School of Finance

University of St.Gallen

INSURABILITY OF CYBER RISK: AN EMPIRICAL ANALYSIS

CHRISTIAN BIENER
MARTIN ELING
JAN HENDRIK WIRFS

WORKING PAPERS ON FINANCE NO. 2015/3

INSTITUTE OF INSURANCE ECONOMICS (I.VW-HSG)

JANUARY 2015

Insurability of Cyber Risk: An Empirical Analysis

Christian Biener, Martin Eling, Jan Hendrik Wirfs*

Abstract

This paper discusses the adequacy of insurance for managing cyber risk. To this end, we extract 994 cases of cyber losses from an operational risk database and analyze their statistical properties. Based on the empirical results and recent literature, we investigate the insurability of cyber risk by systematically reviewing the set of criteria introduced by Berliner (1982). Our findings emphasize the distinct characteristics of cyber risks compared to other operational risks and bring to light significant problems resulting from highly interrelated losses, lack of data, and severe information asymmetries. These problems hinder the development of a sustainable cyber insurance market. We finish by discussing how cyber risk exposure may be better managed and make several suggestions for future research.

Keywords: Cyber risk, cyber insurance, operational risk, insurability

1 Introduction

Every reported incident of data breach or system failure resulting in high financial or reputational loss increases decision maker awareness that current insurance policies do not adequately cover cyber risks. There are many examples of the high economic and social importance of cyber risk.[1] Insurance is seen as one possibility for managing cyber risk exposure.[2] However, the market lags behind the expectations for this potentially huge new

* Christian Biener (christian.biener@unisg.ch), Martin Eling (martin.eling@unisg.ch), and Jan Hendrik Wirfs (jan.wirfs@unisg.ch) are all with the Institute of Insurance Economics at the University of St. Gallen, Rosenbergstrasse 22, 9000 St. Gallen, Switzerland. This paper has been granted the 2014 Shin Research Excellence Award – a partnership between The Geneva Association and the International Insurance Society – for its academic quality and relevance by decision of a panel of judges comprising both business and academic insurance specialists.

1 See, e.g., the Bank of England's current annual systemic risk survey, the WEF Global Risk Landscape, and articles on well-known cyber risk incidents (NSA, Sony, LGT etc.). Recently, the G-20 group denoted cyber attacks as a threat to the global economy; see Ackerman (2013). Both in probability of occurrence and potential severity cyber risks and the failure of critical information infrastructure are one of the top five global risks. More specifically, the World Economic Forum (2014) estimates the probability of a critical information infrastructure breakdown with 10% and the financial consequences after a few days to about US$ 250 billion.

2 Cyber insurance is often discussed as a big market opportunity because of the public's high awareness of cyber risk and its increasing exposure to it (see Betterley, 2010).

line of business.[3] We discuss the adequacy of insurance in managing cyber risk. To this end, we rely on a new, comprehensive cyber risk database, analyze statistical properties, and discuss the insurability of cyber risk. In the empirical part of the paper, we extract cyber risk data from an operational risk database.

In spite of its increasing relevance for businesses today, research on cyber risk is fairly limited. A few papers can be found in the technology domain, but almost no research has been done in the risk and insurance domain.[4] The aim of this paper is to close this research gap in the risk and insurance economics literature and encourage future research on this new and important topic. For this purpose, we provide the first systematic discussion of cyber risk insurability.[5] Moreover, to our knowledge we are the first to provide an empirical analysis of individual cyber risk by using data on operational risk.[6]

The remainder of this paper is structured as follows. In Section 2 we define the term "cyber risk" and provide an overview of existing insurance solutions. In Section 3 we introduce our data and methodology. Then, in Section 4 the empirical analysis is presented and the insurability of cyber risk is discussed. We conclude in Section 5.

2 Definition and Market Overview

2.1 Definition

The term "cyber risk" refers to a multitude of different sources of risk affecting the information and technology assets of a firm. Some prominent examples of cyber risk are outlined by the National Association of Insurance Commissioners[7] and include identity theft, disclosure of sensitive information, and business interruption. Many attempts have been made to define "cyber risk". Some of these employ rather narrow concepts; for example, Mukhopadhyay et al. refer to cyber risk as the risk involved with malicious electronic events

---

[3] The market coverage (the percent of companies that have bought cyber insurance) is estimated between 6% and 10%. See Willis (2013a, b), for the United States, and Marsh (2013), for Europe.

[4] In Appendix B, we present all existing articles on cyber insurance and outline their contributions. Many 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). In short, the extant literature tends to highlight aspects of the insurability of cyber risks; our discussion of insurability is thus based on own data and on a review of this literature.

[5] Haas and Hofmann (2013) discuss risk management and the insurability of cloud computing from an enterprise risk management perspective; in contrast to this paper, they consider only a subsection of the cyber risk landscape, do not use empirical data, and do not systemically review Berliner's (1982) criteria.

[6] To see how our data analysis and literature review compares with practical "real-world" experience, we also conducted interviews with providers and potential buyers of cyber insurance and embed these in the insurability discussion.

[7] See NAIC (2013).

that cause disruption of business and monetary loss.[8] Others take a broader perspective by defining it as information security risk[9] or risk resulting in failure of information systems.[10]

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.[11] The definition of cyber risk we employ here is a broad one and 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 integrity of information or information systems".[12] Following the operational risk frameworks in Basel II[13] and Solvency II[14], we categorize cyber risk into four classes: (1) actions of people, (2) systems and technology failures, (3) failed internal processes, and (4) external events.[15] The categorization is presented in Table 1.

---

8 See Mukhopadhyay et al. (2005, 2013).
9 See Ögüt, Raghunathan, and Menon (2011).
10 See, e.g., Böhme and Kataria (2006).
11 See GCHQ (2012).
12 See Cebula and Young (2010).
13 See BIS (2006).
14 See CEIOPS (2009).
15 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 are included in our discussion.

Table 1 Categories of cyber risk (see 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 Catastrophes	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 dependencies	risks arising from the organization's dependence on external parties	utilities, emergency services, fuel, and transportation

Empirical information on cyber risk is relatively limited. One of the few fields that is well documented is data breach for which the Ponemon Institute annually provides cross-country and cross-industry information.[16] It finds that security and data breaches resulted in an average financial impact of US$ 9.4 million in 2013 and expect that number to increase significantly in the coming years.[17] McAfee estimates the global economic impact of cyber crime and cyber espionage at US$ 300 billion to US$ 1 trillion.[18] A report prepared for the World Economic Forum estimates total economic losses from cyber crime in 2009 in the

[16] See Ponemon Institute (2013a, b).

[17] In addition, the study by NetDiligence (2013) looks at data breach claims from 2010-2012 reported by companies with cyber-liability insurance. Submitted claims range from US$ 2,500 to US$ 20 million, while the average claim payouts amount to US$ 1 million. If it is assumed that, at a minimum, the self-insured retention is met, average claim payouts would increase to US$ 3.5 million. These average numbers are lower than in Ponemon Institute (2013b), which is due to a much smaller subset of all breaches and because NetDiligence (2013) focus on actual claim payouts rather than expenses incurred.

[18] See McAfee (2013).

United States alone at more than US$ 500 million.[19] There are a few other studies that provide more technical data, specific for some countries or type of cyber risk (e.g., cyber attacks).[20] Almost all data published in the sphere of cyber risk provide only broad indications of total cyber risk in that they deal in averages for specific market segments. In this study, we try to expand this knowledge on cyber risk characteristics by looking at individual cyber risks (see Section 3).[21]

2.2 Market Overview

Commercial property and liability insurance is available in most insurance markets worldwide. However, property policies typically only cover damage to physical assets such as production facilities, and exclude cyber risk, as is generally the case with liability policies, too. 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 relatively small. Moreover, outside the United States, insurance coverage for cyber risk is not well known and not much 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.[22] 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.[23] According to Betterley, current annual gross premiums for cyber insurance in the United States are US$ 1.3 billion and growing 10–25% on average per year.[24] Continental Europe is estimated to generate premiums of only around US$ 192 million, but this figure is expected to reach US$ 1.1 billion in 2018.[25]

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 between competitors.

---

19 See World Economic Forum (2012).

20 Among these are the annually published Computer Crime and Security Survey (Computer Security Institute, 2014), the annually Cyber Liability & Data Breach Insurance Claims Study (NetDiligence, 2013), the monthly Internet Security Threat Report (Symantec, 2014), the monthly Cyber Attack Statistics (Hackmageddon, 2014), and several studies by the KPMG Forensic Services (see KPMG, 2013). Furthermore, the annually published Global Corporate IT Security Risks Study (Kaspersky Lab, 2013) has a special focus on key IT security issues and cyber-threats which worry businesses.

21 There is an overlap not only between operational risk and cyber risk, but also between IT risk and cyber risk. IT risk traditionally focuses primarily on physical assets such as hardware, while cyber risk focuses on digital information (see Haas and Hofmann, 2013). Nevertheless, much can be learned about risk management not only from operational risk, but also from IT risk, which has been a topic of research for several decades.

22 See Marsh (2013).

23 See Willis (2013b). 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%.

24 See Betterley (2013).

25 See NAIC (2013).

Another unique 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.[26] Table 2 outlines typical cyber insurance policies.[27]

Table 2 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 the Fortune 500 companies by Willis, companies are most concerned with the loss of confidential data (68%), loss of reputation (42%), malicious acts (49%), and liability (41%).[28] This ranking matches that found in a study of European companies conducted by Marsh. Available cyber risk policies thus seem to address the most pressing needs.[29] However, if the available products are a good solution to extant business problems, why is market coverage so low? There are several answers to this question, including

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

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

[28] See Willis (2013a).

[29] See Marsh (2013).

expensive premiums, ambiguous coverage, and the information asymmetries inherent in cyber risk, all of which will be discussed in detail below.

3 Data and Methodology

3.1 Data

Cyber Risk Data

For our empirical analysis of cyber risk we rely on the dataset used in Hess—the SAS OpRisk Global Data—which is the world's largest collection of publicly reported operational losses.[30] The database consists of 22,075 incidents of operational loss that were reported between March 1971 and September 2009. The incidents occurred all over the world and each loss is categorized in accordance with the Basel II event and effect classification standard.[31] Furthermore, all observations are partitioned into business and subbusiness lines, such that an extensive analysis at the subbusiness-line level is possible. All losses are adjusted by currency and a consumer price index so as to make them comparable. The dataset attempts to provide an estimate of the complete costs of operational risk events (both direct as well as 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 the cause of the cyber risk incident (e.g., hackers, employees, system, nature), and (3) a relevant *outcome* such as the loss of data or misuse of confidential data needs to be present. 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 (see Appendix A for more details). The resulting dataset includes a total of 994 cyber risk incidents, or about 4.5% of the total sample of operational risks.

Literature Review

We reviewed studies on cyber risk that were published between 2003 and early 2014 and that specifically mentioned aspects of its insurability. To capture all relevant references and ensure that only studies meeting academic quality standards were included in the survey, we

[30] See Hess (2011).
[31] See BIS (2006).

followed a strict search and selection strategy.[32] This strategy resulted in the identification of 19 academic papers and six industry studies (see Appendix B).[33]

3.2 Methodology

Berliner introduced a simple, yet stringent and comprehensive, approach for differentiating between insurable and uninsurable risks.[34] This approach, which is based on nine insurability criteria, is frequently used to analyze insurance markets and products.[35] The criteria are categorized into three broad categories that classify risks in terms of actuarial, market, and societal conditions (see Table 3).

Qualifying as insurable in the actuarial category requires independence of risks and reliable estimation of loss probabilities (randomness of loss occurrence), manageable maximum possible losses per event in terms of insurer solvency (maximum possible loss), moderate average loss amounts per event (average loss per event), a sufficiently high number of loss events per annum (loss exposure), and no excessive information asymmetry problems (i.e., moral hazard, adverse selection). The actuarial criteria include the law of large numbers, which is a central paradigm in insurance economics and, briefly stated, means that the larger the number of mutually independent and identically distributed risks in a risk pool, the lower the variance of losses in the risk pool.

Table 3 Insurability criteria and related requirements according to Berliner

Insurability Criteria			**Requirements**
Actuarial	(1)	Randomness of loss occurrence	Independence and predictability of loss exposures
	(2)	Maximum possible loss	Manageable
	(3)	Average loss per event	Moderate
	(4)	Loss exposure	Loss exposure must be large
	(5)	Information asymmetry	Moral hazard and adverse selection not excessive
Market	(6)	Insurance premium	Cost recovery and affordable
	(7)	Cover limits	Acceptable
Societal	(8)	Public policy	Consistent with societal value
	(9)	Legal restrictions	Allow the coverage

Market criteria relate to the adequacy of insurance premiums to provide a sufficient return on capital for the insurer, yet be affordable by the target population, as well as to the

[32] A detailed description of the search strategy is available from the authors upon request.

[33] Seven trade journal articles on cyber insurance and 13 industry studies on cyber risk are included as well (see Appendix B). The industry studies do not discuss cyber insurance, but the data and information on cyber risk provided therein are useful for our discussion of insurability. Moreover, we conducted interviews with four cyber insurance providers (AIG, Allianz, Chubb, Zurich) and 16 (potential) buyers of cyber insurance from the financial services sector. These interviews are helpful in discovering whether our data analysis and literature review results comport with practical experience such as, e.g., actual cover limits. Twenty-five percent of the 16 persons interviewed already have cyber insurance.

[34] See Berliner (1982).

[35] See, e.g., Biener and Eling (2012), Doherty (1991), Jaffee and Russell (1997), Janssen (2000), Karten (1997), Nierhaus (1986), Schmit (1986), and Vermaat (1995).

acceptability of policy cover limits for the target population. A suitable insurance premium is comprised of the pure risk premium covering expected losses, safety loadings for process and parameter risk (to account for fluctuations of expected losses and the uncertainty in the estimation), and an expense loading for underwriting expenses. For the insurer to achieve a certain security level and, at the same time, provide a valuable product, cover limits are important and sometimes necessary to make a risk insurable.

To meet the societal criteria, coverage is required to be in accordance with public policy and societal values and with the legal restrictions governing coverage. Compliance with the public policy criterion includes, among others, not issuing insurance policies for trivial risks and making sure that policies provide no incentive for criminal actions. Legal restrictions involve the types of activities an insurance company is permitted to engage in and prohibitions against insuring certain risks. The stability of the legal framework in a particular country is another important condition that must be met to make a risk insurable.

4 Analysis

4.1 Data Analysis

Cyber Risk Data

Table 4 provides a summary of the cyber risk sample and compares its characteristics with 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.[36] The maximal loss in our sample is US$ 13 billion compared to US$ 89 billion for non-cyber risk.[37] Thus, both on average as well as in extreme cases, the loss amounts for cyber risk are much smaller than for other operational risks.[38]

[36] Mean and median are close to estimations of average losses found in the literature; Ponemon Institute (2013b) 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).

[37] The largest cyber risk case occurred at the Bank of China in February 2005 when US$ 13,313.51 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 U.S. tobacco company Philip Morris, which, in November 2001, was ordered to pay US$ 89,143.99 million in punitive damages to sick smokers.

[38] Cyber risk policies typically cover a maximum such as, e.g., 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.

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	994	40.53	443.88	0.10	0.56	1.87	7.72	89.56	676.88	13,313
Non-Cyber Risk	21,081	99.65	1,160.17	0.10	1.88	6.20	25.37	248.97	1,595.27	89,143
Panel B: Cyber risk subcategories										
Actions of people	903	40.69	463.25	0.10	0.55	1.83	6.87	84.36	679.04	13,313
Systems and technical failure	37	29.07	77.33	0.10	1.10	5.03	11.65	168.95	329.04	370
Failed internal processes	41	47.72	205.92	0.14	0.42	2.04	9.05	158.65	743.40	1,311
External events	13	39.40	115.73	0.28	0.56	1.03	13.77	192.88	422.71	422

Sorting into cyber risk subcategories (Panel B of Table 4) shows 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 risk, while the other categories, such as external disasters, are very rare. The average losses across the different subcategories, however, are relatively similar.

To more closely analyze the distributional characteristics of cyber risk compared to other operational risk, we follow Hess and estimate the loss severity distribution (see Appendix C).[39] The estimation is conducted by means of a spliced distribution, where a generalized Pareto distribution (GPD) models the tail. The results show that distribution of cyber risk differs considerably from the distribution of other operational risk. For example, the distribution of the non-cyber risk sample is much heavier tailed than that of the cyber risk sample, explaining in part the much higher maximal losses in these categories.[40] This finding implies that when modeling operational risk, cyber risk needs to be considered separately.[41]

Table 5 further separates the cyber and non-cyber risk loss data into several subcategories. The geographic separation (Panel A) shows that Northern American companies experience more than twice as many (51.9%) cyber risk incidents than European firms (23.2%) and even more than twice as many as firms located on other continents. For loss severity, we find that Northern America has some of the lowest mean cyber risk and non-cyber risk losses, whereas Europe and Asia have much higher average losses. This situation may be due to North American firms being more capable of and willing to invest in risk mitigating measures for

[39] See Hess (2011).

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

[41] 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.

extreme losses, which results from a longer tradition of recognizing and managing cyber risks as compared to Europe or Asia.

Panel B of Table 5 provides a separation into financial services and nonfinancial services industries. For cyber risk, 78.6% of all incidents occur in the financial services industry. This is not surprising since financial services firms, such as banks and insurance firms, store a significant amount of critical personal data.[42] However, the average loss resulting from cyber risk for firms in nonfinancial services industries is about twice as high as for financial services firms. This finding might be explained by the fact that financial services firms have a higher awareness regarding critical data and better protect against severe losses from cyber risk. For non-cyber risks, firms in the nonfinancial services industries face higher average losses than firms in the financial services sector; however, the difference is not as substantial as it is for cyber risk.

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	19	1.91%	38.99	3.20	165	0.78%	74.47	3.11
Asia	180	18.11%	122.18	2.63	2,284	10.83%	161.97	5.71
Europe	231	23.24%	28.06	1.85	3,931	18.65%	132.75	6.35
North America	516	51.91%	19.86	1.68	14,126	67.01%	81.11	6.30
Other	48	4.83%	17.18	1.38	359	1.73%	88.34	5.93
Panel B: Industry								
Nonfinancial	213	21.40%	61.74	5.00	12,697	60.20%	105.29	7.33
Financial	781	78.60%	34.75	1.44	8,384	39.80%	91.10	4.49
Panel C: Relation to losses in other firms								
One firm affected	827	83.20%	44.51	1.83	15,804	74.97%	92.62	6.20
Multiple firms affected	167	16.80%	20.84	2.04	5,277	25.03%	120.71	6.20
Panel D: Company size by number of employees[*]								
Small	40	4.02%	27.81	1.30	443	2.10%	51.30	2.22
Medium	51	5.13%	10.33	1.33	800	3.79%	26.81	2.50
Large	754	75.86%	46.39	1.50	14,019	66.50%	124.94	6.88

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

An important aspect of cyber risk is contagion, and thus our next separation of the data is between incidents affecting only one single firm and those affecting multiple firms (Panel C of Table 5). If just one firm is involved (83.2% 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 more than one firm is affected, cyber attacks

[42] Our market survey of potential customers in the financial services industry 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.

are identified earlier and thus losses can be limited. Also, there may be economies of scale in solving the problems created by cyber incidents when multiple firms are involved (e.g., forensic investigation costs).[43]

Panel D of Table 5 separates the sample based on firm size. With increasing size, the number of incidents increases, i.e., 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.[44] It may be that smaller firms do not have the awareness and resources to protect against cyber risk, while large firms have diseconomies of scale due to complexity.[45]

4.2 Analysis of Insurability

4.2.1 Actuarial Criteria

(1) Randomness of Loss Occurrence

A central requirement for providing insurance against a specific risk is independence of risks. Following the law of large numbers, the larger the number of mutually independent risks in the insurance pool, the more likely it is that average aggregate losses correspond to expected losses, thus allowing for decreasing safety loadings.[46] The independence condition is thus an important precondition to insuring any type of risk. In the case of cyber risk, several authors find this principal assumption to be violated. Baer and Parkinson argue that existing cyber systems are designed in a similar way and consequently vulnerable to the same incidents, which justifies the hypothesis that incidents may be highly correlated between firms (e.g., DDoS).[47] Several other works also acknowledge the correlated nature of cyber risks.[48] Our empirical analysis shows that in 16.8% of the incidents, losses are related to a loss in another firm. In other words, most cyber risk incidents in our sample are *not* correlated with other cases. It is important to note that correlation does not necessarily occur in all categories of

---

[43] Correcting for outliers (i.e., deleting the 10 highest losses in each subsample), we obtain the same result (average (median) loss for one firm involved of US$ 15.63 (1.77) million and for the case with multiple firms involved US$ 6.77 (1.93) million). We also analyzed the intra-year pattern of cyber risk incidents in order to identify potential concentrations within a year. No intra-year pattern could be identified.

[44] 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.

[45] We also analyzed the development of cyber risks over time and found that the number of cyber risk incidents was relatively 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. 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.

[46] See, e.g., Böhme (2005), Biener (2013).

[47] See Baer and Parkinson (2007).

[48] See, e.g., Haas and Hofmann (2013), Hofmann and Ramaj (2011), Ögüt, Raghunathan, and Menon (2011), Bolot and Lelarge (2009).

cyber risk, such that randomness must be viewed in the context of the actual incident (e.g., physical data theft).

In addition to the correlation issue, pooling of risk could be hindered by the fact that cyber risk portfolios are not large enough, i.e., there are too few contracts, thus resulting in less than optimal diversification. In a related vein, ENISA notes a lack of adequate reinsurance for cyber risks.[49] The development of a viable cyber insurance market could thus benefit from increasing reinsurance capacity for those risks.

When it comes to pricing cyber risk, a principal problem is the scarcity of data.[50] Regardless of how accurate and sophisticated cyber risk modeling becomes, if there are no data to test the models against, the models will not be of much use.[51] Bandyopadhyay, Vijay, and Rao also note that insurers are perceived to have little to no information advantage over individual firms.[52] Insurers react to the high level of uncertainty regarding average losses from cyber incidents by setting high deductibles and low maximum coverage, resulting in insurance policies that are of little value to risk managers. One obvious option to react to data scarcity is to systematically collect empirical data on cyber risk incidents and insurance claims. Insurers could either combine resource and exchange data on a multilateral basis as is done, e.g., with operational risks in banking or alternatively regulators could provide a common platform for data sharing. The rate advisory organizations that exist, for example, in the form of the Insurance Services Organization (ISO) in the United States could provide a starting template. Government involvement may even be more feasible in the case of cyber risk for several reasons. One is the infancy of the industry that impedes the development of an independent organization for this function. A second relates to the fact that governments can require data reporting whereas independent insurers cannot. A third reason is that government schemes should be more closely aligned with public interests than would be an independent entity.

Another problem in insuring cyber risk is that the risk changes, sometimes suddenly and drastically, i.e., the risk is dynamic due to technical progress and the use of novel systems and devices.[53] An analysis of historical cyber risk data thus could be misleading if the nature of the underlying risk has undergone substantive change.[54] Another challenge to the randomness

---

[49] See ENISA (2012).

[50] See Herath and Herath (2011), Gordon, Loeb, and Sohail (2003), Baer and Parkinson (2007), ENISA (2012).

[51] Other authors also acknowledge the data scarcity issue in cyber insurance as a potential barrier to market development (see, e.g., Department of Homeland Security, 2012, Shackelford, 2012; Betterley, 2010); Chabrow (2012) nails the problem on its head: "Cyber insurance remains a gamble to insurance companies; if it's a gamble for them, it's a gamble for you."

[52] See Bandyopadhyay, Vijay, and Rao (2009).

[53] See, e.g., Haas and Hofmann (2013), ENISA (2012).

[54] Healey (2013) shows that past cyber incidents have either been widespread or prolonged, but not both. There are, however, arguments for an increase in the likelihood of such "rare" events and thus dynamic changes in

assumption is the possibility of massive regulatory intervention altering the rules applicable to insuring those losses. There are concerns in the market regarding changes in laws and regulation that may significantly alter corporate risk management strategies and losses insured under a cyber risk policy, thus posing additional risk to insurers.[55] Regular industry surveys may well capture the dynamic changes affecting the cyber insurance market.

(2) Maximum Possible Loss

This criterion is satisfied if the maximum possible loss per event is manageable in terms of insurer solvency. Maximal historical losses in cyber risk are significantly lower than those of general operational risks (see Table 4). Moreover, insurers protect themselves with coverage limits. Maximum possible losses from cyber risk thus appear to be manageable.

(3) Average Loss per Event

The Ponemon Institute finds that security and data breaches result in an average financial impact of US$ 9.4 million.[56] KPMG estimates average losses from theft of data at US$ 2.1 million.[57] According to Kaspersky Lab a successful targeted attack on a large company's IT infrastructure can cost US$ 2.4 million.[58] The estimates in the empirical part of this paper are comparable. We also show that the mean and median losses are much lower than for other operational risk and that they have been on the decrease during the last several years. Moreover, the average loss in the financial services industry is much smaller than in other industries, which might be due to higher awareness and more resources devoted to self-protection.[59]

Regarding size, we observe a U-shaped relation, i.e., smaller and larger firms have higher costs than medium-sized. Possibly, smaller firms are less aware of and less able to deal with cyber risk, while large firms may suffer from complexity. 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

---

cyber risk characteristics. In particular, systems are complex and consequences of interventions are often not easily understood; the interconnectedness of cyber systems involves the risk of shock transmission; the common-mode functionality of cyber system elements leads to shocks affecting multiple elements of the system simultaneously; a lack of incentives for increasing cyber security (e.g., for IT producers) results in an underinvestment in cyber security, increasing connectivity of physical assets to the cyberspace increases the potential impact and thus attractiveness of manipulating cyber systems (see Zurich, 2014).

55 See, e.g., Haas and Hofmann (2013), Gatzlaff and McCullough (2012).

56 See Ponemon Institute (2013b).

57 See KPMG (2013).

58 See Kaspersky Lab (2013).

59 Moreover, we observe that the average loss also depends on region; for instance, firms located in North America have lower average losses than do firms on other continents, which might be due to the North American firms having more experience in identifying and managing cyber losses. Thus, if it turns out that increased experience decreases loss, the criterion of insurability will with time become even easier to satisfy.

firms without strategic security leadership).[60] The institutional commitment demonstrated by having a person responsible for information security thus affects the average loss per event. The average loss per event thus depends on size, effective self-protection, and institutional commitment. Overall, however, we do not see this criterion as an obstacle to cyber insurance.

(4) Loss Exposure

We find an increasing number of cyber risk events over time. The frequency, however, is highly dependent on the event category. As indicated by our empirical results, actions of people is much more frequently found to be culpable than anything else, e.g., natural catastrophes are a very rare source of cyber risk. Furthermore, the loss exposure depends on industry (financial firms have higher exposure) and size (larger firms have higher exposure). In general, this criterion appears to be unproblematic.

(5) Information Asymmetry

Moral hazard and adverse selection are often viewed as primary impediments to market development. Moral hazard results from the insured's lack of incentive to take self-protective measures that would reduce the probability of loss or the size of a loss once it happened subsequent to purchasing insurance.[61] The complex interrelations of modern information systems result in significant vulnerability to cyber risk even though single firms invest in cyber risk self-protective measures. Thus, investments in cyber security exhibit a public good character with positive externalities.[62] Consequently, there is a coordination problem; the utility of cyber security investment by one firm depends on the cyber security investment by all other firms. The interrelated nature of information systems also makes it difficult to discover, much less prove, sources of losses and identity of perpetrators, which potentially increases a firms' reluctance to invest in self-protective measures.[63]

In the extant cyber insurance literature, there is some evidence that firms that have experienced a cyber attack are more likely to purchase insurance, resulting in adverse selection.[64] Furthermore, the lack of data on cyber losses makes it difficult to sort firms into different risk types, thus amplifying adverse selection.[65] Moreover, the works by Majuca, Yurcik, and Kesan, Ögüt, Raghunathan, and Menon, and Shetty, Felegyhazi, and Walrand

---

60 See Shackelford (2012).

61 See Gordon, Loeb, and Sohail (2003).

62 See Baer and Parkinson, 2007; Cylinder (2008).

63 See Ögüt, Raghunathan, and Menon (2011). To mitigate potential moral hazard problems, classical solutions such as deductibles and the introduction of premium reduction systems are discussed (see Gordon, Loeb, and Sohail, 2003). In addition, Baer and Parkinson (2007) suggest regular risk assessments that allow linking coverage to a certain minimum standard of cyber security. Shackelford (2012) suggests monetary incentives for self-protective measures analogous to a safe driving discount in motor insurance.

64 See Shackelford (2012).

65 See ENISA (2012).

suggest significant information asymmetry problems in cyber insurance.[66] However, to date, there is no empirical support for the adverse selection hypothesis.[67]

4.2.2 Market Criteria

(6) Insurance Premium

Cyber insurance policies are often described as costly and far from fairly priced.[68] There are at least four reasons for this: (1) the novelty of the product and thus the small size of risk pools; (2) the novelty of the product and thus the small number of market participants (limited availability); (3) the novelty of the product and limited data in regard thereto, making large risk loadings necessary, and (4) significant information asymmetries that require costly state verification and upfront risk assessment.

According to Betterley, premiums for cyber insurance are currently high, especially for small and medium-sized companies, but relatively moderate considering the large uncertainties involved.[69] Shackelford expects premium prices to decline with expanding and more competitive markets.[70] This expectation is supported by recent market developments in the United States where new players entering the market induced slight premium decreases.[71] Consumers of cyber insurance, according to the Ponemon study, confirm that cyber insurance premiums are not exceptionally high.[72] In a survey of 638 cyber risk specialists in U.S. firms, 62% considered premiums to be "fair"; only 29% indicated that premiums are too high.

Compared to traditional property/liability insurance, however, there are additional costs associated with cyber insurance that must be covered. For example, there may be high upfront costs for assessing company risk (e.g., network security). Insurers demand those assessments and often additional information about past incidents before they will even offer a policy.

---

66 See Majuca, Yurcik, and Kesan (2006), Ögüt, Raghunathan, and Menon (2011), and Shetty, Felegyhazi, and Walrand (2010).

67 Screening, self-selection, and signaling can be used to address adverse selection issues. Gordon, Loeb, and Sohail (2003) suggest information security audits and premium differentiations for proper risk type selection. Similarly, Baer and Parkinson (2007) recommend intense examinations of firm's IT and security processes. Majuca, Yurcik, and Kesan (2006) discuss potential underwriting questions (i.e., self-selection) that should be assessed to alleviate adverse selection issues before an extensive physical review process is conducted. Another type of signaling could be a certification of the data security following ISO standards; in general, there is a lack of exchange of best practices in cyber risk management that inhibits identification of dominant strategies for tackling cyber risk (see ENISA, 2012).

68 Mukhopadhyay et al. (2005, 2006, 2013) apply the collective risk model in conjunction with expected utility theory to make judgments about the theoretical value of cyber insurance to firms with different levels of risk aversion. They find that with increasing risk aversion, firms will accept fairly priced cyber insurance over no insurance. This finding is rather obvious in light of insurance economics, but it does provide a starting point for the discussion of premiums in our context.

69 See Betterley (2013).

70 See Shackelford (2012); Shackelford (2012) also reports large geographic and industry variations; e.g., there are more policies available in the United States than in Europe or in Canada.

71 See Betterley (2013).

72 See Ponemon Institute (2013b).

Acquisition of that information can be a resource-consuming task.[73] The upfront assessment, however, may have positive and valuable side-effects in that it may increase company awareness of cyber risk, potentially increasing self-protective efforts. Indeed, the consulting and risk assessment services that insurance companies provide to firms seem to be a central driver of product value.[74] One of the important economic functions of insurance is to put a price tag on risk and to set incentives for risk-appropriate behavior.

The bottom line of the studies addressing premium adequacy for cyber risk is that cyber insurance premiums can be considered moderate in general; however, they are rather high for small and medium-sized corporations. Trends observed in recent years, however, indicate a decrease of premiums once the market expands and gains experience with cyber losses.

(7) Cover Limits

Cyber risk policies typically cover a maximum loss, but actual coverage limits vary. If we assume a US$ 50 million coverage limit, which is the maximum regular coverage we found for Swiss insurers, 92% of the cases in our data sample would be covered completely by the policy.[75] Whether this amount is acceptable depends on the risk preferences and cyber risk exposure of the individual policyholder. An increase in coverage should be negotiable, but will result in higher premiums.

Policies typically contain several exclusions, e.g., self-inflicted loss, accessing unsecure websites, espionage, and terrorism.[76] Additionally, there might be other indirect effects of cyber losses that cannot be measured and thus are not covered. An example is reputational loss, although some policies do include this type of loss in the coverage. For example, Gatzlaff and McCullough note that insurance often does not cover a large portion of data-breach-related costs, such as losses to reputation and the impact on stock prices;[77] also losses related to trade secrets and propriety information often are not covered.[78]

Another severe problem regarding cover limits is policy complexity. There are a large number of exclusions and the nature of cyber risk is very dynamic so that for the seller and the buyer, there is uncertainty about what the cyber policy actually covers. ENISA notes the lack of clarity as to coverage as one reason companies do not buy cyber insurance;[79] it also notes that

---

[73] For an example of an assessment questionnaire, see Drouin (2004).

[74] See see ENISA (2012).

[75] We compared cyber insurance policies from the four insurers we interviewed (AIG, Allianz, Chubb, and Zurich). Actual cover limits vary between CHF 10 million and CHF 50 million (i.e., US$ 11 million and US$ 55 million). All four insurers emphasize that higher limits are possible, but not preferred by the insurer.

[76] See, e.g., Mukhopadhyay et al. (2005).

[77] See Gatzlaff and McCullough (2012).

[78] See also Wojcik (2012).

[79] See ENISA (2012).

many companies believe that their existing property/liability policies are sufficient to cover cyber risks.[80]

4.2.3 Societal Criteria

(8) Public Policy

The availability of insurance against cyber risks, especially hacking or physical attacks, raises the concern that barriers to committing cyber crime will be lowered or even that such crime will become more attractive. Additionally, insurance fraud might be incentivized, since hacking attacks or physical attacks are difficult to detect and trace back to the perpetrator. Also, firms may have less incentive to engage in self-protection. A reduction in self-protection would increase the overall industry exposure and lead to large losses in social welfare. Indeed, Ögüt, Raghunathan, and Menon find that firms invest less than is socially optimal in self-protection when risks are correlated and loss verification is imperfect.[81] Thus, insurance and self-protection behave as substitutes. However, Kesan, Majuca, and Yurcik find that cyber insurance actually increases investments in cyber security and thus generates positive externalities.[82] These positive effects are mostly due to the facilitation of standards for best practices through specialized insurance firms that assess cyber risk upfront coverage and provide consulting services. Bolot and Lelarge find that a broad use of cyber insurance increases overall Internet security and provides strong incentives to invest in self-protection—a public good with positive externalities.[83]

The latter findings point to a fundamental and unresolved issue regarding the market for cyber security—has cyber security public good characteristics? And if so, should governments intervene to correct for the observed low levels of cyber security? Considering the findings of a positive influence of cyber insurance coverage on cyber security,[84] one solution could be to intervene in the promotion of the cyber insurance market. This aspect regarding the government as an insurer of last resort has been discussed as a solution to a lack of reinsurance capacity.[85] Other mechanisms such as mandatory cyber insurance coverage and subsidies for self-protection could be discussed as well. However, all potential negative externalities from such a massive market intervention need to be considered and balanced with their benefits.

---

[80] The interviewed insurers' response to this problem is to offer a modular product structure where coverage is chosen by the customer; the intensity of the risk assessment then depends on the coverage chosen.

[81] See Ögüt, Raghunathan, and Menon (2011). This result is also supported by Shetty, Felegyhazi, and Walrand (2010).

[82] See Kesan, Majuca, and Yurcik (2004).

[83] See Bolot and Lelarge (2009).

[84] See Kesan, Majuca, and Yurcik (2004) and Bolot and Lelarge (2009).

[85] See ENISA (2012).

(9) Legal Restrictions

Legal restrictions might prevent certain coverage for cyber insurance. For example, in many countries, insuring against regulatory fines is prohibited.[86] Moreover, just recently the European Commission released a proposal for a new data protection and regulation scheme that is expected to come into force in 2014/2015.[87] This new scheme might result in there being additional risks or restrictions that could benefit from insurance coverage. Therefore, the risk of change in regulations and laws is a significant issue for insurers. Also, the general policy conditions need to be adjusted when new regulations come into effect. On the other hand, however, new laws and regulation can drive an increased demand for insurance.[88]

The novelty, complexity, and dynamic nature of cyber risk may pose a legal threat for insurance brokers; an experienced insurance agent or broker will know that an accurate prediction of coverage is not possible and this might limit willingness to offer these products; the result is that only a few specialists will be willing and able to sell cyber insurance. Clearly, this lack of underwriting expertise is not a direct legal restriction, but the legal uncertainty over what will and what will not be considered an insurable cyber risk might have a negative effect on market development.

Finally, the disclosure of necessary information upfront (risk assessment) as well as during the contract (inspections) might be problematic from a data protection point of view. For example, Ouellette notes that hospitals might not be willing to give patient data to a third party.[89]

5 Conclusions

Significant economic impacts from and increasing media attention to cyber risk make managing it imperative. In this context cyber insurance has two virtues. One is that insurance coverage puts a price tag on cyber risk and thus creates incentives for risk-appropriate behavior. The other is that simply by applying for cyber insurance, companies become more aware of and self-protective against this threat. In light of the correlation of risk that occurs in cyberspace, this sort of awareness and behavior exhibit certain public good characteristics.

However, a number of problems with the insurability of cyber risk impede the market development. Table 6 summarizes these in light of the Berliner insurability framework.[90] The main difficulties involve randomness of loss occurrence, information asymmetries, and cover

---

[86] For an international overview, see Barlow Lyde & Gilbert (2007).

[87] See European Commission (2012).

[88] See, e.g., the U.S. Securities and Exchange Commission's (SEC) disclosure guidance on cyber security (SEC, 2011), the U.S. White House Executive Order on cyber security (White House, 2013), and the reform of E.U. data protection laws (European Commission, 2012).

[89] See Ouellette (2012).

[90] See Berliner (1982). An extended version of this table with all references can be found in Appendix B.

limits. However, we are able to conclude on a positive note. With increasing market development, the insurance risk pools will become larger and more data will be available. In addition, we see room for improvement in systematic data collection. Especially platforms for data sharing, organized by national regulators or international associations are worthwhile discussing. In addition, regular industry surveys may capture the dynamic changes affecting the cyber insurance market and provide guidance. A number of new competitors have entered the market in recent years and more are planning to do so. This will increase insurance capacity and market competition and keep prices down. This is also a favorable development in the context of the criticized lack of sufficient reinsurance capacity. In light of our discussion in this paper, it would seem important to establish minimum standards on coverage limits and pre-coverage risk assessment as well as clear-cut definitions of cyber risk, all of which will reduce, if not eliminate, some of the problems of insuring cyber risk. Indeed, the consulting and risk assessment services of insurance companies prior to offering cyber insurance coverage seem to be a central driver of product value, thus increasing demand.

There is a great need for more research on cyber insurance. Lack of data is a problem, however. For example, according to ENISA, there is a lack of empirical evidence as to the strength and maturity of the cyber insurance market.[91] Modeling cyber risk holds a great deal of promise, especially if data become available against which to test the models.[92] Another interesting topic for future research would be discovering approaches that can alleviate the substantial information asymmetry present with cyber risk. Both hidden actions and hidden information will play a role in developing the market further, but exactly how is worth discovering. The interplay of information asymmetries with network effects might be especially interesting in the context of cyber risks, and highly informative not only for the insurance market but for policymakers as well. In this respect, a discussion on potential public good characteristics of cyber security is vital. If the conclusion is that cyber security is a public good and that the market provides insufficient levels of cyber security, government interventions such as mandatory cyber insurance coverage, subsidies for self-protection, or the government as an insurer of last resort could be discussed. However, the potential negative externalities of these market interventions need to be balanced with their benefits.

---

[91] See ENISA (2012).

[92] Seeing that we show that cyber risk is substantially different from other operational risk, it would not be surprising if extant operational risk models turn out to be inappropriate for modeling cyber risks.

Table 6 Assessment of insurability for 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 - 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 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 caps on coverage help reduce moral hazard - Adverse selection poses a strong theoretical threat; upfront risk assessments (screening) and signaling (e.g., ISO certificates) help 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*

References

Ackerman, G. (2013), "G-20 Urged to Treat Cyber-Attacks as Threat to Global Economy," *http://www.bloomberg.com/news/2013-06-13/g-20-urged-to-treat-cyber-attacks-as-threat-to-economy.html*, last accessed: January 18, 2014.

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

Bandyopadhyay, T. M., Vijay, 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," *http://www.bis.org/publ/bcbs128.pdf*, last accessed: December 10, 2013.

Barlow Lyde & Gilbert (2007), "International Comparative Review of Liability Insurance Law," *Insurance Day* May.

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

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

Betterley, R. (2013), "Cyber/Privacy Insurance Market Survey 2013: Carriers Deepen Their Risk Management Services Benefits—Insureds Grow Increasingly Concerned with Coverage Limitations, *http://betterley.com/samples/cpims13_nt.pdf*, last accessed: December 16, 2013.

Biener, C. (2013), "Pricing in Microinsurance Markets," *World Development* 41(1): 132–144.

Biener, C. and Eling, M. (2012), "Insurability in Microinsurance Markets: An Analysis of Problems and Potential Solutions," *Geneva Papers on Risk and Insurance* 37(1): 77–107.

Böhme, R. (2005), "Cyber-Insurance Revisited," Workshop on the Economics of Information Security (WEIS), 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.

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, 269-290.

Cebula, J. J. and Young, L. R. (2010), "A Taxonomy of Operational Cyber Security Risks," Technical Note CMU/SEI-2010-TN-028, CERT 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.

Chabrow, E. (2012), "10 Concerns When Buying Cyber Insurance," *http://www.bankinfosecurity.com/10-concerns-when-buying-cyber-insurance-a-4859/op-1*, last accessed: January 18, 2014.

Computer Security Institute (CSI) (2014), "Computer Crime and Security Survey," *http://gocsi.com/*, last accessed: January 18, 2014.

Cylinder, H. (2008), "Evaluating Cyber Insurance," *CPCU eJournal* 61(14): 1–19.

Department of Homeland Security (2012), "Cybersecurity Insurance Workshop Readout Report," *http://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf*, last accessed: January 17, 2014.

Doherty, N. A. (1991), "The Design of Insurance Contracts When Liability Rules Are Unstable," *Journal of Risk and Insurance* 58(2): 227–246.

Drouin, D. (2004), *Cyber Risk Insurance: A Discourse and Preparatory Guide*. Bethesda, MD: SANS Institute, *http://www.sans.org/reading-room/whitepapers/legal/cyber-risk-insurance-1412*, last accessed: December 19, 2013.

Eling, M. (2012), "Fitting Insurance Claims to Skewed Distributions: Are Skew-Normal and Skew-Student Good Models?" *Insurance: Mathematics and Economics* 51(2): 239–248.
ENISA (2012), "Incentives and Barriers of the Cyber Insurance Market in Europe," *http://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: January 18, 2014.
European Commission (2012), "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)."
Gatzlaff, K. and McCullough, K. A. (2012), "Implications of Privacy Breaches for Insurers," *Journal of Insurance Regulation* 31: 195–214.
Gilli, M. and Käellezi, E. (2006), "An Application of Extreme Value Theory for Measuring Financial Risk," *Computational Economics* 27(1): 1–23.
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," *http://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.
Haas, A. and Hofmann, A. (2013), "Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit," *FZID Discussion Paper*, No. 74-2013.
Hackmageddon (2014), "Cyber Attack Statistics," *http://hackmageddon.com/*, last accessed: January 18, 2014.
Harvard Business Review Analytic Services (2013), *Meeting the Cyber Risk Challenge*. Boston: Harvard Business School Publishing.
Healey, J. (2013), "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012," Vienna, VA: Cyber Conflict Studies Association.
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 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," *Inernational Journal of. Management and Decision Making* 11(5/6): 312–323.
Jaffee, D. M. and Russell, T. (1997), "Catastrophe Insurance, Capital Markets, and Uninsurable Risks," *Journal of Risk and Insurance* 64(2): 205–230.
Janssen, J. (2000), "Implementing the Kyoto Mechanisms: Potential Contributions by Banks and Insurance Companies," *Geneva Papers on Risk and Insurance—Issues and Practice* 25(4): 602–618.
Karten, W. T. (1997), "How to Expand the Limits of Insurability," *Geneva Papers on Risk and Insurance—Issues and Practice* 22(4): 515–522.
Kaspersky Lab (2013), "Global Corporate IT Security Risks: 2013," *http://kasperskycontenthub.com/presscenter/files/2013/10/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf*, last accessed: April 24, 2014.
Kesan, J. P., Majuca, R. P. and Yurcik, W. J. (2004), "The Economic Case for Cyberinsurance," *University of Illinois Law and Economics Working Papers.*
KPMG (2013), "KPMG Forensic Services," *http://www.kpmg.com/CH/de/Library/Articles-Publications/Seiten/e-crime-survey-2013.aspx*, last accessed: January 18, 2014.

Lemos, R. (2010), "Should SMBs Invest in Cyber Risk Insurance?" *http://www.darkreading.com/smb-security/167901073/security/security-management/227400093/index.html*, last accessed: December 19, 2013.

Majuca, R. P., Yurcik, W. and Kesan, J. P. (2006), "The Evolution of Cyberinsurance," *Working Paper*.

Marsh (2012), "Cyber Insurance," *http://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," *https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/partner/Partnerbeitrag_Marsh_Cyber-Risk_Survey.pdf?__blob=publicationFile*, last accessed: December 16, 2013.

McAfee (2013), "The Economic Impact of Cybercrime and Cyber Espionage," *http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf*, last accesses: January 9, 2014.

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," Hawaii International Conference on System Sciences, Hawaii.

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.

National Association of Insurance Commissioners (NAIC) (2013), "Cyber Risk," *http://www.naic.org/cipr_topics/topic_cyber_risk.htm*, last accessed: December 7, 2013.

NetDiligence (2013), "Cyber Liability & Data Breach Insurance Claims – A Study of Actual Payouts of Covered Data Breaches," *http://www.netdiligence.com/files/CyberClaimsStudy-2013.pdf*, last accessed: April 24, 2014.

Nierhaus, F. (1986), "A Strategic Approach to Insurability of Risks," *Geneva Papers on Risk and Insurance—Issues and Practice* 11(2): 83–90.

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.

Ouellette, P. (2012), "Pros and Cons of Cyber Insurance for Health Data Breaches," *http://healthitsecurity.com/2012/10/29/pros-and-cons-of-cyber-insurance-for-health-data-breaches/*, last accessed: January 18, 2014.

Ponemon Institute (2013a), "2013: Cost of Data Breach Study: Global Analysis," *https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf*, last accessed: April 24, 2014.

Ponemon Institute (2013b), "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," *http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf*, last accessed: January 18, 2014.

Schmit, J. T. (1986), "A New View of the Requisites of Insurability," *Journal of Risk and Insurance* 53(2): 320–329.

Securities and Exchange Commission (SEC) (2011), "Cybersecurity," Division of Corporation Finance Securities and Exchange Commission CF Disclosure Guidance: Topic No. 2, Washington.

Shackelford, S. J. (2012), "Should Your Firm Invest in Cyber Risk Insurance?" *Business Horizon* 55: 349–356.

Shetty, N. S. G., Felegyhazi, M., and Walrand, J. (2010), "Competitive Cyber-Insurance and Internet Security," In: Moore, T., Pim, D., and Ioannidis, C. (ed.): *Economics of Information Security and Privacy*, pp. 229–247, Springer.

Symantec (2014), "Internet Security Threat Report," *http://www.symantec.com/security_response/publications/threatreport.jsp*, last accessed: January 18, 2014.

Vermaat, A. J. (1995), "Uninsurability: A Growing Problem," *Geneva Papers on Risk and Insurance—Issues and Practice* 20(4): 446–453.

Villasenor-Alva, J. A. and Gonzalez-Estrada, E. (2009), "A Bootstrap Goodness of Fit Test for the Generalized Pareto Distribution," *Computational Statistics and Data Analysis* 53(11): 3835–3841.

Wang, Q.-H. and Kim, S. H. (2009a), "Cyberattacks: Does Physical Boundary Matter?" *ICIS 2009 Proceedings*, Paper 48.

Wang, Q.-H. and Kim, S. H. (2009b), "Cyber Attacks: Cross-Country Interdependence and Enforcement," *Working Paper*.

White House (2013), "Executive Order: Improving Critical Infrastructure Cybersecurity," Washington.

Willis (2013a), "Willis Fortune 500 Cyber Disclosure Report," *http://blog.willis.com/downloads/cyber-disclosure-fortune-500*, last accessed: December 16, 2013.

Willis (2013b), "Willis Fortune 1000 Cyber Disclosure Report," *http://blog.willis.com/downloads/cyber-disclosure-fortune-1000-2013*, last accessed: December 16, 2013.

Wojcik, J. (2012), "Cyber Insurance Not Always Enough," *Business Insurance* 46: 4.

World Economic Forum (2012), "Global Risks 2012 Seventh Edition," *http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf*, last accessed: January 9, 2014.

World Economic Forum (2014), "Global Risks 2014 Ninth Edition," *http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf*, last accessed: April 17, 2014.

Zurich Insurance Company Ltd and Atlantic Council of the United States (Zurich) (2014), "Risk Nexus: Beyond Data Breaches: Global Interconnections of Cyber Risk," Zurich and Washington.

Appendix A

Table A1 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; furthermore, if we could identify keyword combinations that we missed in the first round, we started all over at Step 2 with these new words

Table A2 Keywords per criteria

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 B

Table B1 Academic articles and industry studies on cyber risk and cyber insurance[93]

	A. Academic Papers on Cyber Risk and Cyber Insurance	
1	Haas and Hofmann (2013)	Discuss risk management and insurability of cloud computing from an enterprise risk management perspective.
2	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.
3	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.
4	Herath and Herath (2011)	Develop a copula framework to price cyber insurance policies.
5	Hofmann and Ramaj (2011)	Develop an economic model that explicitly reflects the interdependent risk structure of a cyber network.
6	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.
7	Cebula and Young (2010)	Provide a taxonomy of operational cyber security risks and identify and organize sources for it (results: four classes).
8	Shetty, Felegyhazi, and Walrand (2010)	Network security may be lower with insurance because of moral hazard.
9	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.
10	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.
11	Wang and Kim (2009a)	Analyze interdependences in cyber attacks across national boundaries by evaluating spatial autocorrelations of cyber attacks.
12	Wang and Kim (2009b)	Characterize empirically the interdependence in cyber attacks and analyze the impact of an international treaty against cyber crimes on it.
13	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.
14	Böhme and Kataria (2006)	Focus on correlation properties of different cyber risks and introduce a classification of cyber risks based on correlation properties.
15	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.
16	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.
17	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.
18	Mukhopadhyay et al. (2005)	Develop a utility model for assessing the benefit of using insurance to manage cyber risk.
19	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 (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.
2	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.
3	Marsh (2013)	Europe: 25% of corporations are not aware of insurance solutions for cyber risk and only 10% have bought insurance coverage.
4	Willis (2013a, b)	United States: coverage at about 6%, but large variations between industries among the Fortune 1000 companies.
5	Betterley (2010)	Global: cyber insurance market grew from US$ 100 million in 2003 to at least US$ 600 million as of 2009.
6	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 cyber crime.

[93] Seven trade journal articles on cyber insurance are also included in our discussion (Ackerman, 2013; Gould, 2013; Chabrow, 2012; Ouellette, 2012; Wojcik, 2012; Lemos, 2010; Cylinder, 2008). Moreover, 13 industry studies on cyber risk are included, i.e., CSI (2014), Hackmageddon (2014), Symantec (2014), World Economic Forum (2014), NetDiligence (2013), Kaspersky Lab (2013), KPMG (2013), McAfee (2013), Ponemon Institute (2013a, b), Department of Homeland Security (2012), ENISA (2012), and GCHQ (2012). The industry studies do not discuss cyber insurance, but the data and information on cyber risk provided therein are useful for our insurability discussion.

Table B2 Assessment of insurability for cyber risk (extended version with all references)

Insurability criteria	Evaluation of compliance
(1) Randomness of loss occurrence *problematic*	- Correlation among risk hinders pooling of risks (Haas and Hofmann, 2013; Herath and Herath, 2011; Hofmann and Ramaj, 2011; Bolot and Lelarge, 2009; Wang and Kim, 2009a, b; Baer and Parkinson, 2007; Böhme and Kataria, 2006) - Risk pools are too small and cannot be diversified; also: lack of adequate reinsurance (e.g., ENISA, 2012; Cylinder, 2008; Bear and Parkinson, 2007) - Lack of data (Chabrow, 2012; Department of Homeland Security, 2012; ENISA, 2012; Shackelford, 2012; Herath and Herath, 2011; Betterley, 2010; Baer and Parkinson, 2007; Gordon, Loeb, and Sohail, 2003) - Risk of change, due to changes in the nature of the risks and new standards/regulation (Haas and Hofmann, 2013; ENISA, 2012; Gatzlaff and McCullough, 2012; Lemos, 2010)
(2) Maximum possible loss *not problematic*	- Maximum possible loss for cyber risk lower than for other OpRisk - Insurers protect themselves by coverage limits; losses can be well covered
(3) Average loss per event *not problematic*	- Average loss for cyber risk lower than for other OpRisk (our data; KPMG, 2013; Ponemom, 2013) - Average loss depends on size, self-protection, and institutional commitment to information security (our data; Shackelford, 2012)
(4) Loss exposure *not problematic*	- Increasing number of cyber risk events, but highly dependent on event category (e.g., malware very frequent, physical data theft less frequent) - Exponentially increasing number of incidents (see Figure 1 in Majuca, Yurcik, and Kesan, 2006)
(5) Information asymmetry *problematic*	- Moral hazard, i.e., lack of incentive for insured to take self-protective measures that reduce the loss probability subsequent to purchasing insurance (Haas and Hofmann, 2013; Shackelford, 2012; Ögüt, Raghunathan, and Menon, 2011; Baer and Parkinson, 2007; Majuca, Yurcik, and Kesan, 2006; Gordon, Loeb, and Sohail, 2003); moreover: investments in cyber security exhibit a public good character with positive externalities; problem of proving source of loss and in the detection of perpetrators; screening and deductibles to mitigate moral hazard - Adverse selection, i.e., firms that have experienced cyber attacks are more likely to buy insurance (Shackelford, 2012; Gordon, Loeb, and Sohail, 2003); screening (audits), self-selection (underwriting questions), and signaling (certificates) to mitigate adverse selection
(6) Insurance premium *increasingly less problematic*	- High premiums and other costs due to large uncertainties, but premiums expected to decline over time (Shackelford, 2012; Betterley, 2010) - Large geographic and industry variations in availability of policies (Shackelford, 2012); in general: low number of competitors; expected to increase over time - Additional costs (e.g., time-consuming upfront assessments)
(7) Cover limits *problematic*	- Cyber risk policies typically cover a maximum such as, e.g., US$ 50 million - Cyber risk policies contain exclusions (e.g., self-inflicted loss, accessing unsecure websites, terrorism) (Mukhopadhyay et al., 2005); some indirect costs cannot be measured and often are not covered (e.g., reputational effects) (Gatzlaff and McCullough, 2012; Wojcik, 2012) - Product complexity can be problematic (exclusions, dynamic risk nature, uncertainty for both insurance seller and buyer regarding actual coverage) (see, e.g., ENISA, 2012)
(8) Public policy *less problematic*	- Cyber insurance may raise incentives to put less effort in self-protection; in combination with high correlations, this increases overall industry exposure (Pro: Ögüt, Raghunathan, and Menon, 2011; Contra: Kesan, Majuca, and Yurcik, 2004) - Insurance fraud might be incentivized, since hacking attacks or physical attacks are difficult to detect and trace
(9) Legal restrictions *less problematic*	- In many countries, insuring regulatory fines is not permitted - Regulatory changes (Haas and Hofmann, 2013; Gatzlaff and McCullough, 2012) - Novelty, complexity, and dynamic nature of risk might pose potential legal threat for insurance brokers that limits their willingness to offer the products; only few specialist are willing and able to sell cyber insurance (Chabrow, 2012) - Disclosure of sensitive information (Ouellette, 2012)

Appendix C

Operational risk models, in general, apply methods from the extreme value theory when estimating the loss severity distribution. We follow Hess and estimate the loss severity distribution using a spliced distribution approach.[94] Losses above a predefined threshold are modeled by a generalized Pareto distribution (GPD), while losses below the threshold are modeled with an exponential distribution. We apply the bootstrap goodness-of-fit test by Villasenor-Alva and Gonzalez-Estrada (2009) and, based on this, choose a threshold at the 90% percentile.[95] The value at risk (VaR) is then approximated by an estimator described by Gilli and Käellezi.[96] The VaR of the estimated loss severity distribution is close to the empirical one (see Table C1).[97] The modeled VaR is much higher than for non-cyber risk. The estimated shape parameter of the GPD distribution gives an indicator for the heaviness of the tails; the higher the parameter, the heavier the tail.[98] Boxplots and distribution and density functions for cyber and non-cyber risk are shown in Figures C1 and C2.

Table C1 Modeling Results

			Exponential and GPD with threshold of				Log-normal	Gamma	Weibull
			90%		92.5%				
Category	N	Empirical VaR(95%)	Shape estimate	Modeled VaR(95%)	Shape estimate	Modeled VaR(95%)	Modeled VaR(95%)	Modeled VaR(95%)	Modeled VaR(95%)
Cyber Risk	994	89.56	1.02	94.82	0.89	98.40	60.95	197.00	83.13
Non-Cyber Risk	21,081	248.97	1.06	236.65	0.90	248.68	198.84	472.03	229.75

We also model losses with other distributions common to actuarial science, such as the log-normal, Gamma, or Weibull distribution.[99] We estimate the respective parameters and present the VaR. The VaR estimator from the log-normal and Gamma distribution are very far from the empirical value, which might indicate that the distribution assumption does not fit the data well. The result for the Weibull distribution is much closer to the empirical VaR. In all cases, the losses for cyber risks are substantially lower than for non-cyber risks.

[94] See Hess (2011).

[95] For purposes of comparison, we also present results for a 92.5% threshold; thresholds below reveal a non-fit for non-cyber risks according to Villasenor-Alva and Gonzalez-Estrada (2009); raising thresholds much higher makes the sample used for the fit in cyber risk too small.

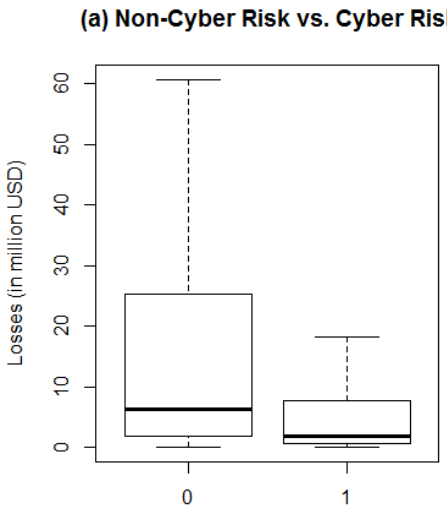
[96] See Gilli and Käellezi (2006).

[97] An approximation of the loss distribution per category was not made, since the sample size would be too small for computation of the tail distribution.

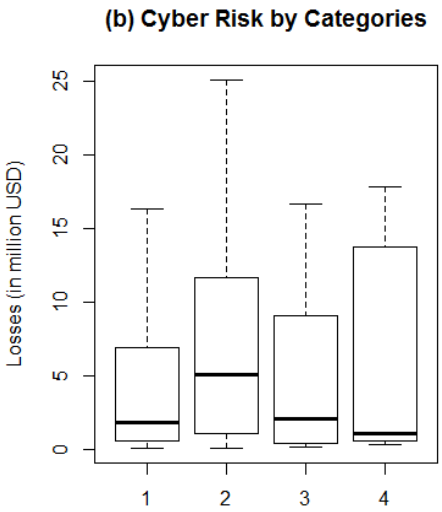
[98] See Gilli and Käellezi (2006).

[99] See, e.g., Eling (2012).

Figure C1 Boxplots of cyber and non-cyber risk categories



0 = Non-Cyber Risk, 1 = Cyber Risk



1 = Actions of people, 2 = Systems and technical failure, 3 = Failed internal processes, 4 = External events

Note: In the figures we use the 1.5 IQR whisker and do not show outliers.

Figure C2 Estimated distribution and density function