

The fixed risk loading, covering costs (e.g., for administration) is varied in this paragraph. Many analyses are conducted under the assumption of no costs (e.g., Mossin, 1968), but given the importance of cost loadings it should not be excluded in an extensive analysis of cyber risk. For the previous setup of the reference model we chose a fixed cost loading parameter of US$ 1 million (Section 4.3.1). First of all, we compare the results with a fixed cost loading parameter that is higher than the one in the reference model (US$ 5 million). In addition, we choose a contract that exhibits no additional costs. The findings can be derived from Figure 25. For Scenario #4 no results are presented, because independent of the fixed cost loading parameter, none of the models shows feasible solutions as observed in the reference model.

Figure 25 Variation of the Fixed Risk Loading in the "Conventional Model" – Overlap



(a) No costs (b) US$ 1 million (reference) (c) US$ 5 million (extreme costs)

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

The analysis with different values for the fixed loading shows significant changes in the solution sets for Scenarios #1 and #2. For the case in which no costs are included (Figure 25(a)) the solution sets are biggest and decrease with increasing cost level. It can be observed that the solution sets shrink for the high deductibles with low cover limits (particularly Scenarios #1 and #2 in Figure 25(b) and (c)). If fixed loadings increase, the premium payments for the risk owner – necessary to cover the same risk as before – are higher. These higher costs must be compensated by losses in feasible solutions. The solution sets for the primary insurer are unchanged, since fixed cost loadings are not connected to the primary insurer's cash flows. The observed effect is consistent with findings from Cummins and Mahul (2004).

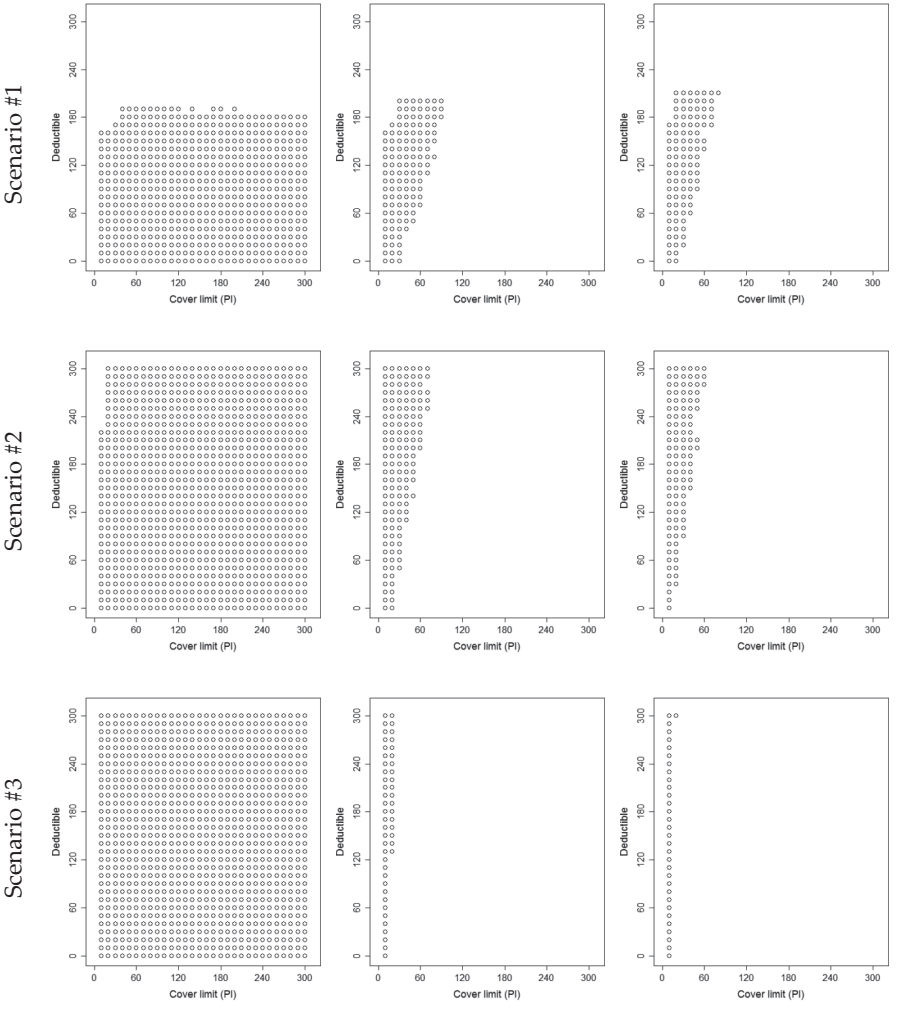
The final result of this paragraph is that costs for the insurance contract should not be too high, such that the insurance contract can be still beneficial to policyholders. This result also gives a first indication for governmental intervention to improve the development of the cyber insurance market. For instance, the state could subsidize the purchase of cyber insurance contracts by providing premiums for the costs emerging (i.e., the fixed loading factor).

Risk Aversion:

Finally, we vary the assumption on risk aversion. We assume different parameters for the model in alignment to arguments presented in Table 15. We will assume slightly lower and higher values for the computation. In the reference model we used a risk aversion coefficient for the risk owner of $a^{RO} = 6.0$ and for the primary insurer of $a^{PI} = 5.0$. In the high risk aversion scenario we estimate results with risk aversions of $a^{RO} = 8.0$ and $a^{PI} = 6.0$, and for the low risk aversion scenario we choose $a^{RO} = 4.0$ and $a^{PI} = 0.0$.[62] The results for this analysis can be found in Figure 26. For Scenario #4 no results are presented, because none of the models provide feasible solutions as observed in the reference model.

[62] The latter value describes risk-neutrality for the primary insurance company. In the reference model we followed the approach of risk aversion also for the insurance company stakeholder, to make sure they can also make decisions under uncertainty. Those were important to make sure that we can make the right decision for reinsurance or capital market solutions. In addition, this approach would be also in line with the results of risk aversion for risk managers in insurance companies found in Kunreuther, Hogarth, and Meszaros (1993). The implementation here illustrates why the assumption of risk-neutrality for the insurance companies in our model setup is not feasible.

Figure 26 Variation of the Risk Aversion Parameters in the "Conventional Model" – Overlap



(a) $a^{RO} = 4.0$ and $a^{PI} = 0.0$ (low risk aversion)

(b) $a^{RO} = 6.0$ and $a^{PI} = 5.0$ (reference)

(c) $a^{RO} = 8.0$ and $a^{PI} = 6.0$ (high risk averse)

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

The discussion of the results for different risk aversion parameters is similar to the one for increased probabilities of loss occurrence or increases in loss severity (scenario analysis). If the participants in the "Conventional Model" become more risk averse, they fear risk (i.e., the variance of losses) more that they would do under lower risk

aversion. Thus, for higher risk aversion parameters the solution sets decrease in cover limits (due to the effect in the primary insurer) and increase in deductibles (due to the effect in the risk owner). This is what we observe in Figure 26.[63]

The second effect that can be observed is the effect of risk-neutrality for the primary insurer on the solution sets (Figure 26(a)). Comparing these solution sets with the risk owner's solution sets in the scenario analysis (Section 4.3.3) shows hardly any difference. This is attributable to the risk-neutrality assumption for the primary insurer. If the primary insurance company is risk-neutral, it will offer any insurance contract as long as the earned premium for that contract exceeds the expected loss of that risk. For the setup in our model the premium for the insurance contract is defined by the expected loss plus an additional security loading $\lambda^{RO} \geq 0$ times the expected loss. The condition for the primary insurer is always satisfied and the primary insurer will always enter the insurance contract, independent of risk severities or frequencies of losses. This effect seems unrealistic, which is why the risk-neutrality condition does not work well with the pricing approach used in the reference model. To check for the effect of different pricing effects, see also Section 4.5.2.[64]

[63] Only the images in Figure 26 for Scenario #1 show the increases in deductibles due to higher willingness to accept those contracts by the risk owner. The decrease in cover limits can be observed in all scenarios.

[64] Another parameter that can be varied is the definition of the utility function. We refer to Wirfs (2016) for more details on this variation.

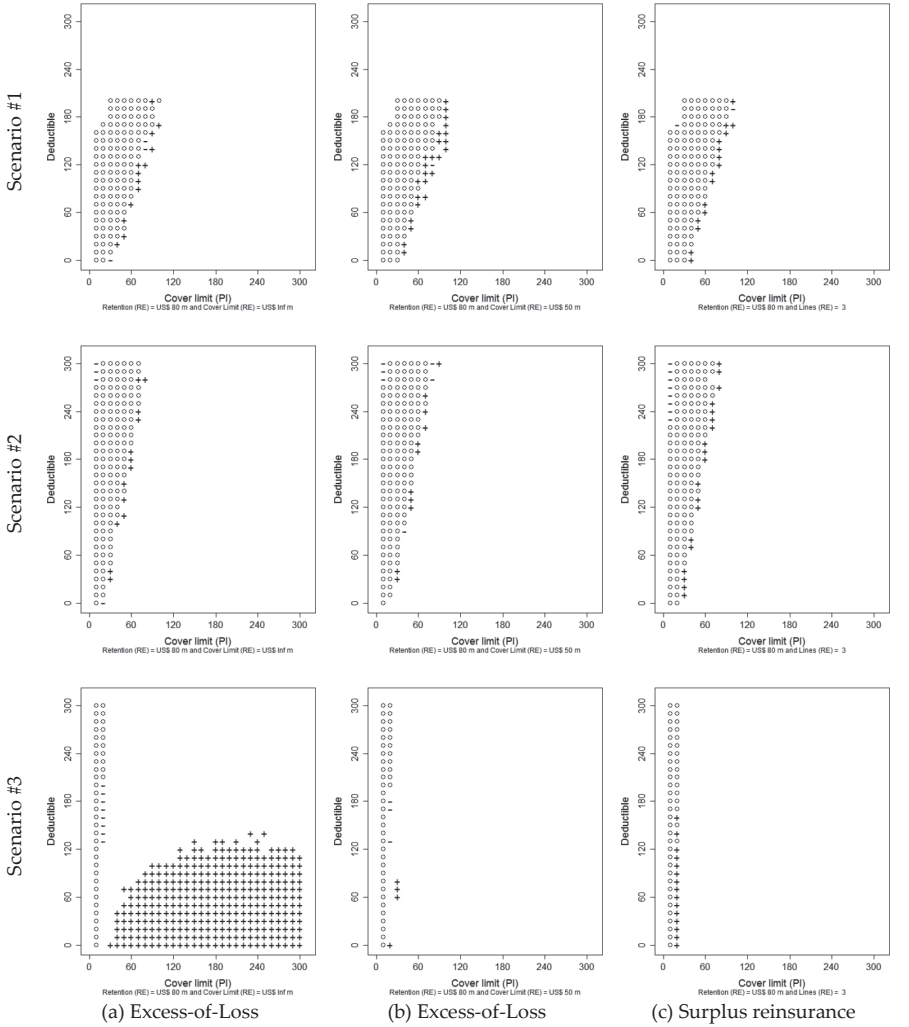
4.5 Extensions in the Reference Model

4.5.1 Analysis of Different Reinsurance Contracts

In Section 4.3.2 we analyzed the "Conventional Model with Reinsurance" with respect to an excess-of-loss reinsurance contract (as a representative of the non-proportional reinsurance category) with no upper limit on coverage. In this section we will determine the effect of a cover limit in the excess-of-loss reinsurance contract on the findings from the reference model (i.e., "Conventional Model with Reinsurance"). For the latter, we vary the cover limits from US$ 5 million to US$ 1,000 million, and identified an optimal cover limit on the excess-of-loss reinsurance contract of US$ 50 million (optimal means it generated the biggest overall solution set). In addition, we apply a surplus reinsurance contract as a representative of the proportional reinsurance category. The actual surplus reinsurance contract defined is a three-line surplus with a retention (line) of US$ 80 million. The retention level is set at US$ 80 million, to guarantee that retention levels under both reinsurance contracts (excess-of-loss and surplus) are similar. Results can be found in Figure 27.[65]

[65] Note, that for the analysis in this section we skip the results of the "Conventional Model," because the actual change in the model only applies to the extended model with reinsurance in place. In addition, we will not show results for Scenario #4, since none of the three reinsurance solutions was able to generate feasible solutions.

Figure 27 Comparison of Solution Sets for different Reinsurance Contracts in the "Conventional Model with Reinsurance" – Overlaps



(a) Excess-of-Loss reinsurance

(b) Excess-of-Loss reinsurance with cover limit

(c) Surplus reinsurance

Note: The dotted areas represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Reinsurance" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

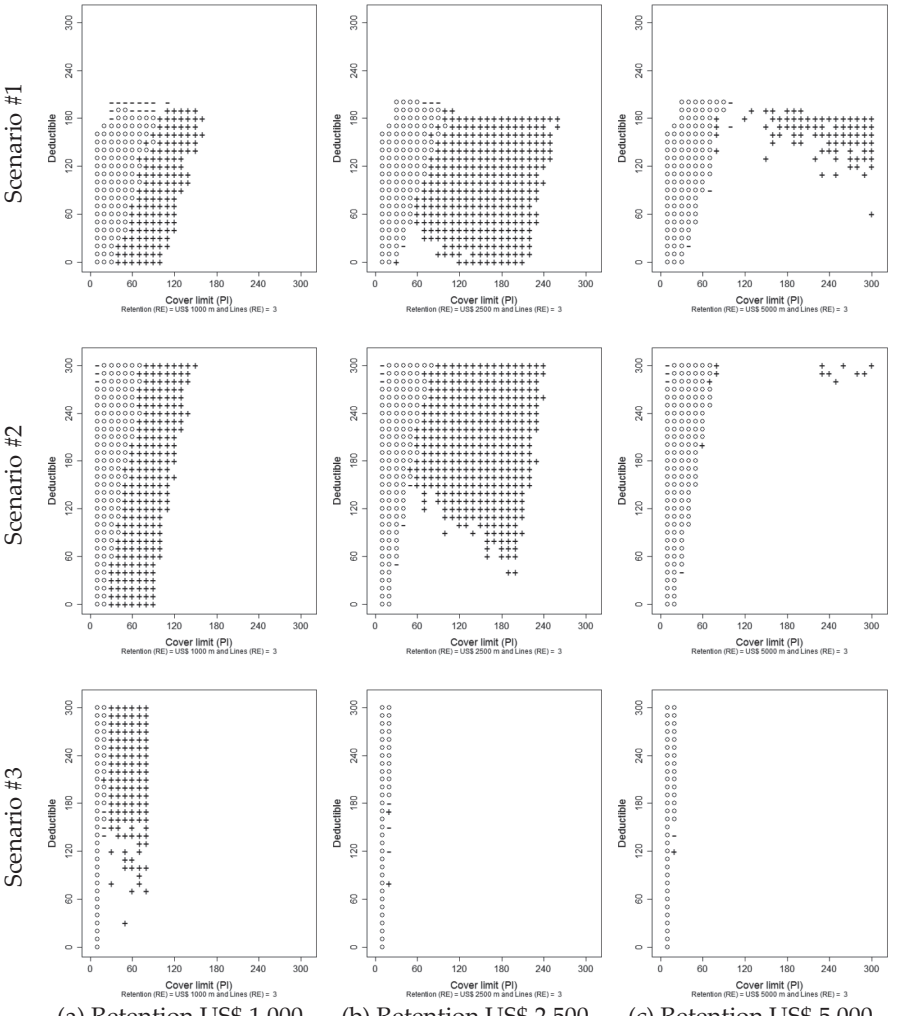
The results presented in Figure 27 do not show significant changes across the contract specifications in Scenarios #1 and #2. However, for Scenario #3, the excess-of-loss reinsurance contract without a cover limit has a much better effect on the cyber

insurance market. Under Scenario #3 the excess-of-loss reinsurance was beneficial for the market because of its ability to cover extreme losses (Section 4.3.3). With the introduction of a cover limit, this advantage is lost (Figure 27(b) and (c) for Scenario #3).[66]

Since the results for the surplus reinsurance contract indicate similar characteristics as an excess-of-loss reinsurance contract, we present different surplus reinsurance contract with higher retention levels of US$ 1,000 million, US$ 2,500 million, and US$ 5,000 million in Figure 28. This is done to analyze if there is a difference between surplus reinsurance and excess-of-loss reinsurance. The results show that the surplus reinsurance contract has advantages if the retention is wisely chosen. This was not the case in the examinations of Figure 27, where we artificially chose a retention level that was equivalent to the excess-of-loss contract. In addition, the appropriateness of the different contract designs (proportional vs. non-proportional) cannot be made on the contract details only, but the risk and the purpose of the instrument must be incorporated.

[66] A three-line surplus reinsurance contract with a retention level US$ 80 million, has also an upper level of coverage (i.e., 3 x US$ 80 million = US$ 240 million).

Figure 28 Surplus Reinsurance Contract with Different Retention Levels – Overlap



(a) Retention US$ 1,000 million (b) Retention US$ 2,500 million (c) Retention US$ 5,000 million

Note: The dotted areas represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance." Areas indicated by a "+" ("-") identify those solutions by which the solutions sets in the "Conventional Model with Reinsurance" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

The surplus reinsurance contracts show significant changes in the solution sets if retention levels are raised (higher than the US$ 80 million of Figure 27). The choice of reinsurance contract can thus have a significant influence on the size of the solution sets if contracts are appropriately defined. The areas gained in Scenarios #1 and #2

show solutions that could not be generated under the excess-of-loss reinsurance contracts (Figure 27). We also observe that if retention levels are set too high, the reinsurance contract's utility for higher scenarios decreases (Figure 28(c)). Conversely, if retention levels under the surplus contract are set too low (Figure 28(a)) the contracts are not that attractive under the none-worst-case scenarios.

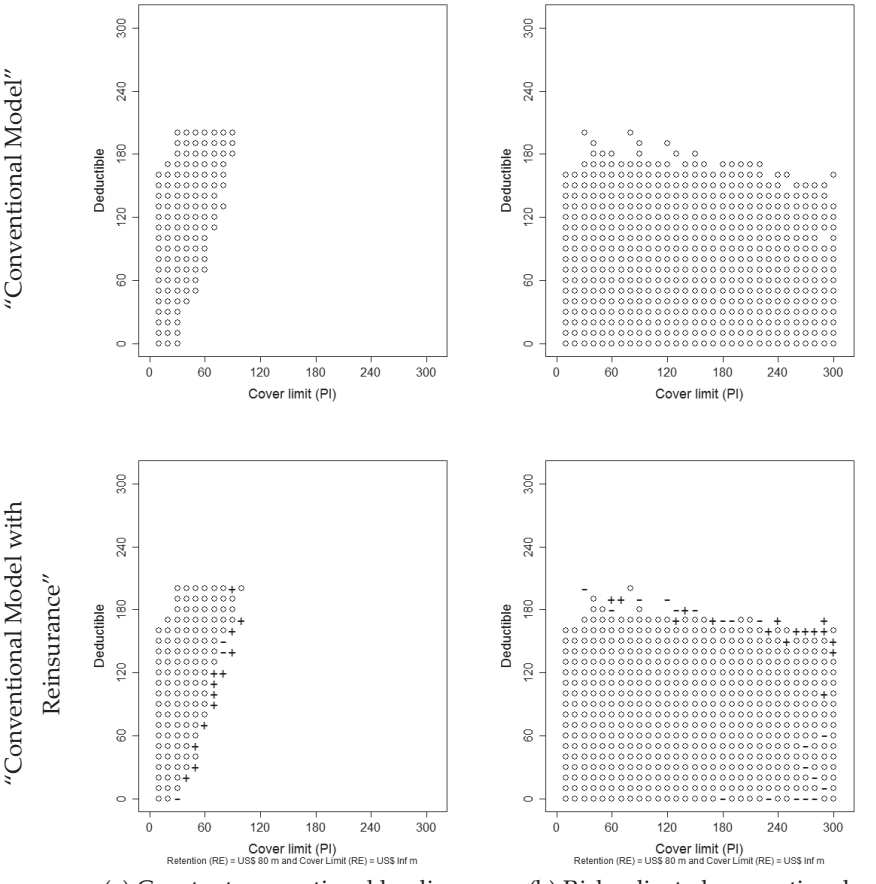
4.5.2 Alternative Pricing Approaches

As mentioned in Section 4.1, uncertainty with respect to data (data limitations) and in the modeling approaches lead to higher risk loadings and thus to high premiums. The approach used in the previous sections computed premiums with a constant proportional risk loading which was chosen in accordance with existing risk loadings for similar risks. These estimates were based on expert's experience with other risk categories, and an interpolation for cyber risk (see Section 4.3.1 for more information). A disadvantage of this model is that the actual loading is independent of the underlying risk. For instance, in cases where the primary insurer offers contracts with a low cover limit and high deductibles the fixed loading might be too high, but under contracts with high cover limits and low deductibles it might be reasonable or too low. In this section we compare the approach used in the reference model with one in which the proportional risk loading is computed risk-adequately. Therefore, we define the risk loadings in a way that the total premiums earned by a primary insurer can cover at least 95% of its expected losses. Thus, for every contract design (deductible-cover limit combination in the risk owner-primary insurer-relationship) a different risk loading is applied (which was equal for all contracts under the constant proportional loading). A similar argumentation of potential calculation approaches can be found in Gatzert and Schmeiser (2012). The results are presented in Figure 29.

The results show that sets of feasible solutions increase under the computations with a risk-adequate loading. This is due to premiums that are computed risk-adequately, which is why the primary insurer is willing to offer more contract combinations than it had been with a constant proportional risk loading. This is especially apparent in solutions with higher cover limits and low deductibles. It is also worth mentioning that for only a few of the insurance designs premiums rose so much that they became unattractive for risk owners (upper edges of solution sets in Figure 29(b)). Contracts with deductibles up to about US$ 200 million (with the accompanying cover limits) were attractive for risk owners under the constant proportional risk loading approach. This benchmark decreased slightly in deductibles from US$ 200 million to about US$

160 million – US$ 180 million (depending on the cover limit; see Figure 29(b)). This proves that uncertainty with respect to data (data limitations) and in the modeling approaches can have a significant effect on the insurance contracts offered.

Figure 29 Comparison of Different Pricing Approaches



(a) Constant proportional loading (b) Risk-adjusted proportional loading

Note: The dotted areas represent the solutions which are common under the "Conventional Model" and the "Conventional Model with Reinsurance." Areas indicated by a "+" ("-") identify those solutions by which the solution sets in the "Conventional Model with Reinsurance" are bigger (smaller) compared to the "Conventional Model." Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

4.5.3 Impact of Self-protection Measures

In the reference model, we analyzed under which insurance policy setups the risk owner would and would not be willing to invest in insurance. An issue that has not been discussed so far is self-protection, which we identified as one of the central aspects of cyber risk in Section 2.5. Instead of buying insurance, the risk owner could mitigate the risk and cover only the remaining losses by the purchase of insurance. In this section we introduce the opportunity of risk owner investments in self-protection in addition to insurance purchase. For the primary insurer we assume that the measures of self-protection are not observable and cannot be included in the underwriting.[67]

In the following we analyze two cases: (1) the risk owner implements self-protection measures; (2) the risk owner reduces existing self-protection measures.[68] The detailed assumptions are:

- Case (1): the probability of loss occurrence drops from 10% (reference model) to 5% with self-protection. For this reduction the risk owner has expenses of half the expected loss that could occur in the case where no insurance is bought.
- Case (2): if the risk owner reduces existing self-protection, an amount of half the expected loss if no insurance is bought can be saved, but the probability of loss occurrence increases from 10% (reference model) to 20%.

We will evaluate the risk owner's utility under this setup and compare it to the results from the "Conventional Model" in the reference section. From the previous results we can derive hypotheses about the effects we will observe under the new setup. Since the primary insurer is not able to assess the actual status of self-protection for its clients, the following arguments and changes will focus solely on the risk owner's solution set, and by that describe the effect on the whole solution set (overlap). In case (1), if the probability of loss decreases for the risk owner, the willingness to buy insurance with higher deductibles decreases (results from Section 4.4.3). In addition to

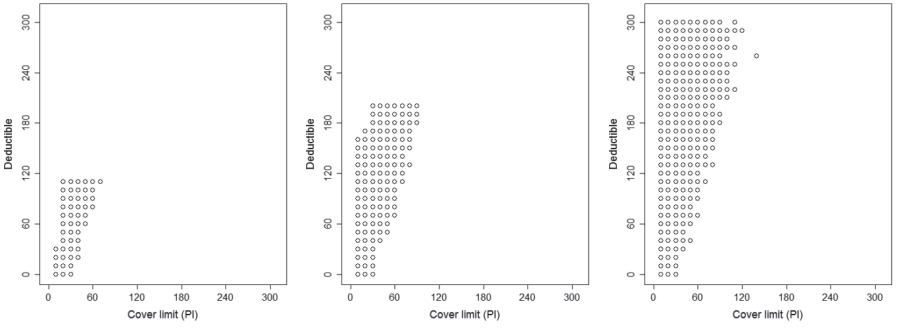
---

[67] In reality, contracts are underwritten individually with up-front risk assessments, which is why the assumption made might be unrealistic. However, the purpose of the analysis is to discuss problems with moral hazard in insuring cyber risks. This motivates the assumption, since the primary insurer does not know what happened after the conclusion of the insurance contract. Thus, even under extensive up-front assessments the whole risk cannot be observed. An approach to mitigate this problem could be the introduction of risk management minimal standards by the government (Section 4.6.2).

[68] For the latter subcase we assume that the reference model presented in Section 4.3.2 already included a particular security standard for mitigation.

the reduction in probability, costs emerge which have to be paid by the risk owner. We observed that a higher fixed cost loading (Section 4.4.3) decreases the willingness to agree on higher deductibles. In addition, insurance contracts with extremely small cover limits for medium-high deductibles will not be accepted either. Thus, we assume that under case (1) there will be a significant decrease in the solution set for the "Conventional Mode." Similar arguments can be made for case (2), under which we hypothesize that the solution sets become bigger. Results are given in Figure 30.

Figure 30 Impact of Self-protection on Insurance Purchase for the Risk Owner – Scenario #1



(a) Self-protection increased (case 1) (b) Reference Model (c) Self-protection decreased (case 2)

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

With self-protection, a part of the stochastic loss is replaced by a deterministic payment (i.e., the expenses for mitigation). Thus, the policyholder is no longer willing to buy insurance for high deductibles (Figure 30(a)). In contrast, the policyholder wants to buy insurance with higher deductibles than in the reference model, if the self-protection measures are reduced. This is because in case (2) a deterministic payment was substituted to a stochastic payment (i.e., a higher exposure). The findings confirm the hypotheses. This simplified approach shows that self-protection has a significant impact on the potential insurance designs that are offered in the market. In addition, it outlines the significant problems primary insurer's face by insuring a risk that exhibits asymmetric information.

4.5.4 Impact of Company Size

The analyses made so far do not incorporate any particular information on the stakeholders except for their loss exposure, their risk aversion, and the contracts they are willing to offer to the other stakeholders. An important feature of all stakeholders should be incorporated into the analysis: the size of the policyholder, or insurance company. This is essential, since extremely small companies might not be able to cover the expected losses under a particular insurance contract design.

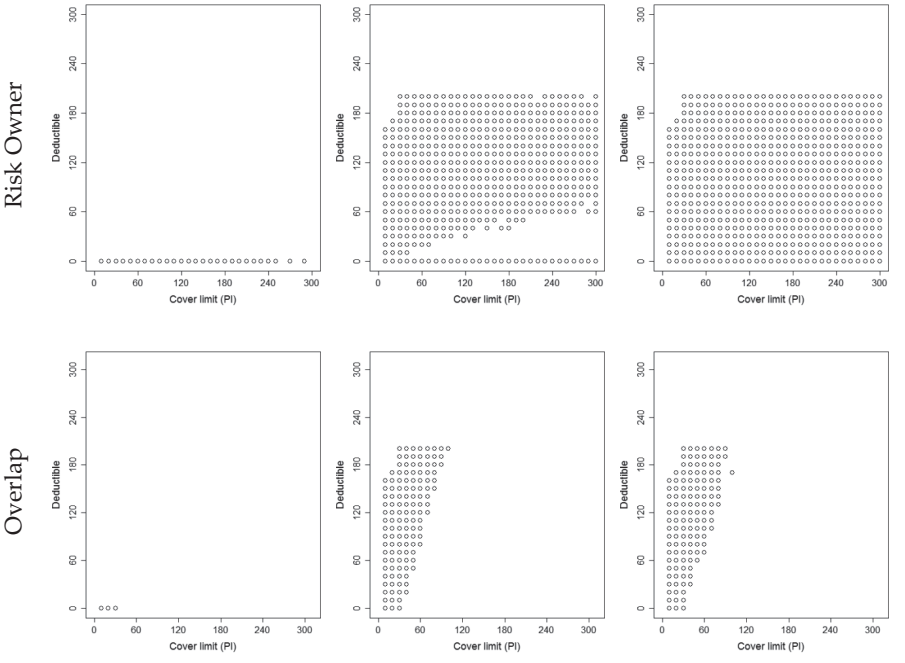
In the reference model, in particular with the definition of the utility function, does not depend on the size of the stakeholders. Therefore, we incorporate a further constraint – besides the utility constraint defined for each stakeholder (Appendix E) – that must be satisfied to qualify as a feasible solution for the respective solution set. We suggest that if the ruin probability of a risk owner for a given insurance contract is higher than a particular level (which we will denote as the target ruin probability (TRP)), the solution cannot be feasible for the stakeholder's solution set.[69] For the implementation we have to define an initial wealth level W_0 (e.g., from the risk owner). Then the condition can be written as

$$\Pr\left[W_0 - X - P + I^{PI}\left(X; C, D\right) < 0\right] \leq TRP,$$

where X is the stochastic loss variable, P the premium charged for the insurance contract, and $I^{PI}(X; C, D)$ is the indemnity payment made by the primary insurer (also Section 4.2.2). If the given constraint is not satisfied for the defined W_0, the particular insurance contract with the indemnity payment of $I^{PI}(X; C, D)$ is not a solution for the risk owner. We define the TRP to be 5%. Furthermore, we analyze the following values for initial wealth: $W_{0, Small} = 3.0$, $W_{0, Medium} = 5.0$, and $W_{0, Large} = 10.0$ (all values measured in million US$). The results for the "Conventional Model" with respect to company size are presented in Figure 31.

[69] Small disadvantage of this approach is that there might be instances under which the initial capital of the risk owner will never be sufficient to provide a ruin probability that is smaller than the TRP. Under such an instance the risk owner would have to buy insurance in any case and under every potential insurance contract. An approach under which the loss distributions and by that the simulated losses can be adjusted by company size can be found in Eling and Wirfs (2016).

Figure 31 Variation of Company Size on Risk Owner Level in the "Conventional Model"



(a) $W_{0,\,Small} = 3.0$ (b) $W_{0,\,Medium} = 5.0$ (c) $W_{0,\,Large} = 10.0$

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

The analyses show that especially for small companies, the solution sets are heavily restricted. This is because contract designs cannot cover as much losses such that the risk owner does not have to face bankruptcy with a 5% probability. The insurance contracts that are least preferable for the risk owner if capital is low are the ones with high deductibles. Well capitalized companies do not face problems in contract restrictions (Figure 31(c)). For a more detailed analysis on the size of the company we refer to Wirfs (2016).

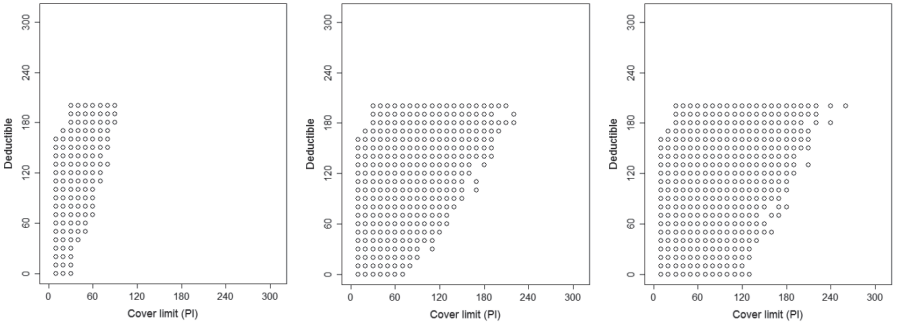
4.6 Ways to Improve Insurability

4.6.1 Impact of a Pool Solution

Under a pool solution, more risks can be aggregated and the benefits of diversification can be exploited. Thus, in the risk pool the portfolio size will be higher than for the individual primary insurers. As observed in the analyses of Section 4.4.2, the increase in portfolio size leads to an increase in the solution set of the "Conventional Model." Moreover, we could assume that the uncertainty loading (which is integrated in the (constant) proportional risk loading) should be lower for the risk pool than for a single insurance company, because diversification effects can be exploited, and experience with the risk, and data availability increase. Therefore, we will also assume a lower uncertainty loading, leading to a further increase in the solution sets, since premiums become less expensive, and thus more insurance contract designs should be attractive to risk owners (Section 4.4.3 or 4.5.2).

The results for the combination of the two model variations are presented in Figure 32. For the analyses presented we chose a size of 200 contracts in the primary insurer's portfolio (i.e., a pool of four exemplary insurers from the reference model), and reduce the constant proportional risk loading from $\lambda^{RO} = 0.5$ to $\lambda^{RO} = 0.3$ (reduction by the additional security loading; see Table 15). In Figure 32 we change the portfolio size first (part (b)) and afterwards adjust the risk loadings (part (c)) to be able to assign the changes in the results to changes made in the model.

Figure 32 Impact of a Pool Solution in the "Conventional Model" in Scenario #1 – Overlap



(a) Reference model (50 policies, $\lambda^{RO} = 0.5$)

(b) Increased portfolio size (200 policies, $\lambda^{RO} = 0.5$)

(c) Decreased loading (200 policies, $\lambda^{RO} = 0.3$)

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

In total, the implementation of a primary insurance risk pool can lead to an increase in the variety of potential cyber insurance policy designs that can be offered. While the effect of the reduced risk loading is relatively small, the increased portfolio size notably increases the solution set. Thus, a pool solution could foster a positive development of the cyber insurance market. A similar analysis can be done for a reinsurance pool, yielding similar results.

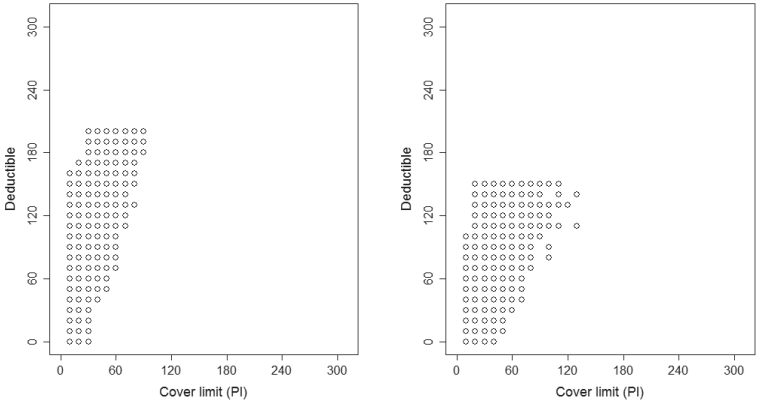
4.6.2 Impact of Governmental Intervention

In this section we discuss how governmental intervention can impact the insurability of cyber risk. We consider the definition of minimal standards for self-protection. Under the model in Section 4.5.3, we analyzed the effect of self-protection on the risk owner's choice to buy insurance products. We assume that legislation defines minimal standards of mitigation, which make a particular level mandatory to implement for the risk owners. The difference in this model from the one in Section 4.5.3 is that the primary insurer is able to identify potential self-protection measures and adjust its underwriting accordingly.

The model we analyze here is thus the same as in Section 4.5.3 only that the probability of loss occurrence is known to the primary insurer. As we saw for the risk owner the solution set decreased with increasing self-protection. The decreased probability of loss occurrence will enable the primary insurer to offer insurance contracts with higher

cover limits, because the aggregated risk in the portfolio declines (results for the loss probability variation in Section 4.4.3). Based on those observations we would hypothesize that with a minimal self-protection standard in place, the solution set will be squeezed downwards (i.e., feasible contracts with high deductibles and low cover limits become unattractive, while contracts with higher cover limits for lower deductibles become feasible). This is the effect that can be observed (see Figure 33 for the results).

Figure 33 Impact of Self-protection Measures in the "Conventional Model"



(a) Reference model

(b) Minimal standards for self-protection in place

Note: Axes are labeled in US$ 1 million; axes: bins of US$ 10 million.

The results in Figure 33 show the hypothesized downward shift of the solution set if self-protection is increased. However, the effect is marginal, and feasible solutions were transferred from high deductible-low cover limit-regions to lower deductible-higher cover limit-regions. We observe the substitutive effects of self-protection and insurance, which were analyzed in literature before. Ehrlich and Becker (1972) show a substitutive relationship between insurance coverage and self-insurance. For the relationship between insurance coverage and self-protection they find that it can be substitutive or complementary. The intuition behind this last result is that the cost of self-protection makes the worst possible outcome even worse while the probability of this state is reduced (also Bryis and Schlesinger, 1990). Therefore, the actual usefulness of this regulatory intervention depends on the costs of implementation. Nevertheless, the introduction of a minimal standard for self-protection could be an interesting instrument to consider for the government to improve national cyber security.

4.7 Key Results of the Expected Utility Analysis

The expected utility analyses presented here are far from complete and more detailed analyses could be generated for several of the approaches. However, this would go beyond the scope in this study. We thus concentrate on the most important aspects of cyber risk. Especially, more robustness tests would be useful, since the parameter assumptions are crucial. In the following we summarize the most important findings from the expected utility analysis:

1) With the given limitations of insurability, the cyber insurance market is relatively small.
2) The introduction of reinsurance contracts and capital market solutions could increase the market size.
3) With respect to worst-case scenarios, the analyzed risk transfer mechanisms are not sufficient to cover the extreme losses.
4) Correlated losses in the insurers' portfolio and the portfolio's size have a significant impact on the available solutions.
5) A precise definition of risk transfer instruments (e.g., the reinsurance contract) is important.
6) The introduction of minimum self-protection standards and the implementation of an insurance pool could be beneficial for the market.

5 Derivation of Implications

A key finding from the previous discussions is that an insurance pool might improve the insurability of cyber risk. Moreover, we have argued that the role of the government needs to be strengthened in order to improve insurability, especially for extreme scenarios. In this section we look into both fields in more detail and discuss potential setups along with their advantages and disadvantages.

5.1 Introduction of an Insurance Pool

In our study we define an insurance pool as a collaboration to create a wider actuarial foundation for particularly high and unbalanced risks (Reichel and Schmeiser, 2015). It is an agreement to underwrite in the name and for the account of all the participants, the insurance of a specific risk category (European Commission, 2014). The discussion in Section 4.3 has illustrated that insurance companies are often only willing to offer coverage in the tens of millions of US dollars, if the risk can be shared with other market participants. The results from Section 4 also emphasize that the insurability of cyber risks can be improved if the risks of the market participants are pooled.

The purpose of an insurance pool is to share unbalanced risks among a larger group of companies or other institutions (policyholders, insurers, reinsurers, government). In most cases insurance pools are a mutual organization of several insurance companies founded for the purpose of insuring a special type of risk (Reichel and Schmeiser, 2015). Examples of such pools can be found for nuclear risks, natural catastrophes, terrorism, aviation or pharma risks. Prominent examples in Switzerland are the Elementarschadenpool (for natural catastrophe risks) or the Schweizer Pool für die Versicherung von Nuklearrisiken (Swiss Pool for the Insurance of Nuclear Risks). In Germany in addition to the nuclear pool (Deutsche Kernreaktor-Versicherungs-gemeinschaft), there arepools for terrorism (Extremus Versicherungs-AG), pharma (Deutsche Pharma-Rückversicherungsgemeinschaft), and aviation (the former Deutscher Luftpool which was disbanded in 2003). Well known are also the coverages for natural catastrophes and terror in the US and the UK (e.g., the Florida Hurricane Catastrophe Fund and the Flood Re for natural catastrophes, TRIA and Pool Re for terrorism). There is considerable variation across the countries over which risks are pooled, reflecting in part the political environment of the countries. For example, in Germany there has been an intense discussion of pooling the risk of flood, but no pool solution has as yet been created. In Switzerland the pooling of earthquake risk has

been a topic of political discussions, but here again there has been no pool solution. The European Commission (2014) has a summary of all pool solutions in Europe.

One major advantage of an insurance pool is the opportunity to accumulate risks of the same type in one portfolio and thereby guarantee a critical size which is needed to benefit from diversification effects. Essential to achieve those benefits is the introduction of a fair sharing mechanism among the pool members (e.g., Fragnelli and Marina, 2003; Ambrosino et al., 2006; or Kraut, 2014). Furthermore, in insurance pools the insurance market's resources, for instance capital, knowledge, and experience, can be bundled and allow the underwriting of heavy risks, something that the single pool member would not be able to do (e.g., Reichel and Schmeiser, 2015).

Table 18 lists the advantages and disadvantages of an insurance pool. 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. From an economic point of view, the introduction of a market pool constitutes a severe intervention into the free markets which can be justified only with the presence of severe market failures in the absence of an intervention. A lack of insurability is an example of the kind of market failure which might justify an intervention.

Table 18 Evaluation for the Insurance Pool

Pro Pool	Contra Pool
• Improvements in data availability (enhanced estimation, smaller risk loadings, lower premiums)	• Limitations in competition
• Improvements in risk diversification (therefore lower premiums)	• Accumulation of cumulative risks
• Improvements in experience by communication (enhanced ratability (estimation), smaller risk loadings, less premiums)	• Less differentiation in the market/less incentives for innovations (in particular, when mandatory participation)
• Better communication and representation of interest (e.g., towards politics)	• Implementation of pool leads to additional expenses (administration, etc.)
• Easier to establish standards (e.g., general terms and conditions, cover modules)	
• Major risks can be made insurable (by an insurance pool)	
• Greater collectives on the primary insurer layer enable reinsurance and thereby fosters the development of the reinsurance market	
• Greater collectives enable scale advantages and efficient management	

One trade-off when implementing an insurance pool is the question of whether a pool increases or reduces the costs of providing insurance coverage. On the one hand, the creation of a pool leads to additional expenses (e.g., administration). On the other hand, the scale advantages made possible by pooling might make pools more desirable. In addition, pooling provides an opportunity for standardization.

Regarding cyber risk, one salient argument is the increase of portfolio size to reduce the uncertainty in the pricing of risks. In this context, we do not argue that an insurance pool must be a permanent solution. Rather one might use the pool for a set period of time (e.g., 10 years) to share data and expertise, and at the end of that period a free market is reintroduced. The decision to stop or to continue the pool can be accompanied by a cost-benefit analysis that analyzes whether or not the benefit of continuing a pool exceeds its cost. Similar ideas have been adopted by the US terrorism insurance pool TRIA. At the beginning of 2015 the program was extended to the end of 2020.

The creation of a pool for cyber risk has already been discussed for the UK. According to a report by Long Finance (2015), three trends necessitate a pooling of cyber risks: (1) the insurance industry lacks the capacity to cover a catastrophic cyber event; (2) the existing cyber coverage will only cover a small portion of losses (e.g., associated with data breaches, network disruption) and by that may leave a significant portion of risks in the economy uninsured; and (3) the UK government is not yet able to back up potentially unlimited liabilities in the event of a catastrophic cyber event which could threaten the whole country's economy. Hence, they suggest a public-private partnership, where 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). Our analysis in Section 4 can be used to justify such a pool solution.

Another open question is the organization of the pool. For instance, on what level should the pool be implemented? As discussed in Section 3, a pool can be implemented at the level of the risk owner in the form of a private or an industry-wide risk pool. In addition, primary insurers and reinsurers can pool their business with other primary insurer/reinsures in ad-hoc co-insurance agreements or co-insurance pools. Under private risk pools only a few risk owners collaborate to cover each other's losses. The risk-taking capacity that can be generated under this approach might suffice for the "cyber risks of daily life"; however, for loss coverage of catastrophic cyber events this

might be inappropriate. In addition, cyber risks exhibit close correlations between incidents (Bear and Parkinson, 2007), meaning that small pools might be even inappropriate for correlated "cyber risks of daily life" (e.g., a DoS). The problem of high correlation might also apply to the industry-wide risk pool, since firms in a single industry might be even more closely linked than firms that are not operating together. Nevertheless, the capacity of the industry-wide risk pool would be much bigger, and thus coverage for catastrophic cyber events might be given. Risk pooling solutions on the primary insurance and reinsurance level seem to be most appropriate. The coverage capacity for catastrophic events will be given and the aggregation of data and expertise might be most beneficial. The initial results can be observed in the analyses of Section 4.

In addition, participation in a pool solution can be voluntary or mandatory. The latter setup can be found in combination with governmental interventions, for instance in the Danish Terror Pool (European Commission, 2014). The German nuclear pool (Deutsche Kernreaktor-Versicherungsgemeinschaft) is a voluntary setup. The advantage of making a pool solution mandatory is that the capacity increases. A significant disadvantage is that the limitations in competition and the argument made about less incentives for innovations (Table 18) might carry more weight for the mandatory solution. A final decision, however, cannot be made.

A third parameter to be discussed is the extent of collaboration. This does not only define the way a pool solution is constructed (e.g., ad-hoc co-insurance agreement vs. co-insurance pool; see differentiation in Section 3.2), but also the way in which premiums and costs are measured, how contributions to the pool are defined. Interesting details on that topic can be extracted from Fragnelli and Marina (2003), Ambrosino et al. (2006), and Kraut (2014).

A further dimension according to which pools can be distinguished is the liability regime, which defines how pool claims should be shared if pool members become insolvent and cannot indemnify their shares. Reichel and Schmeiser (2015) discuss two approaches: (1) the "regime of joint liability" where all insurance pool members provide a guarantee to the policyholder that the solvent pool insurers will jointly indemnify the share of the bankrupt co-insurer; (2) the "regime of several liability" the pool insurers agree that their single liability is limited to their own share, and thus no guarantee to the policyholder can be given for the indemnification of bankrupt co-insurer's shares. The analyses in Reichel and Schmeiser (2015) show that premiums are higher under the regime of joint liability in a two-insurer pool solution setup,

because of the implicitly lower insolvency costs for the policyholder. Furthermore, if the expected insolvency costs are fixed (e.g., by regulation) the regime of joint liability makes lower equity by insurers necessary.

Finally, and this is closely related to the question of costs in the pool, is the way of establishing a pool from an existing scheme as extension (e.g., in terrorism, natural catastrophes) or creating a new scheme. The extension of an existent pool solution might have the following advantages over the creation of a new scheme: (1) there are already a relevant number of members from the insurance industry; (2) a critical reserve is already in place, and thus might not be that extensive for the government to set up; (3) the pool has already experience in (re-)insuring against a critical risk category (e.g., terrorism, natural catastrophes), which is especially important for the management of financial reserves on a large scale; and (4) is known in the market as credible partner and can benefit from this reputation if ILS should be issued. In addition, under some pooling schemes (mainly for terrorism, see Long Finance, 2015) portions of cyber risk are already covered. This can be because no exclusions have been made (e.g., in the French GAREAT [Gestion de l'assurance et de la Réassurance des Risques Attentats et Actes de Terrorisme] and CCR [Caisse Centrale de Réassurance]). Furthermore, it can be due to explicit coverage regulations included in the pool agreement. Examples of the latter are TRIA in the US, under which cyber risk coverage by the pool is included if coverage is included in the individual contract, or the UK's Pool Re scheme that excludes only computer hacking, virus, and denial of services (Long Finance, 2015). In a nutshell, the extension of an existent terrorism pool solution could be preferable to the creation of a new scheme, for the above reasons. We therefore propose a pool solution only as a temporary expedient to encourage the development of the cyber insurance market.

5.2 Improving the Role of the Government

The government has an interest to ensure the insurability of cyber risks in order to protect the economy from harmful scenarios which endanger economic well-being. In the following we discuss prerequisites for governmental intervention and apply those criteria to cyber risk. According to Klein (2013), the economic rationale for regulatory intervention in markets is based on the concept of market failure, which leads to inefficiencies in the economy. Economic theory has identified the following major types of market failure (Labonte, 2010), which we can apply to cyber risk:

The state has to provide public goods. These goods or services are characterized by "free-rider problems," meaning that special customer groups cannot be excluded from their use ("non-excludable") and the use by one person does not affect the use by another ("non-rival"). Because of these free-rider problems, private producers have no incentive to supply the good or service. According to economic theory, government should step in and provide goods and services to make up the shortage. Cyber security could thus be seen as a public good. This discussion can be analogous for national defense and infrastructure, which are good examples of public goods. Because of the increasing interconnectedness, firms can be attacked through backdoors in other companies that were not adequately secured. A private company investing in its security system will then contribute to a more secure global system for all, but will still face significant risk because other companies might have not invested. Discussions of cyber security as a public good have already appeared in the literature (e.g., Asllani, White, and Ettkin, 2013). Therefore, there might be a strong case to be made for government intervention in cyber security regulation (e.g., in the form of setting the adequate framework for risk management standards).

Economic theory assumes that all benefits and costs that are connected with the production of good or a service come at the expense of the producer or the consumer of that product. If a third party benefits from the production of a good (although it is not the consumer of the good) we call those benefits "positive externalities" (e.g., vaccine). If a third party has to bear costs for the production we speak about "negative externalities" (e.g., pollution). Cyber security is seen as a public good with positive externalities (Baer and Parkinson, 2007). If one company adopts cyber security measures, the entire community benefits, since infections going out of this company are minimized. However, the utility of cyber security investments by one firm depends on the cyber security investment made by all other firms. Without government intervention, cyber security might not reach a market-efficient level. The characteristic

of cyber security as a public good with positive externalities might thus be used as another argument in favor of setting risk management standards.

Monopoly power is another market failure under which the state should engage in the market. Under economic theory, perfect competition leads to economically efficient outcomes, because no producer has enough market power to push prices above marginal costs. If no competition is present in the market, one or more producers can push prices up by reducing their production to an economically inefficient level. Monopolies can occur for many reasons, but entry barriers might be one of the most important. The market for cyber insurance is still relatively small and only a few insurers provide coverage to policyholders. In addition, only a few reinsurers provide coverage to primary insurers (see the results from Section 2.3). One could argue that perfect competition is not possible yet, and that it would require governmental involvement, for instance, by subsidizing insurers to enter the cyber insurance market. Furthermore, active involvement such as a governmental backstop could entice insurers to enter the market. However, the cyber insurance market is predicted to increase significantly and more companies are expected to enter the market without government intervention. Thus, we believe that monopoly power is not a justification for the state to engage in the cyber risk (insurance) market.

Another market failure discussed in Labonte (2010) is asymmetric information. Economic theory assumes that markets work only efficiently when both – buyer and seller of products – have the same information when entering the contract. According to Klein (2013) asymmetric information is the most commonly found market failure for insurance markets, since policyholders (in general) know more about their exposure than the insurance company does. Asymmetric information could always be a good reason for the state's active participation in insurance markets. The main problems with asymmetric information are moral hazard and adverse selection. These two problems are also particular challenges to the insurability of cyber risk and cyber insurance (see the discussions in Section 2.4). There are several instruments for government intervention to prevent those problems.[70]

[70] Labonte (2010) describes two additional market failures: common resources, and failure to optimize. We believe that those are not very important to the discussion, which is why we only focus on the ones mentioned above. Common resources are goods that cannot be provided by the private market and for which governmental control and regulation is necessary to maintain an efficient and sustainable use of the good (e.g., environment, ocean fishing, or water supplies). The failure to optimize relates to the assumption in economic theory that people behave rationally and maximize their well-being.

This discussion shows that some of the market failure arguments that motivate government intervention can be well applied to cyber risk. Those arguments could thus justify a more dominant role of the state in cyber risk on economic grounds. According to Klein (2013), the markets could also provide outcomes that are not results of market failures but which are not desirable for consumers and regulators either. In those cases government intervention in insurance markets could be requested. Intervention is specifically required when the insurability of certain risks pose massive problems to the industry (Klein, 2013), for instance, in cases when coverage is too expensive because potential claims are too high, or when insurers are not willing to offer insurance because of severe adverse selection or moral hazard problems, or correlated risk exposures. All these problems are present in cyber risk and were identified as impediments to the cyber insurance market (Section 2.4). Furthermore, these arguments also apply to extreme risks, such as terrorism, natural catastrophes, or the risk of nuclear accidents that government had previously supported. These extreme risks have some common characteristics with cyber risk (see e.g., the comparisons in Table 3). Klein (2013) thus provides additional support for governmental intervention in cyber risk and cyber insurance markets.

In the following we discuss potential ways for the state to enter the cyber risk and cyber insurance market. As discussed in Section 3.5, the government has several ways to intervene in the risk transfer market. First of all, there are "direct"/"explicit" options, where the state takes over actual insurance functions and covers risks itself ("State as Primary Insurer" and "Reinsurer of Last Resort"). Another mechanism by which government can directly influence the cyber risk market is the "Lender of Last Resort." Under this approach the government makes loans to insurance companies who are in need of liquidity, after an extreme event from a particular risk (OECD, 2005). Private (re-)insurers may not be willing to write specific risks since they fear financial distress in case of extreme risks if they cannot access enough recourses to pay future claims. Thus, this approach can vitalize the market for cyber insurance for a relatively low cost – at least ex ante – for the government (OECD, 2005).

Furthermore, there is the "indirect"/"implicit" approach which government can apply to revitalize the private market. The definition of policy measures to set specific incentives for a restart in private insurance markets (or even alternative non-insurance markets) should be the goal of this approach (OECD, 2005). Potential measures could be the facilitation of capital raising and reserving for these particular risk coverages in insurance firms. These instruments can be fiscal, accounting and regulatory. In addition, incentives (fiscal or regulatory) could be defined to incentivize the purchase

of particular coverage (e.g., compulsory insurance, Third Pillar in the pension system in Switzerland and Germany). Furthermore, the definition of regulatory measures to promote the development of alternative risk transfer mechanisms (e.g., ILS) could be beneficial under this indirect approach.[71] Lastly, the building of private capacity and larger mutuality could be encouraged (OECD, 2005).[72]

Since indirect forms of governmental intervention cannot provide actual coverage for some risk categories it might be useful only as a complement to the direct approaches discussed and not as a single approach in use (OECD, 2005). Further potential disadvantages compared to the direct approach can be that they might not be sufficient to avoid rising risk premiums, since crucial issues of risk ambiguity and generalized uncertainty, which are present in most of these risks, are not addressed. Moreover, it might be expensive for the government (e.g., tax incentives), and extreme risks might still be not covered by the private insurance market solutions in place.

The list of potential measures and potential solutions for cyber risk is presented in Table 19. Rather than discussing each intervention in detail, we will focus on the top five activities in the next section and combine this with the idea of an insurance pool in Section 5.1.

[71] An example would be the definition of a tax-free conduit status for SPV of cat bonds, which would reduce transaction costs, since most SPVs are located in off-shore tax-havens and not in the countries the sponsors are headquartered.

[72] For instance, fax-free status for private sector risk-mutualization approaches, as discussed previously.

Table 19 Measures of Governmental Intervention

Measure	Example
"Direct"/"Explicit" Governmental Intervention	
State as a Primary Insurer	• As in the form of the Swiss old-age and survivors' insurance
Reinsurer of Last Resort	• Coverage of particular major risks • As in the form of the Terror Risk Insurance Act (TRIA) in the US or Pool Re in the UK
Lender of Last Resort	• Providing liquidity to (re-)insurers that are in need, after a catastrophic cyber event, similar to the central banking principle
"Indirect"/"Implicit" Governmental Intervention – In General	
Incentivize purchase of insurance coverage	• Compulsory insurance, Third Pillar in the pension system in Switzerland and Germany • Tax refunds
Set incentives for self-protection/self-insurance	• Provide subsidies to firms based on security spending • Establish requirements of disclosure of self-protection security efforts by all firms
Set incentives to provide insurance coverage	• Imposition of a "sales" tax on insurance premiums • Facilitation of capital raising and reserving
Subsidize the introduction of capital market solutions (e.g., ILS)	• Definition of a tax-free conduit status for SPV of cyber cat bonds
Intensification of penalties	• In case of misbehavior, e.g., tougher penalties for data breaches • For cybercrime, e.g., tougher penalties for hacking delicts
Establishment of an insurance pool	• Potentially as an extension of an existent (mandatory) terrorism pool solution (e.g., TRIA); more details in Section 5.1.
"Indirect"/"Implicit" Governmental Intervention – Cyber-specific	
Set up an anonymized data pool	• By providing a common platform for data sharing; rate advisory organizations (e.g., Insurance Services Organization in the US) could be starting templates • Encourage private sector resource combining and exchange of data as it is done for operational risks in the banking industry • Establish a Think Tank for cyber risk with the respective stakeholders
Establishment/intensification of reporting obligations	• Already in discussions in the European Union, and in place in the US.
Improvements in standards for data protection	• New laws for data protection, as e.g., currently discussed in the European Union
Establishment of national standards (minimal standards) for cyber risk	• Cyber risk management: national IT security standards already exist (e.g., ISO/IEC 2700x – Information technology-security techniques, BSI-IT-Grundschutz, Control Objectives for Information and Related Technology (COBIT)); direct investments into infrastructure for companies • Strategies for digitalization (infrastructure of the state)

5.3 Top Five Measures to Improve the Insurability of Cyber Risk

All the measures presented in Table 19 are possible means of governmental intervention. However, some of them might be more appropriate for implementation than others in case of cyber risks. In the following we discuss a selection of those measures that we think might be appropriate for cyber risk and that merit deeper discussion with the stakeholders. We do not postulate that each of the five measures must be implemented since still each activity has its advantages and disadvantages. We believe, however, that those five topics might be fruitful for a deeper discussion among stakeholders (such as politicians, regulators, the industry and customers). A summary of these measures is given in Table 20.

Table 20 Top Five Measures

1. Incentivize the development of an anonymized data pool
2. Minimal standards for risk mitigation
3. Introduce reporting obligations
4. Incentivize the development of "traditional" risk transfer mechanisms
5. Establish a governmental backstop for extreme scenarios

First of all, we believe that setting up an anonymized data pool is the easiest way to intervene in the insurance market and that promises the highest benefit in the coming years. Common knowledge can be easily collected, standards could be more easily established, and – most important – data can be collected. The implementation will thus reduce uncertainties with respect to data (lack of data) and with respect to modeling approaches. The implementation of a data pool can easily be connected with the creation of an insurance pool. This approach could resolve the problems with relatively small insurance portfolios and diversification issues.[73] Clearly, this intervention could be developed as a public private partnership that is the industry can self-create and manage the data pool. But before setting up the data pool, the government has to set the legal framework, especially regarding competitive law.

The second measure we would discuss with the stakeholders is the definition of minimal standards for risk mitigation. Minimal standards for risk mitigation will reduce incentives for moral hazard, which is one of the main properties of cyber risk

[73] A mandatory pool solution often is also used in the context of cross-subsidization. For example, for insurance companies to write business in Florida they have to participate in the pooling of natural catastrophes. While insurance for natural catastrophes is an unprofitable activity, other types of insurance might be profitable so that a cross-subsidization exists.

(Section 2.5) and an essential impediment to cyber risk's insurability. Furthermore, it might help to provide a minimal level of security which then reduces contagion, and by that mitigates problems with dependence of losses. Furthermore, a regulatory intervention like this could be easily justified on economic grounds (cyber security as a public good with positive externalities).

Thirdly, we believe that reporting obligations could be easily implemented and be beneficial for the future development of the cyber insurance market. A significant 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. These regulatory approaches have significantly enhanced the sensitivity for problems with cyber. Reporting obligations in the European Union are already under discussion and given the economic importance of cyber risk we believe that such a discussion is useful.

The subsidization of traditional risk transfer mechanisms could also be interesting for a governmental intervention measure. Without inventing directly, the government might provide incentives for private risk transfer mechanisms. One example could be to support the private insurance industry with the implementation of an insurance pool (Section 5.1). The government could motivate the industry to set up an insurance pool for a limited time period or for selected aspects of cyber risk, such as extreme scenarios. Furthermore, the state could incentivize the introduction of capital market solutions by the definition of a tax-free conduit status for SPV of cyber cat bonds. The reinsurance industry could be subsidized by the facilitation of capital raising and reserving requirements for the coverage of cyber reinsurance. Again, we emphasize that we do not postulate that all the measures shall be implemented, but they might be fruitful directions for discussions between the stakeholders to improve the insurability of cyber risks.

All measures discussed so far are from the "indirect"/"implicit" category of governmental intervention. The current market is emerging and increasing, which is why we do not believe that there is any need for active governmental intervention at this stage. Only if no private market risk transfer solutions develop or if we observe a failure in private insurance markets (as for other risk categories such as natural catastrophe, terrorism, or nuclear accidents) governmental intervention could be needed. If the state has to intervene in the risk transfer market, a governmental backstop solution (i.e., a Reinsurer of Last Resort like the TRIA program in the US)

could catalyze the lagging development in the market. This could also be interesting as an instrument to incentivize the development of "traditional" risk transfer mechanisms.

6 Survey among Market Participants

In this section we present the results of our survey of market participants on the feasibility of risk transfer solutions. The purpose of this evaluation is to test the findings and results provided in the previous sections from a practitioner's perspective. Therefore, we constructed a survey of potential stakeholders in the cyber risk and cyber insurance market. The next paragraphs give a detailed summary of the data collection and the results.

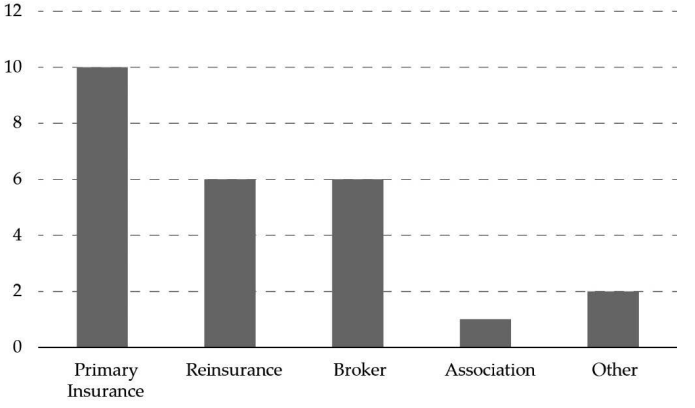
6.1 Data Collection and Descriptive Statistics

In January 2016, we sent an online questionnaire (Appendix F) by email to primary insurers, reinsurers, brokers, governmental/regulatory institutions and insurance associations. We targeted members in all these groups which work and have experience with cyber risk and/or cyber insurance. This is why the selected group was so small. All answers and statements were treated as strictly confidential and anonymous.

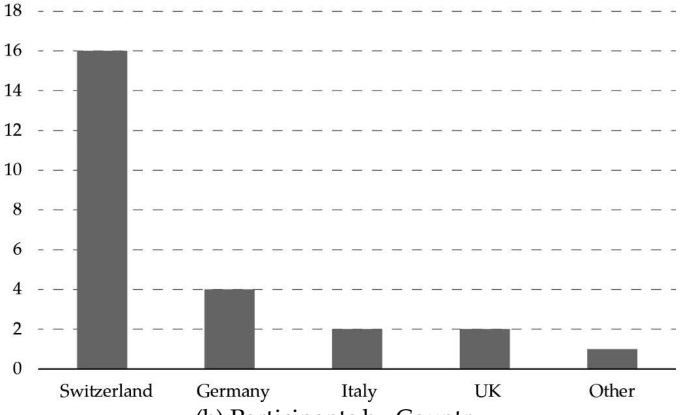
The questionnaire was divided into three parts: (a) descriptive information about the respondent; (b) questions about the status quo of cyber risk and the cyber insurance market; and (c) evaluations about how the insurability of cyber risk can be improved. The third part was connected with the evaluation of potential risk transfer options and their feasibility for cyber risk. The results presented here are from mid-February 2016, and consist of 25 observations. In the presentation of the results, we follow the tripartite setup of the questionnaire.

The sample (Figure 34(a)) consists of participants from the insurance industry: primary insurers (10 participants) and reinsurers (6 participants). Furthermore, there are six answers from broker companies, one from an insurance association member, and two from the "Other" category (excess insurance and engineering). With respect to regional distribution (Figure 34(b)), we have four respondents from Germany, two from Italy, 16 from Switzerland, two from the UK, and one did not answer this question. For the evaluation of expertise, most of the participants work with cyber risk in their job daily (15) or regularly (7). Only three participants reported that their work is seldom connected to cyber risk (Figure 34(c)).

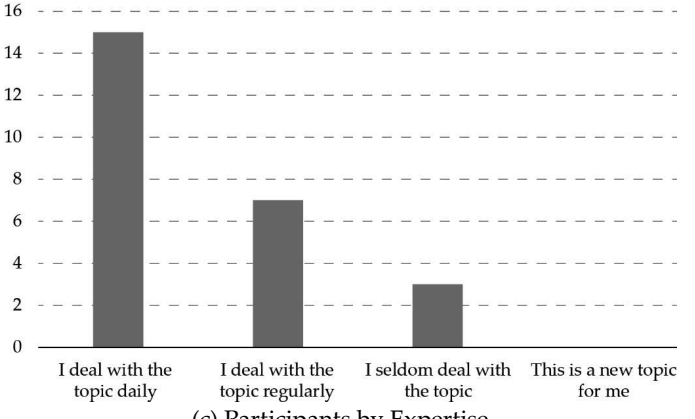
Figure 34 Distribution of Survey Participants



(a) Participants by Field



(b) Participants by Country

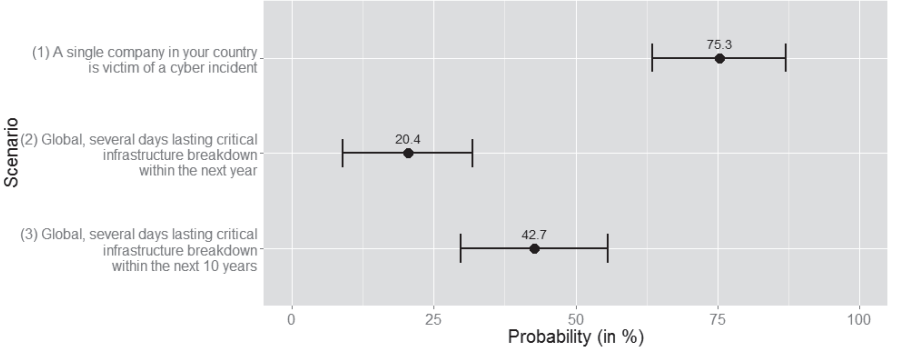


(c) Participants by Expertise

6.2 Cyber Risk and Cyber Insurance: Where do we stand?

The first block of questions in the survey is connected to the status quo for cyber risk and the cyber insurance market. The first question was how participants would estimate the probability of occurrence for three scenarios. The average probability estimates (with their 95% confidence estimates) are given in Figure 35.

Figure 35 Average Probability Estimates for the Scenario Analysis

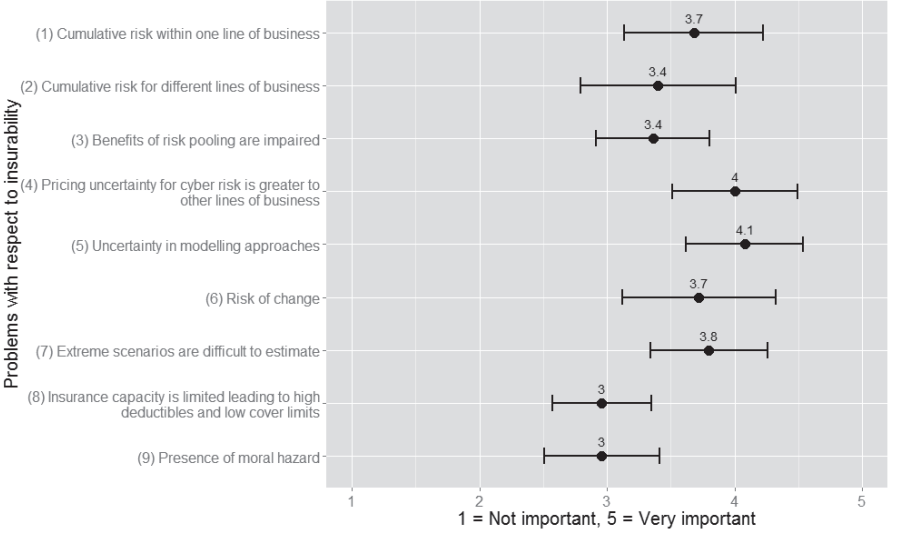


Note: presented in this graph are the average probabilities (dots) and estimates for the 95%-confidence intervals.

All scenarios are estimated with relatively high average estimates. The scenario of a global breakdown of critical infrastructure lasting several days within the next year (scenario 2) is estimated with an average of about 20%. This is very high, considering that first estimates on this scenario by the WEF (2010) for a 10-year period (as in scenario 3) was estimated at only 10-20%. For the same scenario as in WEF (2010) we receive a probability of about 43%, which is more than twice as high as that given six years ago in WEF (2010). These results indicate the increased importance and higher awareness of market participants for cyber risk in the last years. However, it also indicates their awareness of high-severity events and the increasing fragility of the critical infrastructure. The estimate of a single company's probability to become victim of a cyber incident (e.g., data breach, extortion) in the following year is placed at about 75%. Thus, the participants predict that three out of four companies in their country will have to face a cyber incident in the next year, confirming the results of other empirical studies (e.g., according to the Cyber Security Report 2014, more than 92% of all companies in Germany were subject to hacking attacks in 2014; see, T-Systems, 2014).

The second part of the status quo analysis is concerned with problems in the insurability of cyber risk and how the participants evaluate those problems (Figure 36).

Figure 36 Evaluation of Specific Problems for the Insurability of Cyber Risk



Note: presented in this graph are the average probabilities (dots) and estimates for the 95%-confidence intervals.

Almost all of the problems at choice are important for the insurability of cyber risk, as we have seen in the previous listings. The uncertainty in modeling approaches and pricing uncertainty connected to cyber risk compared to other lines of business (LoB) were evaluated to be most important (average scores of 4.1 and 4.0). In addition, the participants see the ability to estimate extreme scenarios (average of 3.8), the cumulative risk within one line of business and the risk of change (both with an average of 3.7) as the second most problematic issue connected with cyber risk. The cumulative risk for different LoB (average of 3.4) that are inherent in cyber risk seem to be less important for the participants than the previous problems. However, in the subsequent discussion it became clear that the participants expect this challenge to become more problematic in the future. For instance, with the introduction of the Internet-of-Things (IoT), the cyber component will add to traditional insurance products. Because of the increased interconnectedness in IoT and the extended use of cloud solutions, problems with potential accumulation losses might be exacerbated (in one as well as across different LoB). With the same score, the participants name the impaired benefits of risk pooling (i.e., that insurers might not be diversified enough to

be able to maintain a portfolio). Presence of moral hazard and the limited insurance capacity that leads to high deductibles and low cover limits (both an average of about 3.0) seem least important for insurability. This finding is interesting, since it was identified as one of the main three problems in the academic considerations of cyber risk's insurability by Biener, Eling, and Wirfs (2015). In the empirical analyses of Section 4 we also observed significant influences of cover limits on cyber insurance contracts.

> *"Internet of things will add the cyber component to traditional insurance products."*
> and
> *"The nature of the risk is constantly changing, new threats, greater systemic consequences as a result of IoT and cloud computing."*
>
> Feedback from two experts in the market survey

An additional problem mentioned by the respondents is a lack of understanding of coverage on all sides (i.e., policyholders, brokers, and insurers). The lack of clarity in contracts about several consequences, for instance damage and business interruption and reputational losses are impediments to insurability. In addition, risk of legal change was not mentioned in our questionnaire and seemed to be relevant for the participants (e.g., privacy liability issues). Apparently, it is important to make distinctions among policyholders. While for large companies it might be easy to implement indicators to measure cyber security and its breaches, a big challenge is to offer insurance to small- and medium-sized businesses (SMB). Those companies might need insurance because they might not be able to mitigate the risk themselves. An interesting point that one participant raised is closely related to the risk of change. Cyber risk faces the risk that desirable portfolios can change drastically and very quickly to a portfolio that might not be wanted. For instance, a previously unknown security loophole could necessitate reassessments of the portfolio and trigger substantial adjustments in reserves.

> *"There is a lack of understanding coverage on all sides (i.e., policyholders, brokers, and insurers alike)."*
>
> Feedback from an expert in the market survey

6.3 Ways to Improve Insurability of Cyber Risk

In the final part of the survey we tested the appropriateness and feasibility of different risk transfer options for the application in cyber risk. We evaluated which mechanisms would best improve the insurability of cyber risk. As before, we asked an open question about the biggest levers to improve the insurability first; in our previous study, we asked for an in-depth evaluation for particular instruments. Means to improve insurability mentioned by the participants are given in Table 21.

Table 21 Means to Improve Insurability given by Participants

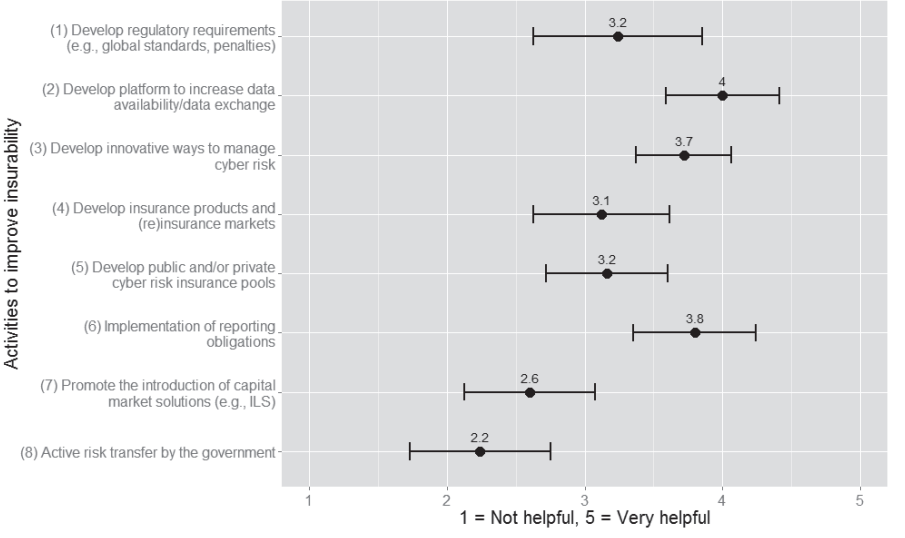
Instrument	Explanation
Exchange and Sharing opportunities	Data, loss information, and experience should be made available to all stakeholders, to increase transparency and get a better understanding for the actual risk.
Simplification and standardizations	• Requested for the insurance purchase process. This includes the standardization of coverage, and increased transparency about services included in the coverage, and limits on the coverage. • Participant also recommend the establishment of best practice standards for proper risk assessment (e.g., mandatory external audits for highly exposed companies, or minimum security standards set by the policymakers).
Develop understanding for customers' needs	• An open dialogue among insurance companies, brokers and clients is requested to evaluate the appropriate protection needs. Discussions about the future loss development and a geographical separation must be incorporated. For instance, in Europe protection against business interruption, extortion, and fraud is important, and not necessarily liability and notification costs that are primary drivers in the US. For Germany, respondents mention that there are less third-party claims following a cyber attack due to less strict legislation, compared to the US. • If customers' needs are understood, the current insurance contracts need to be adjusted. According to a participant, brokers in Switzerland tend to recommend high limits from one carrier, whereas in more mature markets (as e.g., in the UK) layer structures or co-insurance structures are offered that might suit the customer's needs better.
Increase importance of cyber related topics on the C-level	According to the participants, the company boards have a low culture for cyber related topics. In addition, the role of the CISO in Europe is not prominent enough yet, and those positions are not enough involved in the cyber insurance buying processes.
Reinsurance support	Adequate reinsurance support (in particular, for the coverage of cumulative risks) is requested.
Reporting obligations	Reporting obligations as installed in the US are seen to be a good measure to improve insurability

"Reporting obligation for cyber incidents like in the US would be a plus."

Feedback from an expert in the market survey

These instruments were already very close to the activities mentioned in the study. For some of them we wanted to evaluate their feasibility (how helpful they might be to improve insurability), and asked for a rating from the survey participants. A summary of this question's result can be found in Figure 37.

Figure 37 Evaluation of Particular Activities to Improve Insurability



Note: presented in this graph are the average probabilities (dots) and estimates for the 95%-confidence intervals.

The most important activities to improve the insurability of cyber risks are the development of data exchange platforms (average of 4.0), the implementation of reporting obligations (average of 3.8), and the development of innovative ways to manage cyber risk (average of 3.7). The instruments that are seen to be least helpful for the participants are active risk transfer by the government (e.g., "State as Primary Insurer" or "Reinsurer of Last Resort," average of 2.2) and the introduction of capital market solutions (e.g., ILS; average of 2.6). These findings are interesting since they indicate that market participants are confident that cyber risk can be handled by the general risk transfer structures, and governmental intervention (and securitization) is not necessary. Instruments that were assessed to be moderately helpful are the development of public/private cyber insurance pools (average of 3.2), the development

of regulatory standards (e.g., global standards, penalties; average of 3.2) and the development of insurance products and (re-)insurance markets (average of 3.1). In the subsequent discussion of the evaluations, other instruments were named. For instance, the inclusion of additional services provided directly by the insurer (e.g., forensic investigations, or crisis management) could be interesting.

"Why should the state bear the risk (as primary insurer) of private companies which make money out of the use of (client) data? If at all, similar to a TRIPRA [Terrorism Risk Insurance Program Reauthorization Act; law to extend the TRIA program in 2015] in US as a backstop [would be a] suitable solution."

Feedback from an expert in the market survey

6.4 Summary of Key Results

The main findings of our market survey are summarized as follows:

1. Participants' estimated probabilities for worst-case scenarios are relatively high (42.7% likelihood for a breakdown of the critical infrastructure in the next ten years).
2. They predict that three out of four companies in their country to become victim of a cyber incident in the next year.
3. Pricing and modeling uncertainty are the main impediments to the insurability of cyber risk.
4. Platforms for data exchange, the implementation of reporting obligations, and the development of innovative ways to manage cyber risk are seen as the best instruments to improve insurability.
5. Active risk transfer by the government and the promotion of capital market solution for cyber risks seems to be less attractive. The introduction of a backstop solution by the state is still preferable to governmental intervention in the form of a "State as Primary Insurer."

7 Conclusion

Our results show that cyber risks "of daily life" are insurable by mechanisms in the private insurance market. However, today's markets are still undeveloped and could benefit from improvements in insurability. We recommend a broader use of risk transfer mechanisms especially in the reinsurance and alternative risk transfer field. The implementation of an insurance pool might also be an option to promote the market development. Even if temporarily implemented, a pool can help to generate common knowledge, improve the establishment of standards, and enhance diversification. However, there might be concerns with such an extreme market intervention both in the industry and with competition authorities. We thus recommend limiting such a pool at least in a first step to an anonymized data pool which is accessible to the whole industry. Furthermore, certain product standards (e.g., for cover limits or risk assessments) and a coherent terminology of cyber risk and cyber insurance should be defined.

In contrast to the insurability of cyber risks "of daily life," the insurance of "extreme scenarios" like a breakdown of the critical infrastructure seems problematic. Main impediments are essential problems in the insurability, meaning the lack of data or large cumulative risks. We recommend the integration of the government to enhance the insurability of extreme scenarios. The introduction of an anonymized data pool, the establishment of minimal standards for self-protection, and reporting obligations for cyber incidents might be the easiest and most fruitful instruments to install. It is important to mention that all these measures would also enhance insurability in "daily life" cyber risks. For instance, the reporting requirements implemented in the US massively increased the awareness for cyber risk and this might explain why the US cyber insurance market is more developed than the European market.

A positive development of the cyber insurance market can thus also be triggered by new regulation. Moreover, government and the industry should start a dialogue about strategies for the treatment of extreme scenarios, since those events are not unlikely to materialize in the next ten years. In particular, the government should consider insurability within its national security strategies to defend against the increasingly important cyber threats. All these findings are supported both by the results from the theoretical analysis and by the practitioners' feedback from our market survey.

For the future development of the cyber insurance market we can thus conclude with a positive outlook. With ongoing market development, risk pools will increase and

more observations than ever will be available. Also a number of new competitors currently enter the market or plan to do so. Estimates about the cyber insurance market predict a global market growth to about US$ 7.5 billion by 2020 (PwC, 2015a) and US$ 20 billion by 2025 (AGCS, 2015).[74] Thus, availability and competition will increase and prices might decrease. In our opinion, many aspects of today's cyber risk market reflect the development of the D&O insurance a few years ago. At the beginning of its development, D&O insurance was characterized by similar problems of insurability such as a lack of data or no standardized coverage. But by now, D&O insurance is a standardized commodity-product in the commercial insurance business and represents its own line of business in most insurance companies. In 10 or 15 years this might also be the case for cyber risk.

Cyber risk has become more important than ever both in academia and in practice. The industry should not only discuss cyber risk management at the level of the individual company, but also on a broader basis. We believe a national and international discussion of cyber topics is necessary for the economy and society. The construction of think tanks with representatives from IT and insurance industries, the government, and the academic domain could be an option. Cyber risk is a significant field for future research in the academic literature. One example is the modeling of cyber losses and cyber insurance. Another important question is whether or not solvency requirements (e.g., Solvency II, or the Swiss Solvency Test) are adequate for cyber risks. Furthermore, the development of innovative risk management solutions could be an interesting task for the interdisciplinary research teams. And certainly the dynamic technology development (e.g., Internet-of-Things) and the dynamic nature of cyber risks will open manifold new challenges for academics and practitioners.

[74] Predictions about the global cyber market premium volume for 2025 by Swiss Re (2015) range between US$ 12 billion to US$ 18 billion (up to US$ 8 billion in the US and up to US$ 18 billion in the rest of the world).

References

Ackerman, G. (2013): G-20 Urged to Treat Cyber-Attacks as Threat to Economy. http://www.bloomberg.com/news/articles/2013-06-13/g-20-urged-to-treat-cyber-attacks-as-threat-to-economy. Last accessed: March 16, 2015.

Advisen (2015): Cyber Risk Insights Conference, February 10th, 2015 in London. http://www.advisenltd.com/wp-content/uploads/london-cyber-risk-insights-conference-slides-2015-02-17.pdf. Last accessed: September 30, 2015.

Allianz Global Corporate & Specialties (AGCS) (2010): Introduction to D&O insurance – Risk briefing. http://www.agcs.allianz.com/assets/PDFs/risk%20insights/AGCS-DO-infopaper.pdf. Last accessed: November 14, 2015.

Allianz Global Corporate & Specialties (AGCS) (2015): A Guide to Cyber Risk – Managing the Impact of Increasing Interconnectivity. http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf. Last accessed: November 25, 2015.

Ambrosino, D., Fragnelli, V., and Marina, M. E. (2006): Resolving an insurance allocation problem – a procedural approach, Social Choice and Welfare 26(30), 625-643.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., and Savage, S. (2013): Measuring the Cost of Cybercrime, in: Rainer Böhme (ed.), The Economics of Information Security and Privacy (Springer), Chapter 12, pp. 265-300.

Aon Benfield (2014): Insurance Risk Study – Growth, profitability, and opportunity, Ninth edition 2014. http://thoughtleadership.aonbenfield.com/documents/20140912_ab_analytics_insurance_risk_study.pdf. Last accessed: November 27, 2015.

Aon Benfield (2015): Insurance Risk Study – Global Insurance Market Opportunities, Tenth edition 2015. http://thoughtleadership.aonbenfield.com/documents/20150913-ab-analytics-insurance-risk-study.pdf. Last accessed: December 03, 2015.

Arrow, K. J. (1965): Aspects of the Theory of Risk-Bearing, Yrjö Jahnsson Foundation, Helsinki.

Asllani, A., White, C. S., and Ettkin, L. (2013): Viewing Cybersecurity as a Public Good – The Role of Governments, Businesses, and Individuals, Journal of Legal, Ethical and Regulatory Issues 16(1), 7-14.

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

Baettie, A. (2015): The History of Insurance. http://www.investopedia.com/articles/08/history-of-insurance.asp?layout=infini. Last accessed: November 11, 2015.

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

Bank for International Settlements (BIS) (2006): International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version. www.bis.org/publ/bcbs128.pdf. Last accessed December 10, 2013.

Ben Ammar, S., Braun, A., and Eling, M. (2015): Alternative Risk Transfer and Insurance-Linked Securities: Trends, Challenges and New Market Opportunities, I.VW- Schriftenreihe, Band 56.

Berliner, B. (1982): Limits of Insurability of Risks, Englewood Cliffs, NJ: Prentice-Hall.

Bernoulli, D. (1954): Exposition of a new theory on the measurement of risk. Econometrica 22(1), 23-36.

Betterley (2010): Understanding the Cyber Risk Insurance and Remediation Services Marketplace: A Report on the Experiences and Opinions of Middle Market CFOs. www.casact.org/community/affiliates/CANE/0412/Betterley2.pdf. Last accessed: December 16, 2013.

Betterley (2013): The Betterley Report – Cyber/Privacy Insurance Market Survey 2013. http://betterley.com/samples/cpims13_nt.pdf. Last accessed: November 10, 2015.

Betterley (2014): The Betterley Report – Cyber/Privacy Insurance Market Survey 2014. http://betterley.com/samples/cpims14_nt.pdf. Last accessed: March 18, 2015.

Betterley (2015): The Betterley Report – Cyber/Privacy Insurance Market Survey 2015. http://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf. Last accessed: November 10, 2015.

Biener, C., and Eling, M. (2012): Insurability in Microinsurance Markets – An Analysis of Problems and Potential Solutions, The Geneva Papers on Risk and Insurance – Issues and Practice 37, 77-107.
Biener, C., Eling, M., Matt, A., and Wirfs, J. H. (2015): Cyber Risk – Risikomanagement und Versicherbarkeit, I.VW-Schriftenreihe, Band 54.
Biener, C., Eling, M., and Wirfs, J. H. (2015): Insurability of Cyber Risk – An Empirical Analysis, The Geneva Papers on Risk and Insurance – Issues and Practice 40(1), 131–158.
Böhme, R. (2005): Cyber-insurance revisited, in Proceedings of the Fourth Workshop on the Economics of Information Security (WEIS 2005), Harvard University, Cambridge, MA.
Böhme, R. and Kataria, G. (2006): Models and Measures for Correlation in Cyber-Insurance, Working Paper, Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK.
Bolancé, C., Guillen, M., Pelican, E., and Vernic, R. (2008): Skewed bivariate models and nonparametric estimation for the CTE risk measure, Insurance: Mathematics and Economics 43(3), 386-393.
Bolot, J. and Lelarge, M. (2009): Cyber insurance as an incentive for internet security', in M.E. Johnson (ed.) Managing Information Risk and the Economics of Security, New York: Springer, pp. 269–290.
Briys, E., and Schlesinger, H. (1990): Risk Aversion and the Propensities for Self-Insurance and Self-Protection, Southern Economic Journal 57(2), 458–467.
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.
Cannas, G., Masala, G., and Micocci, M. (2009): Quantifying Reputational Effects for Publicly Traded Financial Institutions, Journal of Financial Transformation 27, 76–81.
Cebula, J. J. and Young, L. R. (2010): A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.
CEIOPS (2009): CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR Standard Formula – Article 111 (f): Operational Risk. CEIOPS-DOC-45/09, Frankfurt: Committee of European Insurance and Occupational Pensions Supervisors.
Chavez-Demoulin, V., Embrechts, P., and Hofert, M. (2015): An extreme value approach for modeling Operational Risk losses depending on covariates, The Journal of Risk and Insurance, forthcoming.
Choo, K. K. R. (2014): A cloud security risk-management strategy, Cloud Computing, IEEE 1(2), 52-56.
Cochrane, J. H. (2005); Asset Pricing – Revised Edition, Princeton University Press.
Consorcio de Compensación de Seguros (CSS) (2015): Consorcio de Compensación de Seguros – Scope of Activity. http://www.consorseguros.es/web/ad_re_p. Last accessed: November 02, 2015.
Cossette, H., Gaillardetz, P., Marceau, E., and Rioux, J. (2002): On two dependent individual risk models, Insurance: Mathematics and Economics 30(2), 153-166.
Cummins, J. D., Lewis, C. M., and Wei, R. (2006): The Market Value Impact of Operational Loss Events for US Banks and Insurers, Journal of Banking and Finance 30(10), 2605–2634.
Cummins, J. D., and Mahul, O. (2004): The Demand for Insurance with an Upper Limit on Coverage, The Journal of Risk and Insurance 71(2), 253-264.
Drouin, D. (2004): Cyber Risk Insurance: A Discourse and Preparatory Guide, Bethesda, MD: SANS Institute, www.sans.org/reading-room/whitepapers/legal/cyber-risk-insurance-1412. Last accessed: December 19, 2013.
Edwards, B., Hofmeyr, S., and 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, June 2015.
Ehrlich, I., and Becker, G. S. (1972): Market Insurance, Self-Insurance, and Self-Protection, Journal of Political Economy 80(4), 623–648.
Eling, M. (2012): Fitting insurance claims to skewed distributions – Are the skew-normal and skew-student good models? Insurance: Mathematics and Economics 51(2), 239-248.
Eling, M. and Wirfs, J. H. (2016): Modelling and Management of Cyber Risk. Working Paper.
ENISA (2012): Incentives and barriers of the cyber insurance market in Europe. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe. Last accessed: November 09, 2015.

Enz, W. (2015): Werweissen über VW-Versicherung. http://www.nzz.ch/wirtschaft/werweissen-ueber-vw-versicherung-1.18621672. Last accessed: November 26, 2015.

European Commission (2014): Study on co(re)insurance pools and on ad-hoc co(re)insurance agreements on the subscription market – New edition July 2014. Luxembourg – Publication Office of the European Union, 2014.

Farny (2011): Versicherungsbetriebslehre. Verlag Versicherungswirtschaft GmbH, Karlsruhe, Germany, 5th edition.

Federal Social Insurance Office (FSIO) (2015): Purpose of old-age and survivors' insurance. http://www.bsv.admin.ch/themen/ahv/00011/01259/index.html?lang=en. Last accessed: November 14, 2015.

Finkle, J. (2015): Ace offers $100 million cyber policies with added services, scrutiny. http://www.reuters.com/article/2015/09/24/us-ace-ltd-cyberinsurance-idUSKCN0RO2LD20150924#epgXi5Y5uU11kXSA.97. Last accessed: November 05, 2015.

Fragnelli, V., and Marina, M. E. (2003): A fair procedure in insurance, Insurance: Mathematics and Economics 33, 75-85.

Friendsurance (2015): Homepage. https://www.friendsurance.de/. Last accessed: October 28, 2015.

Fundación Mapfre (2013): An Introduction to Reinsurance. http://www.baskent.edu.tr/~erdemk/introduction%20to%20reinsurance.pdf. Last accessed: October 18, 2015.

Gatzert, N., and Schmeiser, H. (2012): The merits of pooling claims revisited, Journal of Risk Finance 13(3), 184-198.

General Accounting Office (GAO) (2001): Terrorism Insurance – Alternative Programs for Protecting Insurance Consumers. United States General Accounting Office, GAO-02-175T.

Gestion de l'Assurance et de la Réassurance des risques Attentats et actes de Terrorisme (GAREAT) (2015): Homepage. http://www.gareat.com/en. Last accessed: November 03. 2015.

Gilli, M., and Këllezi, E. (2006): An application of extreme value theory for measuring financial risk, Computational Economics 27(2-3), 1-23.

Golubin, A. Y. (2014): Optimal insurance and reinsurance policies chosen jointly in the individual risk model, Scandinavian Actuarial Journal, http://dx.doi.org/10.1080/03461238.2014.918696. Last accessed: August 24, 2015.

Gordon, L. A., Loeb, M. P. and Sohail, T. (2003): A framework for using insurance for cyber-risk management, Communications of the ACM 44(9), 70–75.

Gould, J. (2013): Allianz eyes growth in computer hacking insurance. uk.reuters.com/article/2013/07/10/us-allianz-hacking-cover-idUKBRE9690O120130710. Last accessed: December 16, 2013.

Government Communications Headquarters (GCHQ) (2012): 10 Steps to Cyber Security. White Paper of the Information Security Arm of GCHG, London.

Gray, A. (2015): Cyber risks too big to cover, says Lloyd's insurer. http://www.ft.com/intl/cms/s/0/94243f5a-ad38-11e4-bfcf-00144feab7de.html#axzz3twAlZLsP. Last accessed: December 04, 2015.

Guevara (2015): Homepage. https://heyguevara.com/. Last accessed: October 18, 2015.

Guy Carpenter (2015): Guy Carpenter Mid-Year Review Assesses Key Industry Trends. http://www.guycarp.com/content/dam/guycarp/en/documents/PressRelease/2015/Guy%20Carpenter%20Mid-Year%20Review%20Assesses%20Key%20Industry%20Trends.pdf. Last accessed: September 17, 2015.

Haas, A., and Hofmann, A. (2013): Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit, FZID Discussion Paper No. 74-2013.

Harvard Business Review Analytic Services (2013): Meeting the Cyber Risk Challenge, Boston, MA: Harvard Business School Publishing.

Herath, H. and Herath, T. (2011): Copula-based actuarial model for pricing cyber-insurance policies, Insurance Markets and Companies: Analyses and Actuarial Computations 2(1), 7–20.

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.

Hofmann, A. and Ramaj, H. (2011): Interdependent risk networks: The threat of cyber attack, International Journal of Management and Decision Making 11(5/6): 312–323.

Insurance Information Institute (III) (2005): Public/Private Mechanisms for Handling Catastrophic Risks in the United States. www.iii.org.

Insurance Journal (2015): Allianz is Lead Underwriter for Crashed Germanwings Airbus A320. http://www.insurancejournal.com/news/international/2015/03/25/362024.htm. Last accessed: November 14, 2015.

Japan Earthquake Reinsurance Co., Ltd. (JER) (2013): Japan Earthquake Reinsurance Co., Ltd. – Annual Report 2013. http://www.nihonjishin.co.jp/disclosure/2013/en_02.pdf. Last accessed: November 03, 2015.

Jarque, C. M., and Bera, A. K. (1987): A test for normality of observations and regression residuals, International Statistical Review 55, 163-172.

Kaas, R., Goovaerts, M., Dhaene, J., and Denuit, M. (2008): Modern Actuarial Risk Theory, 2nd ed., Springer.

Kaspersky Lab (2013): Global Corporate IT Security Risks: 2013. www.kasperskycontenthub.com/pres scenter/files/2013/10/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf. Last accessed: April 24, 2014.

Klein, R. W. (2013): Insurance Market Regulation – Catastrophe Risk, Competition, and Systemic Risk, in: G. Dionne (ed.), Handbook of Insurance (2nd edition), Chapter 31, pp. 909-939.

Klugman, S. A., Panjer,H. H., and Willmot, G. E. (2012): Loss Models: From Data to Decisions, fourth edition, Wiley Series in Probability and Statistics, John Wiley & Sons, Inc.

KPMG (2013): e-Crime – Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz, KPMG Forensic Services. www.kpmg.com/CH/de/Library/Articles-Publications/Seiten/e-crimesurvey-2013.aspx. Last accessed: January 18, 2014.

Kraut, G. (2014): A Fair Pool Sharing Mechanism for Illiquid Catastrophe Risk Markets, Munich Risk and Insurance Center Working Paper, No. 19.

Kshetri, N. (2010): The Global Cybercrime Industry. Springer.

Kunreuther, H., Hogarth, R., and Meszaros, J. (1993): Insurer Ambiguity and Market Failure, Journal of Risk and Insurance 7(1), 71-87.

Kunreuther, H., Kleindorfer, P., and Grossi, P. (2005): The Impact of Risk Transfer Instruments: An Analysis of Model Cities, in: P. Grossi and H. Kunreuther (eds.), Catastrophe Modeling: A New Approach to Managing Risk, Chapter 9, pp.189-208.

Kuypers, M. A., Heon, G., Martin, P., Smith, J., Ward, K., and Paté-Cornell, E. (2014): Cyber Security – the Risk of Supply Chain Vulnerabilities in an Enterprise Firewall, Working Paper – Stanford University.

Labonte, M. (2010): The Size and Role of Government – Economic Issues, Congressional Research Service.

Lale, Ö. (2013): Alternative risk Transfer: Advantages and risks of transferring insurance risks to capital markets. https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2013/fa_bj_2013_06_alternativer_risikotransfer_en.html;jsessionid=E2966268C6AF397FF011FDF982A70070.1_cid372. Last accessed: April 23, 2015.

Levy, H., and Markowitz, H. M. (1979): Approximating expected utility by a function of mean and variance, The American Economic Review 69(3), 308-317.

Lloyd's (2015): Business Blackout – The insurance implications of a cyber attack on the US power grid. https://www.lloyds.com/news-and-insight/risk-insight/library/society-and-security/business-blackout. Last accessed: November 06, 2015.

Long Finance (2015): Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance. http://www.longfinance.net/images/Promoting_UK_Cyber_Prosperity_28July2015.pdf. Last accessed: September 16, 2015.

Maillart, T., and Sornette, D. (2010): Heavy-tailed distribution of cyber-risks, The European Physical Journal B 75, 357-364.

Majuca, R.P., Yurcik, W. and Kesan, J.P. (2006): The evolution of cyberinsurance, working paper, arxiv.org/abs/cs/0601020. Last accessed: January 18, 2014.

Marsh (2012): Cyber Insurance. www.iod.org.nz/Portals/0/Branches%20and%20events/Canterbury/Marsh%20Cyber%20Insurance.pdf. Last accessed: January 17, 2014.
Marsh (2013): Cyber Risk Survey 2013. www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/partner/Partnerbeitrag_Marsh_Cyber-Risk_Survey.pdf?__blob=publicationFile. Last accessed: December 16, 2013.
Marsh (2014): Historical Development of Cyber (Re)Insurance. http://www.gccapitalideas.com/2014/10/23/historical-development-of-cyber-reinsurance/. Last accessed: March 18, 2015.
Marsh (2015): European 2015 Cyber Risk Survey Report. http://uk.marsh.com/Portals/18/Documents/European%202015%20Cyber%20Risk%20Survey%20Report-10-2015.pdf. Last accessed: November 25, 2015.
McAfee (2014): Net Losses – Estimating the Global Cost of Cybercrime. http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf. Last accessed: March 16, 2015.
McNeil, A. J., Frey, R., and Embrechts, P. (2015): Quantitative Risk Management – Concepts, Techniques, Tools, Revised Edition. Princeton Series in Finance.
Mossin, J. (1968): Aspects of Rational Insurance Purchasing, Journal of Political Economy 76(4), 553-568.
Müller, W. (1981): Theoretical Concepts of Insurance Production, The Geneva Papers in Risk and Insurance 6(21), 63-83.
Müller, K., Schmeiser, H., and Wagner, J. (2011): Insurance Claims Fraud: Optimal Auditing Strategies in Insurance Companies, Working Papers on Risk Management and Insurance No. 92, September 2011.
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K. (2006): e-Risk management with insurance: A framework using copula aided Bayesian belief networks' in Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS), Koba, HI, 4–7 January 2006.
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and 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. and Chakrabarti, B. B. (2005): Insurance for Cyber-Risk: A Utility Model, Decision 32(1), 153–169.
Munich Re (2010): Reinsurance – A Basic Guide to facultative and Treaty Reinsurance. http://www.munichre.com/site/mram-mobile/get/documents_E96160999/mram/assetpool.mr_america/PDFs/3_Publications/reinsurance_basic_guide.pdf. Last accessed: November 03, 2015.
National Academy of Science (2008): Severe Space Weather Events – Understanding Societal and Economic Impacts. http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf. Last accessed: November 12, 2015.
National Association of Insurance Commissioners (NAIC) (2013): Cyber Risk. http://www.naic.org/cipr_topics/topic_cyber_risk.htm. Last accessed: December 7, 2013.
OECD (2005): Terrorism Risk Insurance in OECD Countries, Policy Issues in Insurance No. 9, OECD Publishing.
Ögüt, H., Raghunathan, S., and 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.
PeerCover (2015): Homepage. http://www.peercover.co.nz/p2pinsurance-around-the-world.html. Last accessed: October 28, 2015.
Podolak, G. D. (2015): Insurance for Cyber Risks – A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges, Quinnipiac Law Review 33, 369-409.
Ponemon Institute (2013): Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age. www.assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf. Last accessed: January 18, 2014.
Ponemon Institute (2015a): 2015 Cost of Cyber Crime Study – Global. http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/. Last accessed: March 03, 2016.

Ponemon Institute (2015b): 2015 Cost of Data Breach Study – Global Analysis. https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF. Last accessed: March 03, 2016.
Pool Inquinamento (2015): Homepage. http://www.poolinquinamento.it/about/english/?lang=it_IT. Last accessed: November 03, 2015.
Pool Re (2015): Homepage. https://www.poolre.co.uk/.Last accessed: November 03, 2015.
Pratt, J. (1964): Risk Aversion in the Small and in the Large, Econometrica 32(1-2), 122-136.
PwC (2015a): Insurance 2020 & beyond – Repeating the dividends of cyber resilience. https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf. Last accessed: March 02, 2016.
PwC (2015b): Insurance Banana Skins 2015 – The CSFI survey of the risks facing insurers. Center for the Study of Financial Innovation.
Reichel, L., and Schmeiser, H. (2015): The Liability Regime of Insurance Pools and Its Impact on Pricing. Working Papers on Risk Management and Insurance. St. Gallen: Institute of Insurance Economics, University of St. Gallen, 2015.
Renard, G. F., and Terry, D. (2011): Guilds in the Middle Ages. Ulan Press.
Samuelson, P. A. (1963): Risk and uncertainty – The fallacy of the Law of Large Numbers, Scientia 98, 108-113.
Shackelford, S. J. (2012): Should your firm invest in cyber risk insurance? In: Business Horizon 55, 349–356.
Shackelford, S., and Russell, S. L. (2014): Risky Business – Lessons for Mitigating Cyber Attacks from the International Insurance Law on Piracy, Minnesota Journal of International Law Online (forthcoming).
Shetty, N., Schwarz, G., Felegyhazi, M. and Walrand, J. (2010): Competitive cyber-insurance and internet security, in T. Moore, D. Pim and C. Ioannidis (eds.) Economics of Information Security and Privacy, New York: Springer, pp. 229–247.
Smolka, A. (2003): The principle of risk partnership and the role of insurance in risk mitigation, in: P. Sahni and M. M. Ariyabandu (eds.), Disaster Risk Reduction in South Asia, chapter 3, pp. 37-43.
Statista (2015): Share of companies with standalone cyber insurance in the United States from 2013 to 2014, by industry. www.statista.com. Last accessed: September 16, 2015.
Swiss Insurance Association (2015): The Swiss Natural Perils Pool. http://www.svv.ch/en/consumer-info/non-life-insurance/swiss-natural-perils-pool. Last accesses: October 29, 2015.
Swiss Re (2013): The essential guide to reinsurance. http://media.swissre.com/documents/The_essential_guide_to_reinsurance_updated_2013.pdf. Last accessed: September 17, 2015.
Swiss Re (2014): Working together with clients to find cyber risk solutions. http://www.swissre.com/reinsurance/insurers/casualty/smarter_together/working_smarter_together_for_cyberrisk_solutions_in_EMEA.html. Last accessed: March 18, 2015.
Swiss Re (2015): Investors' Day – Rüschlikon, December 8, 2015. http://media.swissre.com/documents/id2015_full_slide_package.pdf. Last accessed: March 14, 2016.
Symantec Corporation (2013): 2013 Norton Report. http://www.symantec.com/content/de/de/about/downloads/2013_Norton_Report_Deck.pdf. Last accessed: March 16, 2015.
Symantec Corporation (2015): Internet Security Threat Report – April 2015, Volume 20. http://know.symantec.com/LP=1123. Last accessed: November 05, 2015.
Takaful Pakistan Ltd. (2015): Difference between Takaful and Conventional Insurance. http://www.takaful.com.pk/TakafulVsConventional.html. Last accessed: November 03, 2015.
Thomas, L., and Finkle, J. (2014): Insurers struggle to get grip on burgeoning cyber risk market. http://www.reuters.com/article/2014/07/14/us-insurance-cybersecurity-idUSKBN0FJ0B820140714. Last accessed: March 18, 2015.
T-Systems (2014): Cyber Security Report 2014 – Ergebnisse einer Repräsentativen Befragung von Abgeordneten sowie Top-Führungskräften in Mittleren und Grossen Unternehmen. https://www.google.ch/search?q=Cyber+Security+Report+2014&ie=utf-8&oe=utf-8&gws_rd=cr&ei=N7vFVqPWGIa9sQHPu57YDQ#q=%22Cyber+Security+Report+2014%22. Last accessed: February 18, 2016.

Villaseñor-Alva, J. A., and González-Estrada, E. (2009): A bootstrap goodness of fit test for generalized Pareto distribution, Computational Statistics and Data Analysis 53(11), 3835-3841.

VOV GmbH (2015): Homepage. http://www.vovgmbh.de/home/. Last accessed: November 03.2015.

Wang, Q.-H. and Kim, S.H. (2009a): Cyberattacks: Does physical boundary matter?, ICIS 2009 Proceedings – Thirtieth International Conference on Information Systems, Paper 48.

Wang, Q.-H. and Kim, S.H. (2009b): Cyber attacks: Cross-country interdependence and enforcement, working paper.

Wheatley, S., Maillart, T., and Sornette, D. (2015): The Extreme Risk of Personal Data Breaches & The Erosion of Privacy. Working Paper – Cornell University Library. http://arxiv.org/abs/1505.07684. Last accessed: November 17, 2015.

Willis (2013a): Willis Fortune 500 Cyber Disclosure Study, 2013. blog.willis.com/downloads/cyber-disclosurefortune-500. Last accessed: December 16, 2013.

Willis (2013b): Willis Fortune 1000 Cyber Disclosure Report. blog.willis.com/downloads/cyber-disclosurefortune-1000-2013. Last accessed: December 16, 2013.

Wirfs, J. H. (2016): Optimal Risk Transfer for Cyber Risk, Working Paper.

World Bank (2013): Mexico – Agricultural Insurance Market Review, Fondos – Mexico's Unique Agricultural Mutual Insurance Funds. http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2014/05/20/000442464_20140520130945/Rendered/PDF/880990BRI0P1300urance04Pager0Fondos.pdf. Last accessed: October 28, 2015.

World Economic Forum (2010): Global Risk Report 2010 – A Global Risk Network Report. http://www.weforum.org/pdf/globalrisk/globalrisks2010.pdf. Last accessed: November 17, 2015.

World Economic Forum (2015): Global Risks Report 2015 – Tenth Edition. http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf. Last accessed: October 9, 2015.

Zelle, A. R., and Whitehead, S. M. (2014): Cyber Liability – It's Just a Click Away, Journal of Insurance Regulation, 33, 145.

Zweifel, P., and Eisen, R. (2012): Insurance Economics. Springer.

Appendix A: Existing Literature and Data Sources

Table A1 Existing Literature

	A. Academic Papers on Cyber Risk and Cyber Insurance	
1	Biener, Eling, and Wirfs (2015)	Discuss the adequacy of insurance for managing cyber risk. Analysis of insurability by a combination or literature review and statistical property analysis of cyber losses, which are extracted from an operational risk database.
2	Edwards, Hofmeyr, and Forrest (2015)	Develop a Bayesian Generalized Linear Model to investigate trends in data breaches. Their evaluations show that neither size not frequency of data breaches has increased over the past decade.
3	Podolak (2015)	Focuses on the legal aspects in cyber insurance, the today's litigation trends and their impact on tomorrow's design of cyber insurance products.
4	Wheatley, Maillart, and Sornette (2015)	Model data breaches by an extremely heavy-tailed truncated Pareto distribution, and analyze the effects of firm size and industry sector on breach size and frequency.
5	Choo (2014)	Defines a cloud security risk management strategy for cloud service provides as well as the organizational cloud service users.
6	Kuypers et al. (2014)	Define a probabilistic risk analysis model for a firewall, and evaluate the trade-off between costs and security.
7	Shackelford and Russell (2014)	Discuss the impact of cyber attacks on the private sector with analyzing the benefits and drawbacks of relying on cyber insurance to enhance cybersecurity by drawing from the maritime insurance industry's response to piracy. Their result is that firms have to be proactive in managing cyber risks and need to help secure critical international infrastructure.
8	Zelle and Whitehead (2014)	Discuss the evolution of cyber risk disputes in litigation involving traditional policies and explore possible future coverage issues under cyber liability policies.
9	Haas and Hofmann (2013)	Discuss risk management and insurability of cloud computing from an enterprise risk management perspective.
10	Mukhopadhyay et al. (2013)	Utility models to aid a firm's decision on whether to use cyber insurance policies; expand Mukhopadhyay et al. (2005) by use of copula-aided Bayesian belief network.
11	Shackelford (2012)	Analyzes the impact of cyber attacks on firms, some of the applicable U.S. law, and the extent to which cyber insurance mitigates the cyber threat.
12	Herath and Herath (2011)	Develop a copula framework to price cyber insurance policies.
13	Hofmann and Ramaj (2011)	Develop an economic model that explicitly reflects the interdependent risk structure of a cyber network.
14	Ögüt, Raghunathan, and Menon (2011)	Discuss the use of insurance and self-protection in the context of correlated cyber risk and imperfect ability to verify losses.
15	Cebula and Young (2010)	Provide a taxonomy of operational cyber security risks and identify and organize sources for it (results: four classes).
16	Maillart and Sornette (2010)	Analyze the statistical properties of cyber risks by quantifying the distribution and time evolution of information risk. They fit a heavy-tailed power-law distribution to severities of personal information theft events, and identify a connection of the loss distribution with company size.
17	Shetty, Felegyhazi, and Walrand (2010)	Network security may be lower with insurance because of moral hazard.
18	Bandyopadhyay, Vijay, and Rao (2009)	Show that insurers react to the high level of uncertainty regarding average losses from cyber incidents by setting high deductibles and low maximum coverage.
19	Bolot and Lelarge (2009)	Combine ideas from risk theory and network modeling to analyze the impact of positive externalities of cyber insurance on overall internet security.
20	Wang and Kim (2009a)	Analyze interdependences in cyber attacks across national boundaries by evaluating spatial autocorrelations of cyber attacks.
21	Wang and Kim (2009b)	Characterize empirically the interdependence in cyber attacks and analyze the impact of an international treaty against cybercrimes on it.
22	Baer and Parkinson (2007)	Discuss barriers to cyber insurance markets such as information asymmetries and correlation of cyber risks and also in the context of the public good character of self-protective measures.
23	Böhme and Kataria (2006)	Focus on correlation properties of different cyber risks and introduce a classification of cyber risks based on correlation properties.
24	Majuca, Yurcik, and Kesan (2006)	Discuss the development of the market for cyber insurance, finding that the evolution of internet security risk and increasing compliance requirements significantly drive demand.
25	Mukhopadhyay et al. (2006)	Introduce an approach to estimate cyber risk probabilities based on Bayesian belief networks as a basis to determine cyber insurance premiums.
26	Böhme (2005)	Discusses the formation of a proper cyber insurance market and problems by correlated losses; also the conditions under which coverage of cyber risk is possible are evaluated.
27	Mukhopadhyay et al. (2005)	Develop a utility model for assessing the benefit of using insurance to manage cyber risk.
28	Gordon, Loeb, and Sohail (2003)	Discuss the information asymmetries (adverse selection, moral hazard) in cyber insurance and provide an overview on products in the United States.

	B. Industry Studies on Cyber Insurance	
1	Betterley (2015)	Global: annual gross premiums written for cyber insurance in the United States are at US$ 2.75 billion, growing 26–50% per year on average.
2	Marsh (2015)	Only 7% of the respondents evaluate the available cyber insurance products in the European market as sufficient to meet the organization's needs. That is why only 12% of the organization already bought and 6% are in the process of busing insurance.
3	AGCS (2015)	Estimated total cost of cybercrime per year for the global economy to be US$ 445 billion and provide a country ranking by GDP for the world's top 10 economies. Furthermore, they estimate the market currently to about US$ 2 billion in yearly premiums worldwide, with US business accounting for approximately 90%.
4	Betterley (2014)	Global: annual gross premiums written for cyber insurance in the United States are at US$ 2 billion, growing 10–25% per year on average.
5	Betterley (2013)	Global: annual gross premiums written for cyber insurance in the United States are at US$ 1.3 billion, growing 10–25% per year on average.
6	Harvard Bus. Review An. Services (2013)	Survey among 152 U.S. companies in the public and private sectors; 19% of the companies already have cyber insurance, but the majority (60%) has no plan to buy cyber insurance.
7	Marsh (2013)	Europe: 25% of corporations are not aware of insurance solutions for cyber risk and only 10% have bought insurance coverage.
8	Willis (2013a, b)	United States: coverage at about 6%, but large variations between industries among the Fortune 1000 companies.
9	Betterley (2010)	Global: cyber insurance market grew from US$ 100 million in 2003 to at least US$ 600 million as of 2009.
10	Drouin (2004)	Examines what cyber insurance is available, what protection is likely required, the liabilities an organization faces, and remedies that will lessen the impact of cybercrime.

Note: Table is an updated and extended version of the metarial presented in Biener, Eling, and Wirfs (2015).

Table A2 Existing Data Sources

#	**Source**
1	Ponemon Institute: Global Cost of Data Breach Study and Global Cost of Cyber Crime Study
2	CSI/FBI: Computer Crime and Security Survey
3	Hackmageddon: Cyber Attacks Time line Master Index
4	Symantec: Internet Security Threat Report, Norton Cybercrime Report
5	McAfee: The Economic Impact of Cyber Crime and Cyber Espionage, Net Losses – Estimating the Global Cost of Cyber Crime
6	World Economic Forum: Global Risk Report
7	NetDiligence: Cyber Claims Study
8	KPMG: KPMG Forensics Services

Appendix B: Categories of Cyber Risk

Table B1 Categories of Cyber Risk (Cebula and Young, 2010)

Category	Description	Elements
Subcategory 1: actions of people		
1.1 Inadvertent	unintentional actions taken without malicious or harmful intent	mistakes, errors, omissions
1.2 Deliberate	actions taken intentionally and with intent to do harm	fraud, sabotage, theft, and vandalism
1.3 Inaction	lack of action or failure to act in a given situation	lack of appropriate skills, knowledge, guidance, and availability of personnel to take action
Subcategory 2: systems and technology failures		
2.1 Hardware	risks traceable to failures in physical equipment	failure due to capacity, performance, maintenance, and obsolescence
2.2 Software	risks stemming from software assets of all types, including programs, applications, and operating systems	compatibility, configuration management, change control, security settings, coding practices, and testing
2.3 Systems	failures of integrated systems to perform as expected	design, specifications, integration, and complexity
Subcategory 3: failed internal processes		
3.1 Process design and/or execution	failures of processes to achieve their desired outcomes due to poor process design or execution	process flow, process documentation, roles and responsibilities, notifications and alerts, information flow, escalation of issues, service level agreements, and task hand-off
3.2 Process controls	inadequate controls on the operation of the process	status monitoring, metrics, periodic review, and process ownership
3.3 Supporting processes	failure of organizational supporting processes to deliver the appropriate resources	staffing, accounting, training and development, and procurement
Subcategory 4: external events		
4.1 Catastrophe	events, both natural and of human origin, over which the organization has no control and that can occur without notice	weather event, fire, flood, earthquake, unrest
4.2 Legal issues	risk arising from legal issues	regulatory compliance, legislation, and litigation
4.3 Business issues	risks arising from changes in the business environment of the organization	supplier failure, market conditions, and economic conditions
4.4 Service dependency	risks arising from the organization's dependence on external parties	utilities, emergency services, fuel, and transportation

Appendix C: Data Search and Identification Strategy

To be categorized as a cyber risk incident, a loss event must meet three criteria: (1) a *critical asset* such as a company server or database needs to be affected, (2) a relevant *actor* (e.g., hackers, employees, system, nature) needs to be involved in causing the cyber risk incident, and (3) a relevant *outcome* such as the loss of data or misuse of confidential data needs to be present (Table C1). For each category we defined a comprehensive set of keywords, which we then systematically scanned for in the incident descriptions of our SAS OpRisk Global Data database (Table C2). The resulting dataset includes a total of 1,579 cyber risk incidents, or about 5.9% of the total sample of operational risks.

Table C1 Data Search Strategy

Step	Description
1.	For all three criteria – critical asset, actor, and outcome – we identify keywords that describe terms in the appropriate group
2.	We searched the descriptions of each observation in our sample data for a combination of keywords, where each combination consisted of one word from each group (three-word combinations)
3.	We checked all identified observations individually (reading each description) for their affiliation to cyber risk or non-cyber risk and if necessary we excluded the incidents from the cyber risk term; while checking the observations we also decided in which of the cyber risk categories they fit best
4.	For all observations that were not identified by one of our keyword combinations we checked randomly chosen incidents and included them if necessary. If we could identify keyword combinations that we missed in the first round, we started over at Step 2 with these new words.

Table C2 Keywords per Criterion

Critical Asset	Actor	Actor (cont.)	Outcome
account	*(1) Actions by people*	*(2) Systems and technical failure*	availability
accounting system	administrator	defect	available
address	deadline	hardware	breach
code	denial of service, DoS	loading	breakdown
communication	destruction	malicious code	confidential
computer	devastation	software	congestion
computer system	employee	stress	constrain
confidential	extortion	system crash	control
confidential document	forgot, forget, forgotten		delete
consumer information	hacker, hacked	*(3) Failed internal processes*	deletion
data	hacking	unauthorized access	disclosure
disk	human error		disorder
document	infect	*(4) External events*	disruption
file	infection	Blizzard	disturbance
hard-disk	infiltrate	Earthquake	encryption
hard-drive	infiltrated	Eruption	espionage
homepage	key logger	Explosion	failure
info(rmation)	lapse	Fire	false
information system	logic bomb	Flood	falsification
internet site	maintenance	Hail	falsified
names	malware	heat wave	falsifying
network	manager	Hurricane	incompatibility
numbers	manipulate	Lightning	incompatible
online banking	miscommunication	natural catastrophe	incomplete
payment system	mistake	Outage	integrity
PC	misuse	pipe burst	interruption
personal information	omission	Riot	limit
phone	online attack	Smoke	lose
purchase information	oversight	Storm	loss
record	phish	Thunder	lost
reports	phishing	Tornado	malfunction
server	spam	Tsunami	missing
site	Trojan	Typhoon	modification
social security number	vandalism	Unrest	modified
stored information	virus	Utilities	modify
tablet	worm	War	overload
trade secret		Weather	publication
webpage		Wind	restrict
website			sabotage
			steal
			stole
			theft

Note: We used regular expressions to ensure that different spellings were captured (e.g., "homepage" and "home page").

Appendix D: Risk Modeling Results

Operational risk models apply methods form the extreme value theory when estimating the loss severity distribution. We follow Hess (2011) and estimate the loss severity distribution using a spliced distribution approach (also called "Peak-over-Threshold" or POT). Losses above a predefined threshold are modelled by a generalized Pareto distribution (GPD), while losses below the threshold are modelled with an exponential (or log-normal) distribution. We apply the bootstrap goodness-of-fit test by Villaseñor-Alva and González-Estrada (2009) and, based on this, choose a threshold at the 90% percentile.[75] The value at risk (VaR) and the Tail VaR (TVaR) are then approximated by an estimator described by Gilli and Këllezi (2006). We also model losses with other distributions common to actuarial science, such as the log-normal, Gamma or Weibull distribution (e.g., Eling, 2012). We estimate the respective parameters and present the VaR and TVaR (Table D1).

Table D1 Risk Measurement

Model	Cyber Risk (N = 1,579)		Non-Cyber Risk (N = 24,962)	
	VaR	TVaR	VaR	TVaR
POT (threshold of 90%)	**104.63**	1,720.03	226.78	4,565.33
Exponential	130.20	173.72	295.51	393.73
Gamma	213.03	352.20	474.48	772.17
GPD	**94.35**	222,554.60	**237.39**	24,730.33
Log-normal	63.15	238.18	206.62	851.67
Weibull	88.61	196.32	232.64	496.80
Empirical	100.55	730.52	271.60	1,565.81

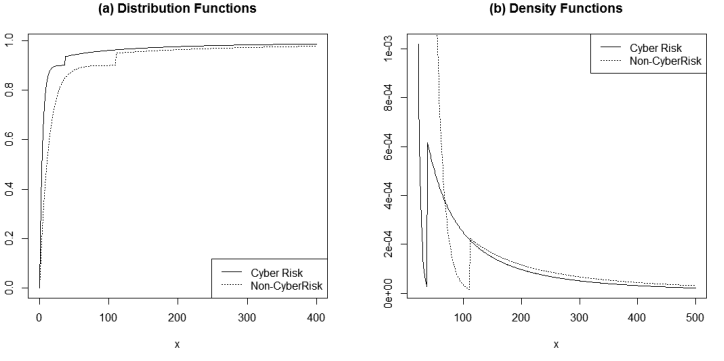
Note: Value at risk (VaR) and tail value at risk (TVaR) at 95% confidence level.

The VaR estimator for cyber risk, applying the Exponential, Gamma, Log-normal, and Weibull distribution, is significantly different from the empirical VaR, which indicates that the distribution assumption does not fit the data well in the tails. The result for the GPD distribution is much closer to the empirical VaR than to the other four parametric distributions. However, the estimate from the POT provides the best fit for the VaR. Similar results can be observed for the TVaR, although the deviation in all models are more significant. The Exponential, Gamma, Log-normal, and Weibull distribution significantly underestimate the TVaR, while the GPD significantly overestimates the TVaR. This suggests that they are not modeling the tail-behavior

[75] For purposes of comparison, we also computed results for a 92.5 per cent threshold (which can be made available upon request); thresholds below this threshold reveal a non-fit for non-cyber risks according to Villaseñor-Alva and González-Estrada (2009); raising thresholds much higher makes the sample used for the fit in cyber risk too small.

appropriately. Although overestimating the tail-losses, the POT approach again provides the best fit. Moreover, a more conservative estimation might be appropriate for regulatory purposes.[76] In the comparison of non-cyber risks, GPD provides the best fit for VaR. The POT approach does not show a very good approximation of the VaR and the TVaR, which motivates a more extensive analysis. Furthermore, the results show that the distribution of cyber risk differs significantly from the distribution of other operational risks. For example, the distribution of the non-cyber risk sample shows much higher VaR and TVaR than that of the cyber risk sample, explaining in part the much higher maximal losses in these categories.[77] This finding implies that when modeling operational risk, cyber risk needs to be considered separately. Distribution and density functions for cyber and non-cyber risk are shown in Figure D1.

Figure D1 Estimated Distribution and Density Function



The presented analysis is only a very small portion of the results presented in Eling and Wirfs (2016). Their paper contains a much more detailed analysis and more information on this topic.

[76] An approximation of the loss distribution per category was not conducted, since the sample size would be too small for the computation of the tail distribution, in particular the category "External events." However, an analysis of this issue is possible by the approach described in Chavez-Demoulin, Embrechts, and Hofert (2015).

[77] The modeled VaR for non-cyber risk is more than twice as high as for cyber risk.

Appendix E: Technical Details

In this appendix part we discuss the technical details used in the expected utility analysis of Section 4. The model used here is a special version of the constructs in Wirfs (2016). For more detailed analyses and a more detailed definition of the model we refer also to this work. In the following we will describe three topics: (1) the simulation approach for loss data under each risk transfer layer; (2) the expected utility approach for each risk transfer layer; and (3) a more detailed definition of Scenario #4 used in the scenario analyses of Section 4.3.3.

(1) Simulation Approach for Loss Data:

For the expected utility model we need to simulate losses for each risk transfer layer (i.e., risk owner, primary insurer, reinsurer, and capital market). While the risk owner faces a risk of having a cyber risk loss of a particular size or no loss, the primary insurer (reinsurer) faces losses in a portfolio of losses. Similar applies to the capital market, which takes over risks from a primary insurer's (reinsurer's) portfolio. Moreover, the losses on each layer highly depend on the assumptions made for the contract specifications (e.g., I^{PI}, I^{RE}, or the specifications in the cyber cat bond). The loss simulation approach is described in the following.

The simulation of the risk owner's losses is based on actual cyber loss incident observations. The data used for this purpose is the SAS OpRisk Global data, which is an operational risk database from which cyber incidents were separated (Appendix C). The observations are then used to fit a loss severity distribution by actuarial standard approaches (Eling and Wirfs, 2016, who accomplish this task on the same dataset). This distribution function however, does not incorporate the possibility of a risk owner not having any loss. We compute a mixed distribution, by assuming that a company faces a loss X which is defined as follows:

$$X = Y \times Z,$$

where Z is an indicator random variable, with values $Z = 1$ (a loss occurs with probability p, $0 \leq p \leq 1$) or $Z = 0$ (no loss occurs with probability $1\text{-}p$) and Y being a random variable described by the fitted loss-severity distribution. Afterwards, losses of the form X can be easily generated by random number generators (e.g., given in the statistical software packages of *R*). The final loss for the risk owner then can be adjusted by the indemnity payment I^{PI}, which then leaves the risk owner with an overall loss of $X - I^{PI}(X)$.

The loss for the primary insurer can be generated from the risk owner's losses. For the interested reader, the general modeling approaches for aggregated losses in a portfolio can be found in Kaas et al. (2008) or Klugman, Panjer, and Willmot (2012). Because of the simulation, we will not need the exact distribution for the primary insurer's loss. We will generate random losses on risk owner level by the distribution of random variable X and apply the indemnity function I^{PI}. By aggregating n^{PI} of these losses, we will yield an aggregated random loss L^{PI} for the primary insurer.

The reinsurer's losses are simulated by the same approach used for the primary insurer. We generate random losses L^{PI}, apply I^{RE} to it, which we then aggregate to a loss of a reinsurer's loss portfolio L^{RE} with n^{RE} contracts. The capital market solutions are modelled such that the cyber cat bond will cover losses from a primary insurer's portfolio ("Conventional Model with Capital Markets") or from a reinsurer's portfolio ("Conventional Model with Reinsurance and Capital Markets"). Therefore, depending on the layer the capital market instrument is issued from, the losses are determined as for the primary insurer's loss L^{PI} or the reinsurer's loss L^{RE}.[78] The advantage of this approach is that we can generate correlated losses. The approach used to do so is presented in Cossette et al. (2002).

(2) Expected Utility Approach for each Risk Layer:

This paragraph is a draft of the modeling framework. We define five potential risk transfer layers which can actively engage in the risk transfer market: the risk owner, primary insurers, reinsurers, capital markets, and the government. In this framework, we observe the cash-flows on each risk layer at the time of contracting $t = t_0$ and at the time of loss realization and settlement in $t = t_1$. We then analyze the cash flows in our expected utility framework. The modeling setup for each layer is explained in the following subparagraphs.

"No insurance":

In this model, we assume that the market for cyber risk consists of a risk owner only. There is no form of risk transfer in place. We assume that the individual risk owner faces a loss from cyber risk that is described by the random variable X, which has to be paid by the individual's initial wealth W_0. Because there is no opportunity to transfer risk, the future wealth position W_1 depends only on the future loss and thus

$$W_1 = W_0 - X .$$

[78] The losses for governmental representatives are in general similar to those of the primary insurer or the reinsurer, depending on the layer the state enters the risk transfer.

Under the assumption of a mean-standard deviation utility function U^{RO} of the risk owner, the final expected utility for the risk owner under the "No insurance" model is given by

$$U^{RO}_{No\,Insurance} = W_0 - E[X] - \frac{a^{RO}}{2}\sqrt{Var[X]},$$

with $E[\cdot]$ the expected value, $Var[\cdot]$ the variance, and a^{RO} the risk aversion parameter greater than zero.

"Conventional Model":

The second model is characterized by a primary insurer being the only risk transfer option to the risk owner, offering a cyber insurance contract $I^{PI}(X; C, D)$ depending on the risk owner's loss, with cover limits C and deductibles D (Section 4.2.2). The premium charged for this indemnity payment is P^{RO} (also Section 4.2.2). In case where no insurance is purchased by the risk owner the expected payout at the end of the period is as in the "No insurance" model (above). If the decision to sign an insurance contract is made, the initial value of the individual risk owner will be reduced by the up-front premium payment. The payout at the end of the period with an insurance contract in place is given as

$$W_1^{with\,Insurance} = W_0 - P^{RO} - X + I^{PI}(X; C, D).$$

The expected utility of this payout at the end of the period is then given by

$$U^{RO}_{with\,Insurance} = W_0 - P^{RO} - E\left[X - I^{PI}(X; C, D)\right] - \frac{a^{RO}}{2}\sqrt{Var\left[X - I^{PI}(X; C, D)\right]}.$$

The decision of the risk owner to buy the insurance contract depends on the following inequality:

$$U^{RO}_{with\,Insurance} \geq U^{RO}_{No\,Insurance}. \qquad (1)$$

Only if the expected utility with insurance is greater than the expected utility without it, can an insurance contract be bought. This decision will depend on the definition of I^{PI} and its contract details (i.e., the particular *(C, D)*-combination).

All assumptions made so far have considered only one individual policyholder. Under the "Conventional Model" we also consider a primary insurer with a portfolio of n^{PI} contracts, for which the aggregated loss can be defined by

$$L^{PI}(C, D) = \sum_{i=1}^{n^{PI}} I^{PI}(X_i; C, D),$$

with X_i being the random loss from the i-th contract in the insurer's portfolio (also simulation approach above). As for the risk owner, we assume that the primary insurer is holding total initial funds A_0 which can be used to pay the claims amounting to L^{PI}.

In addition to the initial funds, the primary insurer receives premium payments from each policyholder. The total amount of premiums earned P^{earned} in each period is

$$P^{earned} = \sum_{i=1}^{n^{PI}} P_i^{RO},$$

with P_i^{RO} being the premium payment from the *i*-th policyholder in the portfolio. The funds of the primary insurer at the end of the period then are

$$A_1 = A_0 + P^{earned} - L^{PI}.$$

The final expected utility of the primary insurer is then defined as

$$U^{PI} = A_0 + P^{earned} - E\left[L^{PI}\right] - \frac{a^{PI}}{2}\sqrt{Var\left[L^{PI}\right]},$$

where we assumed a mean-standard deviation-utility function U^{PI} of the primary insurer. For the primary insurer, entering into the risk transfer is only profitable if

$$U^{PI} \geq E\left[U^{PI}\left(A_0\right)\right] = A_0, \qquad \text{(2a)}$$

which means that the expected utility of interacting with the policyholders must be greater than the utility of doing nothing. If this constraint is not satisfied for the specifications given in the contract details (which means function I^{PI}) the insurer would not interact with the risk owners.

Finally, based on the actual loss distribution of *X*, only those contract designs (i.e., *(C, D)*-combinations) are applicable in the market under which (1) and (2a) are satisfied. We will simulate potential *(C, D)*-combinations and identify all feasible solutions, by overlapping the individual solution sets.

"Conventional Model with Reinsurance":

The third model extends the "Conventional Model" by incorporating the reinsurance market as a potential further risk transfer option. We assume the setup from the "Conventional Model" and add a reinsurer, that covers $I^{RE}(L^{PI})$ of the primary insurer's loss and charges a premium of $P^{PI} = \left(1+\lambda^{PI}\right)\cdot E\left[I^{RE}\left(L^{PI}\right)\right] + \lambda_{fixed}^{PI}$ (definitions in Section 4.2.2). In this case, the initial capital a primary insurer has available reduces to $A_0 - P^{PI}$ in the first period. Furthermore, the payout after occurrence of a loss is given by

$$A_1^{with\ reinsurance} = A_0 - P^{PI} + P^{earned} - L^{PI} + I^{RE}\left(L^{PI}\right).$$

The final expected utility of the primary insurer is then defined as

$$U_{with\ reinsurance}^{PI} = A_0 - P^{PI} + P^{earned} - E\left[L^{PI} - I^{RE}\left(L^{PI}\right)\right] - \frac{a^{PI}}{2}\sqrt{Var\left[L^{PI} - I^{RE}\left(L^{PI}\right)\right]}.$$

The primary insurer, will interact with the reinsurance contract only if

$$U^{PI}_{with\ reinsurance} \geq U^{PI}\left(\geq A_0\right), \qquad (2b)$$

with U^{PI} from the previous model without reinsurance.

In addition, we define an expected utility constraint for the reinsurance company that must be satisfied for the overall solution. We assume an exemplary reinsurance firm with a portfolio of n^{RE} reinsurance contracts. The reinsurer covers $I^{RE}\left(L_i^{PI}\right)$ from the *i*-th reinsurance contract's loss in exchange for the premium P_i^{PI}. The aggregated loss paid by the reinsurer is

$$L^{RE} = \sum_{i=1}^{n^{RE}} I^{RE}\left(L_i^{PI}\right).$$

The total premiums earned are summarized by

$$P^{earned,RE} = \sum_{i=1}^{n^{RE}} P_i^{PI}.$$

The reinsurer has an initial fund K_0. If the reinsurer interacts with the primary insurer, the initial payment increases because of the premium payments made by their customers; however, the final payout will be reduced by the indemnity payment to the primary insurer

$$K_1^{with\ reinsurance} = K_0 + P^{earned,RE} - L^{RE}.$$

Under the assumption of a mean-standard deviation-utility function U^{RE} for the reinsurer, the final expected utility is then summarized by

$$U^{RE}_{no\ reinsurance} = E\left[U^{RE}\left(K_0\right)\right] = K_0,$$

in the case of no reinsurance is sold, and

$$U^{RE}_{with\ reinsurance} = E\left[U^{RE}\left(K_1^{with\ reinsurance}\right)\right] = K_0 + P^{earned,RE} - E\left[L^{RE}\right] - \frac{a^{RE}}{2}\sqrt{Var\left[L^{RE}\right]},$$

for the case with reinsurance. We have to assume that the reinsurance company is willing to enter the market only if

$$U^{RE}_{with\ reinsurance} \geq U^{RE}_{no\ reinsurance}, \qquad (3)$$

which provides an additional constraint for the overall solution, that must be satisfied jointly with (1) and (2b).

"Conventional Model with Reinsurance and Capital Markets":

In Section 4.2.2 we define this model in two ways: (1) a primary insurer issues the cyber cat bond (and no reinsurer is in place); and (2) a reinsurer is in place and issues the cyber cat bond. In the following model description we will focus on case (1). Case (2) is modelled analogously.

The approach used in this model follows Kunreuther, Kleindorfer, and Grossi (2005). We assume an insurer (called sponsor) that issues a cyber risk cat bond (analogous to a cat bond), that pays investors an interest payment $r^{Cyber\ Cat}$ in exchange for their guarantee to provide funds in case of a disastrous cyber loss (meaning a loss that cannot be covered by the primary insurer alone). For the implementation of the cyber cat bond we assume a one-period time horizon as before. At the beginning of the period, the investors make a payment to the sponsor (SPV) of

$$\frac{B}{\left(1+r^{Zero-Coupon}\right)},$$

where $r^{Zero-Coupon}$ is the promised return on the zero-coupon catastrophe bond and B is the face value (promised value of the zero-coupon bond (payment if no loss is triggered)). At the end of the period, the investor is paid the face value reduced by the potential indemnity payments to the insurance company. The payments made from the cyber cat bond to the investors is thus given as

$$PO^{Investor} = B - PO^{Sponsor}.$$

The payout from the cyber cat bond to the insurer is given by

$$PO^{Sponsor} = \min\left\{\max\left\{L^{PI} - AP; 0\right\}; K\right\},$$

where L^{PI} is the primary insurer's aggregated loss. The further parameters in this definition of the payout are given as in Section 4.2.2 defined (AP = attachment point, $K (\leq B)$ = maximum payment by the bond). The payments made from the primary insurance company to the investor (premium for taking over the risk) are given by

$$B \cdot r^{Zero-Coupon}.$$

Under this setup the insurer's final fund looks as follows:

$$A_1^{with\ CyberCatBond} = A_0 + P^{earned} - B \cdot r^{Zero-Coupon} - L^{PI} + PO^{Sponsor}.$$

The final expected utility for the primary insurer is thus given by

$$U^{PI}_{with\ CyberCatBond} = A_0 + P^{earned} - B \cdot r^{Zero-Coupon} - E\left[L^{PI} - PO^{Sponsor}\right] - \frac{a^{PI}}{2}\sqrt{Var\left[L^{PI} - PO^{Sponsor}\right]}.$$

As in the "Conventional Model with Reinsurance" this value must be greater than A_0 in the case without the capital market solution (and/or a reinsurance contract), i.e.,

$$U^{PI}_{with CyberCatBond} \geq A_0. \qquad (2c)$$

For the capital market investor we derive the actual return of the investors $r^{CyberCat}$ from the following equations. The overall investor's return can be estimated by

$$R^{Cyber\ CatBond} = r^{Zero-Coupon} - \frac{\left(1+r^{Zero-Coupon}\right) \cdot PO^{Sponsor}}{B}.$$

$R^{CyberCatBond}$ depends on the random variable $PO^{Sponsor}$, and so is itself a random variable. This is also the reason for denoting it $R^{CyberCatBond}$ and not $r^{CyberCat}$. The optimality criterion we will use is then determined by:

$$\frac{E\left[R^{CyberCatBond}\right] - r^{risk-free}}{\sqrt{Var\left[R^{CyberCatBond}\right]}} \geq S. \qquad (4)$$

We determine only solutions as feasible (i.e., part of the investor's solution set) if the estimated annual return to the investor is higher than a benchmark value S (Sharpe ratio).[79] The Sharpe Ratio is then defined by a historical value that is requested by investors today for (natural) catastrophe bonds (see also Kunreuther, Kleindorfer, and Grossi, 2005).

The solution in the "Conventional Model with Capital Markets" must satisfy (1), (2c), and (4).

(3) Definition of Scenario #4:

While Scenarios #1-#3 are based on actual cyber loss data, Scenario #4 is based on estimates provided in WEF (2010) and Lloyd's (2015). We assume that a single primary insurer faces an aggregated loss of US$ 250 billion with a probability of occurrence of 10%. In addition, we assume that in case such a loss occurs, the correlation in the primary insurer's portfolio is 1. If we assume that the primary insurer has n^{PI} contracts in its portfolio, we equally distribute the aggregated loss on the risk owners (i.e., every risk owner has to cover US$ 250 billion/n^{PI}).

Above, we model the losses on each layer by random number generators. This will also be done here, except that the loss distribution of the risk owner is now discrete (i.e., with probability 10% a loss of US$ 250 million/n^{PI} occurs, and in 90% of the cases no loss occurs) and no longer continuous. With those losses the approach can be worked through as before.

[79] Note that investors do not solely price the value of a cat bond by a Sharpe Ratio, but for simplicity we assume this setup here. They might also incorporate metrics like the spread as a measure of expected loss in their decision processes.

Appendix F: Questionnaire

Market Survey "Insurability of Cyber Risk"

The intention of this survey is to identify ways to improve the insurability of cyber risk. Completing the survey shall not need more than 15 minutes. We would be pleased to receive your answers by January 31, 2016.

a. In which of the following fields do you work?
☐ Primary Insurance ☐ Reinsurance ☐ Broker
☐ Government/Regulation ☐ Association ☐ Other: _____

b. In which department do you work? _____

c. In which country are you working? _____

d. How closely is your daily work connected to cyber risk?
☐ I deal with the topic daily ☐ I deal with the topic regularly
☐ I seldom deal with the topic ☐ This is a new topic for me

I. Cyber risk and cyber insurance: Where do we stand?

Cyber risk is defined as any risk emanating from the use and transmission of electronic data.
(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)

a. How would you predict the probability of the following scenarios?
(Probability of occurrence between 0 and 100%)

	Example	*Probability*
1	Probability that a single company in your country will be victim of a cyber incident (e.g., data breach, extortion) within the next year.	%
2	Probability of a global critical infrastructure breakdown (e.g., internet, energy system) lasting several days within the next year.	%
3	Probability of a global critical infrastructure breakdown (e.g., internet, energy system) lasting several days within the next 10 years.	%

Insurance is seen as one potential way to manage cyber risks. However, the actual cyber insurance market is very underdeveloped. In our study we explain this in connection with major problems in insurability. Insurability is a construct to describe conditions which should be satisfied (at least to a degree) to make insurance companies willing to sell and policyholders to buy insurance for that specific risk.

b. In your opinion, what are the biggest challenges for the insurability of cyber risk?

c. How would you rate the following specific problems with respect to the insurability of cyber risks?

(1: Not important, 5: Very important)	1	2	3	4	5
Cyber risk contains a cumulative risk within one line of business (i.e., one cyber incident triggers several losses in different cyber insurance policies)	☐	☐	☐	☐	☐
Cyber risk contains cumulative risks for different lines of business (i.e., one cyber incident triggers losses of one policyholder under different insurance policies; e.g., overloading of IT system ignites a fire and leads to physical damage)	☐	☐	☐	☐	☐
Benefits of risk pooling are impaired (e.g., due to relatively small insurance portfolios)	☐	☐	☐	☐	☐
Pricing uncertainty for cyber risk is greater relative to other lines of business (i.e., uncertainty with respect to data)	☐	☐	☐	☐	☐
Uncertainty in modeling approaches (i.e., no actuarial standards)	☐	☐	☐	☐	☐
Risk of change (i.e., historical data is not necessarily a good predictor for future losses)	☐	☐	☐	☐	☐
Extreme scenarios are difficult to estimate (i.e., low frequency, high severity)	☐	☐	☐	☐	☐
Insurance capacity is limited leading to high deductibles and low cover limits	☐	☐	☐	☐	☐
Presence of moral hazard (i.e., policyholders' change of behavior after purchasing)	☐	☐	☐	☐	☐

d. Do you see any further problems with respect to the insurability of cyber risks?

II. What can we do to improve the insurability of cyber risk?

The discussions with market participants illustrate the increasing interest in the topic of cyber risk and show that insurance and reinsurance companies would be willing to enter a cyber insurance market, if particular problems concerning the insurability of cyber risk were solved.

a. In your opinion, what are the biggest levers to improve the insurability of cyber risk?

b. How do you evaluate the following activities to improve the insurability of cyber risk?

(1: Not helpful, 5: Very helpful)	1	2	3	4	5
Develop regulatory requirements (e.g., a global standard for cyber risk assessment and mitigation; intensification of penalties)	☐	☐	☐	☐	☐
Develop platforms to increase data availability/data exchange for cyber risk incidents	☐	☐	☐	☐	☐
Develop innovative ways to manage cyber risks	☐	☐	☐	☐	☐
Develop insurance products and (re)insurance markets to cover cyber risks	☐	☐	☐	☐	☐
Develop public and/or private cyber insurance pools (i.e., a collaboration between primary insurers (and reinsurers) to create a wider actuarial foundation for particularly high and unbalanced risks)	☐	☐	☐	☐	☐
Implementation of reporting obligations for cyber risk incidents	☐	☐	☐	☐	☐
Promote the introduction of capital market solutions (e.g., ILS) for cyber risk	☐	☐	☐	☐	☐
Active risk transfer by the government (e.g., state as a primary insurer, or as reinsurer of last resort)	☐	☐	☐	☐	☐

c. Do you have any further ideas or thoughts on how to improve the insurability of cyber risk?

III. Other comments

Feel free to leave us any feedback or comments on this survey:

If you are interested in receiving a copy of this study, please note your address (email or mail address) here or on a separate sheet to ensure anonymity.

Thank you very much for your participation!

About the Authors

Prof. Dr. Martin Eling

Martin Eling has studied business administration at the University of Münster (Germany), where he also received his doctoral degree in 2005. From 2005 to 2009, he worked as a postdoc at the Institute of Insurance Economics of the University of St. Gallen, where he also received his Habilitation in 2009. In 2008 he was Visiting Professor at the University of Wisconsin-Madison (USA) and in 2010 and 2011 Visiting Lecturer at the University of Torino and University of Urbino (Italy). From 2009 to 2011 he was Director of the Institute of Insurance and Professor in Insurance at the University of Ulm (Germany). Since November 2011 he has been professor of insurance management and director of the Institute of Insurance Economics at the University of St. Gallen.

martin.eling@unisg.ch

Jan Hendrik Wirfs

Jan Hendrik Wirfs holds a diploma in mathematics and economics from the University of Ulm (Germany) as well as a M.Sc. in mathematics from the University of Wisconsin – Milwaukee (USA). Jan Hendrik has been project manager and research assistant at the Institute of Insurance Economics (I.VW-HSG) at the University of St. Gallen since 2013. He is also working toward his Ph.D. at the Chair of Insurance Economics, which he expects to complete in mid-2016. His main research work includes topics in cyber risk. In his work he discusses impediments to the insurability of cyber risk and analyzes the adequacy of potential risk transfer schemes. Due to his actuarial background, he as well focuses on cyber risk loss modeling. Further research interest of Jan Hendrik is the performance measurement in the insurance industry.

jan.wirfs@unisg.ch

Management Summary

Cyber risk is an increasingly important, but under-researched topic. Moreover, the cyber insurance market is very small and its development has been hampered by problems of insurability. Some market participants claim that cyber risks present such a danger to global business that insurance pools are needed or even that governments need to step in to cover the risks. Does this mean that cyber risks are too big to insure? This study is the first systematic discussion of potential risk transfer options for cyber risks. We compare several risk transfer options, including insurance, reinsurance and alternative risk transfer. Moreover, we discuss the potential role of the government and the capacity of insurance pools to improve insurability. On the methodological side, we rely on both qualitative and quantitative analyses to justify our conclusions. We use Berliner's insurability framework and expected utility analysis of different cyber specific scenarios. We then compare our theoretical findings with the opinions of market participants in an empirical study. Our main conclusion is that cyber risks «of daily life» are not too big to insure. We show that the broader use of reinsurance would help to improve insurability. An insurance pool might also be useful to generate common knowledge, establish standards, and improve diversification. In contrast, «extreme scenarios» (e.g., a breakdown of the critical infrastructure) are difficult to insure, especially given the lack of data, cumulative risk, and other problems of insurability. A discussion between the government and the industry regarding those extreme scenarios seems useful. Both need a strategy for treating extreme scenarios, which – as we show empirically – are not unlikely to materialize in the next ten years. We discuss minimum standards for self-protection and reporting obligations for cyber incidents as measures in this context. Consequently, we call for a two-tier approach to improve the insurability of cyber risks: First, we recommend improving the insurability for cyber risks «of daily life» by a within-industry collaboration. Second, we propose improving the insurability for «extreme scenarios» by integrating the government in various ways. Insurability should be an aspect of any national strategy against increasingly serious cyber threats.

Highlights

Institute of Insurance Economics

University of St.Gallen

Institute of Insurance Economics
University of St. Gallen (I·VW-HSG)
Tannenstrasse 19
9000 St. Gallen / Schweiz
www.ivw.unisg.ch