Institute of Insurance Economics

University of St.Gallen

How to Organize Cyber Risk Transfer?

Jan Hendrik Wirfs

Working Papers on Risk Management and Insurance No. 183

Edited by Hato Schmeiser

Chair for Risk Management and Insurance

October 2016

How to Organize Cyber Risk Transfer?

Jan Hendrik Wirfs[a,*]

[a] *Institute of Insurance Economics, University of St. Gallen, Rosenbergstrasse 22, 9000 St. Gallen, Switzerland*

Abstract

Cyber risk has become a topic of great importance in today's risk management and insurance is seen as a powerful means of countering it. However, the actual cyber insurance market is greatly underdeveloped. Challenges in the insurability of cyber risk were identified as the central impediments to cyber insurance market growth. This paper investigates potential risk transfer schemes for cyber risk that can improve its insurability and foster market development. The work is the first to compare different risk transfer options for cyber risk and test them in a simulation approach. We show that the current market is relatively small and can benefit from the introduction of risk transfer mechanisms for the primary insurer (e.g., reinsurance and capital market solutions). For extreme scenarios the definition of an insurance pool is an effective way to foster market development. In worst-case scenarios – for instance a breakdown of the critical information infrastructure – the active risk transfer by the government is shown to be vital. Minimum standards for mitigation are effective in the presence of correlations in an insurer's portfolios.

Keywords: Cyber risk, risk management, risk transfer mechanisms, insurance

1 Introduction

Significant economic and social impacts as well as the growing attention in media have made cyber risk a topic of great importance in today's risk management.[1] In synergy with other measures, insurance is seen as a powerful means to handle cyber risks and cyber insurance is anticipated to become a major line of business in the next ten years (Aon Benfield, 2015). Today

[*] Corresponding author: Tel.: +41 71 244 7971.
E-mail address: jan.wirfs@unisg.ch (J. H. Wirfs).
The author gratefully acknowledges the financial support provided by the Geneva Association (*Geneva Association's Research Grant on Cyber Risk* in 2016). I also thank Semir Ben Ammar, Christian Biener, Alexander Braun, Martin Eling, Felix Hentschel, Daliana Luca, Veselina Milanova, Lukas Reichel, and Philipp Schaper for their helpful suggestions that substantially improved this paper. In addition, the paper greatly benefitted from discussions with conference participants at the 2016 Annual Conference of the Asia-Pacific Risk and Insurance Association (APRIA) in Chengdu, in particular with W. Jean Kwon and Soichiro Moridaira, and at a research seminar in St. Gallen with Randy E. Dumm in May 2016.

[1] There are several examples for the economic and social relevance of cyber risk. For instance, McAfee (2014) evaluates the annual costs to the global economy from cybercrime at more than US$ 400 billion (US$ 200 billion only in the four largest economies: US, China, Japan, and Germany). Those costs are up to 1.6% of GDP, depending on the country. Furthermore, McAfee estimates that cyber risk could cause as many as 150,000 Europeans to lose their jobs. Estimates from 2010 already determine the costs of global cybercrime to range from about US$ 100 billion to US$ 1 trillion (Kshetri, 2010), indicating a huge loss potential. Furthermore, discussions about cyber catastrophes gain significant importance in literature; see, e.g., Ruffle et al. (2014), Lloyd's (2015), or Long Finance (2015).

the cyber risk insurance market is greatly underdeveloped and far below expectations.[2] A central impediment to market development are challenges in the insurability of cyber risk (Biener, Eling, and Wirfs, 2015). In particular, correlations among risks hinder efficient pooling and risk pools are too small. Moreover, the absence of reliable data, the dynamic nature of cyber risk, information asymmetries, and restrictive contract designs (e.g., cover limits) all impede market growth. Discussions with stakeholders in the insurance and reinsurance industry, however, clearly illustrate the increasing interest in the topic and show that insurance companies would be willing to enter a cyber risk insurance market, if certain obstacles to insurability were removed. In this context, market participants emphasize the need for governmental intervention. They call for governmental risk transfer mechanisms that proved useful for other risk categories (e.g., natural catastrophe risk) to be adapted to cyber risks (Gray, 2015). We build upon these observations and investigate potential schemes to organize risk transfer for cyber risk that overcome these challenges to insurability.

The main goal of this paper is to investigate potential risk transfer schemes for cyber risk, which can improve its insurability and encourage market development. We define five potential risk transfer layers which can engage into the risk transfer market: the risk owner, primary insurers, reinsurers, capital markets, and the government. For each party we derive risk transfer instruments and evaluate their impact on the development of a cyber insurance market in a simulation approach. We propose a modeling framework for all potential stakeholders in the risk transfer market based on standards from expected utility theory. Scenario analysis is applied to test how the suggested risk transfer options can handle the financial implications resulting from cyber-related scenarios.

The literature comprises work on the modeling of cyber insurance markets with respect to different challenges to the insurability of cyber risk. For instance, Böhme (2005) and Böhme and Kataria (2006) analyze insurance markets in the presence of correlated cyber risks. Bandyopadhyay et al. (2009) and Shetty et al. (2010) investigate cyber insurance markets under the assumption of information asymmetries. Other research addresses the interdependence in security systems (e.g., Bolot and Lelarge, 2009). Böhme and Schwartz (2010) provide a comprehensive review of cyber-related literature in this area up to 2010.[3] Mukhopadhyay et al. (2013) define a

[2] Estimates back in 2003 for 2005 expected US premiums to reach already US$3.6 billion (III, 2003). However, these expectations are not met. More than a decade later the annual premium volume for the US and Europe together (the major two markets) is valued at about US$3 billion for 2014 (Advisen, 2015).

[3] Several other papers were published in this area, focusing only on one of the parties in the cyber insurance market; e.g., Öğüt et al. (2011) or Herath and Herath (2011).

copula-based Bayesian Belief Network to assess potential policyholders' exposure to cyber risk. The assessment facilitates the policyholder's decision to buy or not buy cyber insurance. In addition, Mukhopadhyay et al. (2013) propose models that allow insurance companies to design and evaluate the appropriateness of insurance contracts. However, all these setups model only the first stage of a cyber risk transfer market (i.e., the relationship between policyholders and the primary insurer), with respect to some of the challenges in insurability. Our analysis extends the models of a primary insurance market by incorporating a reinsurance industry, capital market solutions, and two measures for governmental intervention. In addition, we incorporate most of the challenges in insurability.

To the best of our knowledge, this paper is the first to analyze the risk transfer market for cyber risk beyond the primary insurance market.[4] The suggested setup enables the analysis of potential risk transfer schemes for cyber risk and their impact on market development under the consideration of the main impediments to insurability. Additionally, we contribute to the literature by providing deeper insights into the underrepresented strand of literature about cyber risk in the domain of risk and insurance. We test the appropriateness of innovative risk transfer solutions (e.g., risk transfer by capital market solutions) in the management of cyber risk and contribute to the adequacy evaluation of primary insurance and reinsurance products to cover cyber risks. The scenario analysis validates the appropriateness of those instruments for different cyber risk developments. Our results are also important for regulators because they provide insights about how to structure the market and how to respond to catastrophic cyber incidents.

The results show that without any further opportunity to transfer risk, insurers offer only insurance contracts with small cover limits. Those are unattractive to policyholders, which explains the small insurance market. Market size increases with the promotion of reinsurance and capital market solutions. However, the challenges in insurability of cyber risk significantly decrease market size. For instance, with increasing severity of scenarios, the market decreases and the analyzed risk transfer mechanisms cannot compensate for these effects. Only the establishment of an insurance pool fosters market development for extreme scenarios. Unfortunately, the effectiveness of this instrument is impaired if losses are correlated. Minimum mitigation standards could alleviate the problems caused by correlated losses. Under worst-case scenarios none of the analyzed risk transfer instruments can prevent a cyber insurance market from its non-existence. Under these circumstances, instruments under which the government actively covers risks (e.g., a governmental backstop as in terrorism risks) seem to be the ultimate choice.

[4] We discuss an initial version of our model in Eling and Wirfs (2016a).

The remainder of this article is structured as follows. Section 2 defines the modeling framework and illustrates the potential risk transfer options for a primary insurer. We also discuss the inclusion of the challenges in insurability to the model. In Section 3, we discuss the empirical results. Section 4 concludes.

2 The Risk Transfer Modeling Framework

2.1 A Primary Insurance Market for Cyber Risk

For our model, we consider a market with an exemplary insurance company that issues cyber insurance policies to n^{PI} identical risk-averse individuals. We assume that these individuals (we will call them risk owners) have an initial wealth W_0, and face a stochastic loss of size X, that occurs with a probability of p. For the modeling of X we refer to Appendix A for more details. We define the insurance contract offered by the primary insurer by the function $I^{PI}(X)$ (I^{PI} = indemnity), with $0 \leq I^{PI}(X) \leq X$. For taking over the amount of $I^{PI}(X)$ from the risk owner's loss, the insurer charges a premium P^{RO}. The risk owners are defined to be risk-averse, with a utility function U^{RO} describing their risk preferences (U^{RO} is a twice continuously differentiable von Neumann-Morgenstern utility function, as, e.g., in Cummins and Mahul, 2004). From this setup we derive the risk owner's demand decision for the cyber insurance policy by the following inequality:

$$E\left[U^{RO}\left(W_0 - P^{RO} - X + I^{PI}\left(X\right)\right)\right] \geq E\left[U^{RO}\left(W_0 - X\right)\right]. \ (1)$$

The risk owner purchases insurance if the expected utility with insurance is greater than the expected utility without coverage.

Based on the assumptions for the risk owner, the exemplary primary insurer holds a cyber insurance portfolio of n^{PI} contracts, for which the aggregated loss of

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

has to be settled. X_i denotes the random loss from the i-th contract in the insurer's portfolio. As for the risk owner, the primary insurer holds total initial funds, denoted by $A_{0,PI}$. In addition to the initial funds, the insurer receives premium payments from each policyholder. The total amount of premiums earned is

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

where P_i^{RO} is the premium payment from the i-th policyholder in the portfolio.

The primary insurer's decision to offer insurance to the risk owner depends on its risk appetite. The literature presents two strands of decision processing in insurance companies. Insurers are risk-neutral or risk-averse in terms of their decision to offer insurance.[5] The assumption of risk-neutrality and risk-aversion has not yet been determined. Risk-neutrality is equivalent to the assumption that the decision for or against offering insurance to policyholders is based solely on (expected) profit maximization. The justification for this definition is based on the assumption that insurance companies can adequately diversify and have access to sufficient reinsurance (Kelly and Kleffner, 2003). However, literature for cyber risk shows that the arguments that justify risk-neutral behavior in insurance companies do not exist for cyber risk. According to Biener, Eling, and Wirfs (2015) risk pools are relatively small, thus hindering efficient pooling, and reinsurance is virtually nonexistent. We thus suppose that the insurer is risk-averse in terms of offering cyber insurance. We model this by the introduction of a utility function U^{PI} that describes the insurance management's preferences to cover losses from cyber risk. This has already been done in literature; for instance, Kelly and Kleffner (2003) analyze both risk-aversion and risk-neutrality, while Golubin (2014) assumes only risk-aversion. It has also been assumed for the primary insurance decisions to buy reinsurance; see Mossin (1986) or Cummins and Mahul (2004).[6]

Under the assumption of risk-aversion decision to supply insurance coverage is given by

$$E\left[U^{PI}\left(A_{0,PI}+P^{PI,earned}-L^{PI}\right)\right]\geq E\left[U^{PI}\left(A_{0,PI}\right)\right]. \quad (2)$$

The primary insurer would enter the market only if the expected utility of offering insurance contract I^{PI} to n^{PI} individuals outweighs the expected utility of not entering the market.

Based on the definition of inequality (1) and (2), the model allows to test – given a particular insurance contract I^{PI} – if the risk owner and the insurance company would enter the market (respectively, buy and offer the product). The simulation approach is grounded in the test of various contract specifications I^{PI} and the measurement of how many of them are feasible (i.e., inequality (1) and (2) must be satisfied simultaneously). The number of feasible solutions is an indicator of market size. We use here a simplistic measure: the ratio of feasible solutions to

[5] Note that most of the literature for these models formulates this in a way that "insurance companies are risk-neutral or risk-averse" (e.g., Kelly and Kleffner, 2003; Schlesinger, 2013; and many more). However, it is important to us that this refers always to the way decisions are made in the company; in other words it refers to the behavior of decision-making units. For the decision to underwrite a particular risk this would be the behavior of the insurer's risk management unit.

[6] However, since literature has not conclusively supported neither the assumption for risk-aversion nor risk-neutrality, we follow Kelly and Kleffner's (2003) approach, and investigate the impact of this assumption in the appendix; in other words we analyze risk-aversion in the main part of the paper and risk-neutrality in Appendix C.

tested contract designs. In the next step, we investigate how this size changes with the integration of insurability challenges and the inclusion of further layers of risk transfer (reinsurance, capital markets, and governmental intervention), providing an indicator for the development of the cyber insurance market. When economists describe the level of insurance market development, they consult figures such as insurance density (ratio of premiums underwritten to total population) or the insurance penetration rate (premiums underwritten to GPD); see, e.g., Outreville (2013). Therefore, we add a second size measure based on the potential premiums earned in the exemplary market. Since we have different contracts I^{PI} with different premiums, we compute the average premium in the market. An estimation of an insurance density or a penetration rate is impossible in this case, since we lack the reference measures in our analysis (total population or GPD).

2.2 Modeling the Challenges to Insurability

The model defined so far describes a general primary insurance market. According to Biener, Eling, and Wirfs (2015), several difficulties in the insurability of cyber risk hinder market development. We discuss how to include and account for these difficulties in the basic model of Section 2.1.

Correlation among Cyber Risks

One obstacle to the insurability of cyber risk is the correlation among cyber risks (Biener, Eling, and Wirfs, 2015). We account for this effect in our simulation by generating correlated losses in insurers' portfolios. Our approach stems from Cossette et al. (2002), who define two approaches to model dependence in portfolios: risk arrival processes and copulas. In the former they define the dependence in insurance portfolios by a risk arrival process that is represented by three random variables, each corresponding to an individual, collective, and class risk factor. We choose each factor to model the dependence of losses for the risk owner (individual), the primary insurers' (collective) and reinsurers' (class) portfolios.

Böhme (2005) and Böhme and Kataria (2006) have addressed correlation in cyber insurance markets within the field of technology. Our model setup is similar to Böhme and Kataria's (2006) in two ways. First, they propose a mixture of a risk arrival process and a copula approach to model correlation for the demand- and supply-side of cyber insurance. Second, the demand-decision is based on expected utility theory, while the supply-side decision is based on profit-maximization with a solvency constraint (see the analysis in Appendix C). The two approaches differ in that Cossette et al. (2002) allows the incorporation of distributional assumptions for the loss sizes (e.g., the heaviness of losses is incorporated; see, Eling and Wirfs, 2016b). Furthermore, our setup allows the analysis of further risk transfer layers, also under the assumption of correlated losses. These differences also apply to Böhme (2005). The model used therein generates correlated losses in the insurer's portfolio by a correlation of loss occurrences to a latent systemic risk random variable. This approach is also different from the one discussed in Cossette et al. (2002). The decision model (expected utility theory for policyholders, and profit-maximization for insurers) is identical to the one in Böhme and Kataria (2006) and our approach in Appendix C.

Information Asymmetries in Cyber Risks

Another insurability challenge addressed in the literature is that of information asymmetries. In Section 2.1 we assume identical risk owners, which allows us to solely focus on moral hazard effects. We adjust the model by allowing risk owners to invest in risk mitigation measures[7] or reduce their cyber security expenditures. For this analysis we adopt a setup similar to Kelly and Kleffner's (2003). We define the risk owner's loss from cyber risk after investing the amount *r* (ex-ante) in mitigation measures by

$$X\left(r\right)=X\cdot e^{-\beta r},$$

where *X* is the original risk owner's exposure, and β is a parameter measuring the effectiveness of the mitigation instrument. Note that we do not restrict $r \geq 0$, which allows for the analysis of moral hazard effects. Inequality (1) thus changes to

$$E\left[U^{RO}\left(W_0-r-P^{RO}-X\left(r\right)+I^{PI}\left(X\left(r\right)\right)\right)\right]\geq E\left[U^{RO}\left(W_0-r-X\left(r\right)\right)\right]. \quad (1.1)$$

The investments in mitigation are difficult to observe for the primary insurer or are connected with high costs (see, e.g., Shetty at al., 2010). Therefore, we assume that the primary insurer cannot determine the amount *r* invested. This leads to an unchanged primary insurer's solution constraints (inequality (2)). In addition, the premium P^{RO} for the insurance contract is the same as in Section 2.1.

Shetty et al. (2010) incorporate moral hazard into a model for a cyber insurance market.[8] They propose an insurance market model with a risk-averse policyholder that can buy insurance

[7] We define mitigation measures to be all instruments that lower the loss size. This has been denoted "self-insurance" by Ehrlich and Becker (1972). We thus do not incorporate self-protection measures that reduce the probability of loss occurrence (see also Ehrlich and Becker, 1972, for the definition of self-protection).

[8] Bandyopadhyay et al. (2009) discuss an insurer's reaction to uncertainties about losses from cyber incidents and asymmetric information. They do not describe a model to analyze a cyber insurance market, but find that insurers respond to those uncertainties with high deductibles and low cover limits.

and/or mitigation, and a risk-neutral insurance company. However, their primary focus is not on the insurance market itself, but on the mitigation incentives insurance can provide and their effect on overall network security. The insurance market model is similar to the one in Section 2.1, while the inclusion of mitigation measures is more technical and related to actual network specifics than just a pure investment amount, as in our approach. Shetty et al. (2010) find that insurance is effective in the management of cyber risk, but it cannot give users an incentive to mitigate. This is due to network externalities, in other words the moral hazard effects present in cyber risk.

Changing Nature of Cyber Risks

Another problem with the insurability of cyber risk is its changing nature by virtue of new standards, regulations and technologies (see, e.g., Biener, Eling, and Wirfs, 2015). To account for this dynamism we use scenario analysis. We define three scenarios based on different assumptions about the loss exposure for the risk owner (and consequently for the other layers; see Appendix A for more information on the loss modeling). Scenario 1 is the base scenario and relies on the total observed losses in the cyber loss database. Scenario 2 defines extreme losses. Based on the analyses in Eling and Wirfs (2010b), this data exhibits extreme cases for losses above a 56% threshold. This scenario thus rests on only 44% of the highest losses in the database. Finally, scenario 3 is not based on real loss data, but estimates a worst-case scenario defined in the literature. WEF (2010) and Ruffle et al. (2014) both study a timely restricted critical information infrastructure breakdown, amounting to total losses of about US$250 billion to the industry. In WEF (2010) the probability of occurrence of such an event is estimated at 10%. We use this information to define a scenario in which our market faces a US$250 billion loss. The amount is distributed equally to all risk owners. We assume that this event happens with a 10% probability and affects all risk owners simultaneously. The event leads to an accumulation of losses (correlation of 1) in the primary insurer's portfolio. To the best of our knowledge, no study that models an insurance market has applied a scenario approach before.

Further Challenges in the Insurability of Cyber Risks

The model adjustments do not explicitly cover all challenges to the insurability of cyber risk, however, the model itself does allow for their analysis. Biener, Eling, and Wirfs (2015) find that risk pools are relatively small and that efficient pooling is impaired. We can easily analyze the effect of changing portfolio sizes on market development. The general absence of reliable data is compensated for by the estimation of risk exposures based on cyber incident loss data given by an operational risk database (see Appendix A). Finally, current cyber insurance policies exhibit cover limits, deductibles, and exclusions (Biener et al., 2015). The effect of restrictive contract designs is investigated by the variation in contract specifications in the simulation approach. Table 1 summarizes the challenges in the insurability of cyber risk based on Biener, Eling, and Wirfs (2015) and how they are incorporated in the simulation approach.

Table 1 Challenges in Insurability of Cyber Risk and Integration in the Model

Challenges in Insurability	**Integration in the Model**
Correlations among cyber risks	Inclusion of correlation in the (re-)insurer's portfolios by the approach discussed in Cossette et al. (2002).
Information asymmetries	Accounting for moral hazard by the inclusion of the effects of mitigation on the demand of cyber risk insurance, analog to the discussions in Kelly and Kleffner (2003).
Dynamic nature of cyber risk	Scenario analysis and inclusion of a cyber catastrophe (worst-case) event as described in WEF (2010) and Ruffle et al. (2014).
Extant risk pools are too small	Effect of portfolio sizes is analyzed by the variation of portfolio sizes; in addition, the effect of an insurance pool is incorporated.
Wide absence of reliable data	Analysis of a cyber risk database which is derived from operational risk (SAS Global OpRisk dataset).
Restrictive contract designs (e.g., cover limits)	Variation of contract specifications (e.g., deductibles, cover limits in the primary insurance contracts, retention levels in the reinsurance contracts) in the simulation approach.

2.3 Risk Transfer by Reinsurance

This section defines the first risk transfer solution for a primary insurer. We include a reinsurance company that covers $I^{RE}(L^{PI})$ $(0 \leq I^{RE}(L^{PI}) \leq L^{PI})$ of the aggregated primary insurer's loss L^{PI} and charges a premium of P^{PI}. In this case, the primary insurer's decision constraint changes to

$$E\left[U^{PI}\left(A_{0,PI} - P^{PI} + P^{PI,earned} - L^{PI} + I^{RE}\left(L^{PI}\right)\right)\right] \geq E\left[U^{PI}\left(A_{0,PI}\right)\right]. \quad (3)$$

The reinsurance company is modeled similarly to the primary insurer. We assume an exemplary reinsurance company with a portfolio of n^{RE} reinsurance contracts. For each contract, the reinsurer covers $I^{RE}(L^{PI,i})$ of the i-th reinsurance contract's loss in exchange for the premium $P^{PI,i}$. The aggregated loss payed by the reinsurer is then

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

and the total premiums earned by the reinsurance company are

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

In addition, we assume the reinsurer has an initial capital $A_{0,RE}$. For a utility function U^{RE}, the reinsurer's decision to offer reinsurance is described by

$$E\left[U^{RE}\left(A_{0,RE} + P^{RE,earned} - L^{RE}\right)\right] \geq E\left[U^{RE}\left(A_{0,RE}\right)\right]. \quad (4)$$

Only if constraints (1), (3), and (4) are satisfied simultaneously for specific I^{PI} and I^{RE}, does a market for cyber insurance thrive.

2.4 Risk Transfer by Capital Market Solutions

Over the last year, the risk transfer for cyber risk by capital market solutions has attracted significant interest in practice. For instance, an industry study by Traynor et al. (2016) discusses the coverage of cyber risk by cyber catastrophe bonds. Their results point out that, in particular, catastrophic cyber risk events could be well securitized by capital market solutions; however, before this can be done, there must be significant progress in aggregating and modeling of cyber risk. Moreover, an operational risk catastrophe bond launched in May 2016 also covers IT system failures that cause business interruption, accounting, or documentation errors, which could be counted as cyber risk (Artemis, 2016). In the academic literature, Pandey and Snekkenes (2016) investigate capital market-based financial instruments (e.g., options, vanilla options, swaps, and futures) to address limitations in the cyber insurance and reinsurance markets. They find that these tools can solve at least some of the problems in insurance markets.

The relevance of a capital market solution as discussed in the literature justifies its inclusion in the model. We define a "cyber cat bond" and apply it in two models: (a) replacing the reinsurer in the previous model (Section 2.3), and (b) a capital market solution that covers losses from a reinsurer. The approach used for the modeling of the capital market follows the one proposed by Kunreuther, Kleindorfer, and Grossi (2005).[9] We assume a sponsor (primary insurer in (a) or reinsurer in (b)) that issues a cyber risk cat bond (similar to a natural catastrophe bond) and pays investors an interest payment $r^{Cyber\ Cat}$ in exchange for their guarantee to provide funds in

[9] The definition in this part of the model is already very specific and cannot be adjusted flexibly as the definitions of I^{PI} and I^{RE}. However, we can provide a first indication of how capital market solutions could affect the market development in a cyber insurance market.

case of a disastrous cyber loss faced by the sponsor. For the implementation of the cyber cat bond we assume a one-period time horizon.[10] We assume an exemplary investor making a payment to the sponsor of

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

where $r^{Zero\text{-}Coupon}$ is the promised return on the zero-coupon catastrophe bond and B is the face value (promised value of the zero-coupon bond (payment if no loss is triggered)). At the end of the contract period, the investor receives the face value less the potential indemnity payments to the (a) insurance or (b) reinsurance company. The payments made from the cyber cat bond to the investors are thus given by

$$Payout^{Investors}\left(L\right)=B-Payout^{Insurer}\left(L\right).$$

We define the payout from the cyber cat bond to the (re-)insurance companies by the formula:

$$Payout^{Insurer}\left(L\right)=\min\left\{\max\left\{L-AP;0\right\};K\right\},$$

where L denotes the sponsor's loss (random) variable (i.e., $L = L^{PI}$ if the model is attached to the primary insurance layer (model (a)), and $L = L^{RE}$ in the case of attachment to the reinsurance layer (model (b))). The other parameters in this definition of the payout are as follows:

- Parameter AP is the attachment point (trigger) and defines the value that needs to be exceeded by loss L such that the bond pays the indemnity. In the analysis we define an indemnity triggered cat bond (see, e.g., Kunreuther, Kleindorfer, and Grossi, 2005). At the time of writing this paper, we were not aware of a parametric cyber-related index that would have been applicable as another trigger option.
- K $(\leq B)$ specifies the maximum value the bond will pay above the attachment point.[11]

In model (a) the feasibility constraint (2) changes to

$$E\left[U^{PI}\left(A_{0,PI}-B\cdot r^{Zero-Coupon}+P^{PI,earned}-L^{PI}+Payout^{Insurers}\left(L^{PI}\right)\right)\right]\geq E\left[U^{PI}\left(A_{0,PI}\right)\right], \quad (2.1)$$

and in model (b) constraint (4) changes to

$$E\left[U^{RE}\left(A_{0,RE}-B\cdot r^{Zero-Coupon}+P^{RE,earned}-L^{RE}+Payout^{Insurer}\left(L^{RE}\right)\right)\right]\geq E\left[U^{RE}\left(A_{0,RE}\right)\right]. \quad (4.1)$$

Note, that in (2.1) and (4.1) the interest payments $B\cdot r^{Zero\text{-}Coupon}$ must be considered.

[10] In general, cat bonds are multi-year protection (see, e.g., Ben Ammar, Braun, and Eling, 2015), meaning that the assumption of a one-year contract as in a reinsurance contract might not be quite feasible here. Because of simplicity and the alignment to the general model setup, we need to accept this limitation here.

[11] Note that Kunreuther, Kleindorfer, and Grossi (2005) define the cat bond with a co-payment rate that defines the fraction of losses to be paid by the bond holder for losses exceeding AP. For simplicity, we leave the analysis of such effects to research in cyber cat bonds.

For the capital market investor we derive the actual return $R^{Cyber\ Cat}$ from the following equations. The overall return is estimated by

$$R^{Cyber\,Cat} = \frac{\frac{B - Payout^{Insurer}\left(L\right)}{B}}{\left(1 + r^{Zero-Coupon}\right)} - 1 = r^{Zero-Coupon} - \frac{\left(1 + r^{Zero-Coupon}\right) \cdot Payout^{Insurer}\left(L\right)}{B}.$$

$R^{Cyber\ Cat}$ depends on the random variable $Payout^{Insurer}(L)$, and so $R^{Cyber\ Cat}$ itself is a random variable. The decision criterion for the investor is then determined by:

$$\frac{E\left[R^{Cyber\,Cat}\right] - r^{risk-free}}{\sqrt{Var\left[R^{Cyber\,Cat}\right]}} \geq S. \ (5)$$

We determine solutions as feasible (i.e., part of the investor's solution) only if the estimated annual return to the investor is higher than a benchmark value *S*. Thus, for the interest payment we assume that investors demand a Sharpe ratio of *S*, which describes the excess return required by investors for an additional unit of risk (Kunreuther, Kleindorfer, and Grossi, 2005).[12] Overall, constraints (1), (2.1), and (5) form the decision criteria that must be satisfied if the primary insurer issues the bond (model (a)). If the reinsurer issues the bond (model (b)), constraints (1), (3), (4.1), and (5) must be satisfied.

2.5 Risk Transfer by Governmental Intervention

Market participants point to the fairly intractable insurability problems, emphasize the need for governmental intervention and call for mechanisms already in place for protection against catastrophic risk from natural events (Gray, 2015). Potential instruments for governmental involvement are manifold and can be structured into approaches in which the state directly enters the risk transfer market (e.g., "State as Primary Insurer" or "State as Reinsurer of Last Resort", see OECD, 2005), and those in which the government sets the regulatory framework to improve insurability (e.g., the introduction of reporting obligations, already standard in the US; and which have been defined and will take effect in the EU in 2018; European Union, 2016). The direct risk transfer is a special variant of the models described in the previous sections. In the following, we analyze two indirect approaches of governmental intervention. First, we measure the effects of minimum standards for mitigation. This model is based on the adjustments of Section 2.2 for the moral hazard analysis. While we assumed in Section 2.2 that the primary

[12] Note that investors do not solely price the value of a cat bond by a Sharpe ratio, but for simplicity we assume this set-up here. They might also incorporate metrics like the spread as a measure of expected loss in their decision processes (see, e.g., Ben Ammar, Braun, and Eling, 2015).

insurer cannot observe the investment *r* into mitigation measures, under the minimum mitigation standard this is possible. In addition, the insurer can observe the real loss *X(r)* and adjust its premiums. The constraint (2) changes to

$$E\left[U^{PI}\left(A_{0,PI}+P^{PI,earned,mitigation}-L^{PI,mitigation}\right)\right]\geq E\left[U^{PI}\left(A_{0,PI}\right)\right], \text{(2.2)}$$

with premiums $P^{PI,\ earned,\ mitigation}$ and $L^{PI,\ mitigation}$ based on the indemnity payments $I^{PI}(X(r))$ and not on the original $I^{PI}(X)$.

Furthermore, we introduce the effect of an insurance pool solution. This has already been discussed in practice. For instance, Long Finance (2015) discusses a public-private cyber catastrophe reinsurance scheme for the UK that provides risk transfer for participating primary insurers. They find that such a scheme can enable the insurance industry to manage the huge risks to their balance sheets, if they offer cyber insurance. The scheme also has some additional advantages. It generates risk pools that can be transferred more efficiently to capital markets, encourages information and data sharing, and facilitates the definition of standards or best practices (Long Finance, 2015).

Since the logic behind the installment of insurance pools is the same as the logic that single insurers apply for their portfolios, only on a larger scale (see Kraut, 2014), this model enables the analysis of insurance pools. For instance, the model allows the analysis of effects connected with the portfolio size n^{PI} for a pool solution on primary insurer level. In addition, with the pool scheme cyber insurance collectives and experience with cyber risk increase. This both reduces uncertainty such that smaller security loadings for the premiums should be possible (see, e.g., Gatzert and Schmeiser, 2012).

3 Empirical Results

3.1 Model Calibration

Utility Function

The function used in the results is defined by

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

with $\alpha \geq 0$, being the risk-aversion parameter (see, e.g., Carmona, 2009). For the definition of an appropriate utility function we face two challenges. First, not all of the general utility approaches are applicable (e.g., utilities with constant relative risk aversion; see Ikefuji et al., 2014) because cyber losses are heavy-tailed (see Eling and Wirfs, 2016b). Second, most of the utility functions assume that the wealth *w* is non-negative. For the extreme losses that will occur in the simulation approach, we would have to assume unrealistically high amounts of initial capital to keep the final wealth states positive.[13] We choose the above utility function because it allows for non-negative wealth states, and can easily be implemented in a simulation approach. Furthermore, it allows analyses of diversification effects in the insurance portfolios (see, e.g., Gatzert and Schmeiser, 2012).[14]

Risk Transfer Instruments

Analyses of insurance policies for cyber risk indicate that contracts are defined with cover limits (Biener et al., 2015). In addition, we incorporate deductibles to allow for moral hazard prevention. The indemnity function $I^{PI}(X)$ in the primary insurance market is thus defined by

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

where C denotes the cover limit and D the deductible. Cummins and Mahul (2004) analyze effects connected to insurance contracts with upper limits on coverage. Their main result is that risk-averse policyholders accept deductibles greater than zero in the presence of cover limits. For the reinsurance contract I^{RE} we choose a similar approach as for the primary insurance contract. We define I^{RE} as

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

D^{RE} denotes the retention level, and C^{RE} defines the cover limit. In this paper we look at an excess-of-loss reinsurance contract with an upper limit, i.e., $C^{RE} < \infty$.

Premiums

We define the premiums P^{RO} (for the risk transfer instrument I^{PI}) and P^{PI} (for the risk transfer instrument I^{RE}) by the expectation pricing principle described in Embrechts (2000). Premiums are defined as

$$P=(1+\lambda)\cdot E\left[I\left(X;C,D\right)\right],$$

where $E[I(X; C, D)]$ (expected value of the indemnity payment) is the net premium and $\lambda\cdot E[I(X; C, D)]$ a (proportional) uncertainty loading (with $\lambda \geq 0$). The motivation for this loading is provided in Kunreuther, Hogarth, and Meszaros (1993). The authors find that actuaries,

[13] An additional solvency constraint for each individual resolves this problem. We present robustness results for such a constrained approach in Appendix C. The results underline our findings without such constraints.

[14] As a robustness test, we computed our results for an exponential utility function, which – according to Ikefuji et al. (2014) – provides an adequate model for the analysis. The results are similar to the findings in the main part of this paper, and are available upon request.

underwriters, and reinsurers are risk-averse when setting premiums for ambiguous and uncertain risks. Currently, cyber risks are still ambiguous and uncertain, so risk-averse pricing behavior can be expected. To account for expenses in the contract (e.g., for administration) we add a fixed risk loading λ_{fix} (i.e., $P = (1+\lambda)\cdot E[I(X;C,D)]+\lambda_{fix}$). For the assumption of a fair premium we set $\lambda = \lambda_{fix} = 0$.

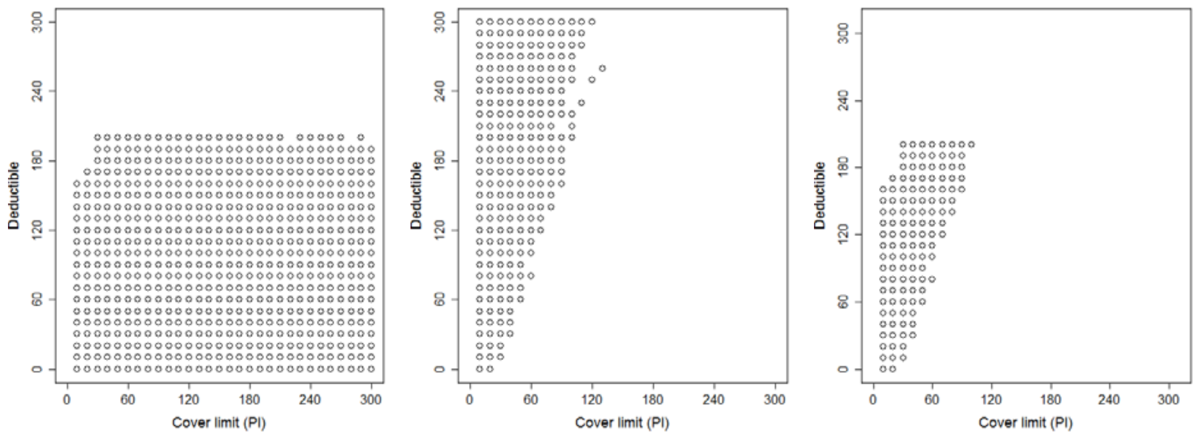
Further Parameters

The analysis depends on the definition of several parameters. Market observations and expert opinions (e.g., survey results from practitioners in the insurance industry; see Eling and Wirfs, 2016a) motivate the choice of model parameters. Table 2 summarizes all parameter values, with a short description and a rationale for their choice. Robustness tests to verify the results with respect to these assumption are available upon request.

3.2 Results of the Simulation Approach

In a first step we look closely at the relationship between the risk owner and the primary insurer and explain the evaluation approach described in Section 2.1. For the insurance contract I^{PI} defined in Section 3.1, we evaluate different combinations of cover limits C and deductibles D. For all combinations, we compute the risk owner's and primary insurer's utility with and without the insurance contract. These numbers are then used in constraints (1) and (2) of Section 2.1 to determine if the risk owner would buy and/or the primary insurer would offer the insurance contract. Figure 1 shows the *(C, D)*-combinations which are feasible for the risk owner (a), the primary insurer (b), and the solutions' overlap (c); in other words, all solutions that are present in both (a) and (b).

Figure 1 Results for the Risk Owner-Primary Insurer-Relationship (Reference)



(a) Risk owner (b) Primary insurer (c) Overlap

Table 2 Parameter Definition

Parameter	Value	Description	Motivation
Panel A: Reference Model with Risk Owner and Primary Insurer			
X	Random variable	Random variable describing the losses at the risk owner level. The losses are generated by resampling of cyber risk losses with replacement. A loss of size X occurs with probability p, and with a probability of $(1$-p) no loss occurs. See Appendix A how those assumptions are used to generate losses for the other risk transfer layers.	Standard model in actuarial science (e.g., Kaas et al., 2008, p. 18). Eling and Wirfs (2016b) analyze the distributional assumptions for cyber risk losses, and find that the generalized Pareto distribution (GPD) provides a reasonable fit for the cyber risk loss sample. We use resampling here, since the GPD estimated in Eling and Wirfs (2016b) is an infinite-mean model, and thus provides unstable estimates if used in loss generation (see, e.g., Chavez-Demoulin et al., 2015).
p	0.1	Probability that a loss of size X occurs	Based on findings in WEF (2010).
λ^{RO}	0.5	Risk loading factor for security loading in primary insurance premiums	Based on historical loss ratios and expert opinions: loss ratios for the top 50 global property/casualty markets are on average 73% for 2010-2014 (Aon Benfield, 2014). We approximate the security loading by the inverse of the loss ratio (minus 1), which is 0.36 for the numbers above. The survey in Eling and Wirfs (2016a) shows that general property/liability contracts have a loading of 0.3. For new types of risk additional safety loadings of 0.2 are added to this amount.
$\lambda^{RO\text{-}fixed}$	US\$1 m	Fixed loading, describes costs in primary insurance premiums	Based on historical expense ratios and expert opinions (survey in Eling and Wirfs, 2016a).
α^{RO}	6.0	Risk owner's risk aversion parameter in the mean-standard deviation-utility function	The parameter is motivated by the choice in Müller, Schmeiser, and Wagner (2011). Parameters greater than zero indicate risk aversion.
α^{PI}	5.0	Primary insurer's risk aversion parameter in the mean-standard-deviation-utility function	Since primary insurers have the opportunity to diversify more adequately than individuals, we assume $\alpha^{PI} < \alpha^{RO}$.
n^{PI}	50	Number of policies in the primary insurer's portfolio	Based on expert opinions (survey in Eling and Wirfs, 2016a). For the diversification effects analysis we present results for n^{PI} = 100 and 500.
Panel B: Risk Transfer by Reinsurance			
λ^{PI}	0.5	Risk loading factor for security loading in reinsurance premiums	Based on historical loss ratios and expert opinions; see also λ^{RO}.
$\lambda^{PI\text{-}fixed}$	US\$3 m	Fixed loading, describes costs in reinsurance premiums	Based on historical expense ratios and expert opinions.
α^{RE}	4.0	Reinsurer's risk aversion parameter in the mean-standard deviation-utility function	Since reinsurers have the opportunity to diversify more adequately than primary insurers, we assume $\alpha^{RE} < \alpha^{PI}$.
n^{RE}	10	Number of policies in the reinsurer's portfolio	Based on expert opinions (survey in Eling and Wirfs, 2016a).
D^{RE}	US\$80 m	Retention level in the excess-of-loss reinsurance contract	We test contract designs with retention levels between US\$10 and 300 million, in combination with cover limits between US\$10 and 500 million and identified D^{RE} and C^{RE} as the design with the best results.
C^{RE}	US\$100 m	Cover limit in the excess-of-loss reinsurance contract	
Panel C: Risk Transfer by Capital Market Solution issued (a) by the Primary Insurer and (b) by the Reinsurer			
B	(a) US\$500 m (b) US\$500 m	Face value of the cyber risk catastrophe bond	(a) We test face values between US\$10 million and US\$500 million, and identified the one with the best results; (b) We test face values between US\$10 million and US\$500 million, and identified the one with the best results.
AP	(a) US\$80 m (b) US\$50 m	Attachment point of the cyber risk catastrophe bond – the amount which must be exceeded by the loss before the bond pays an indemnity	(a) This model presents an alternative to the reinsurance contract; therefore, we assume that the amount that has to be covered by the primary insurer is equal to the one in Panel B; (b) This value was up to variation, since the introduction of a risk transfer mechanism for the reinsurer was not in place in another model before. We choose the one that generates the biggest effect on the overall solutions in the reference model.
K	= B	Maximal payment from the cyber risk catastrophe bond	This parameter is similar to a cover limit in the reinsurance contract. In case the loss above the AP exceeds K all initial payments of the investor are used to cover the losses (worst outcome for investor).
$r^{Zero\text{-}Coupon}$	3%	Rate of return for the zero-coupon catastrophe bond	This value is motivated by the average over USA 10-year zero-coupon yields for the last ten years (which is approximately 3.2%).
r_f	1%	Risk-free interest rate (necessary to determine the excess return in the Sharpe ratio)	Chosen relatively high in the current low-interest environment. It is only used in the computation of the Sharpe ratio where it leads to a conservative investor's decision criterion, if it is too high (see Section 2.4).
Sharpe ratio	0.6	The Sharpe ratio: benchmark that must be exceeded by the investment such that the investor will buy the instrument	The Sharpe ratio assumed in Kunreuther, Kleindorfer, and Grossi (2005) is 0.6. They ground this value on historical data. Investors will at least require the same benchmark for the uncertain and innovative risk category of cyber risk (even higher security premiums would be realistic).
Panel D: Further Parameters for the Insurability Challenges Analysis			
β	0.00008	Parameter that indicates the effectiveness of mitigation instruments	Parameter choice analog to the approach in Kelly and Kleffner (2003).
r	(a) US\$ -0.5/-0.25m (b) US\$ 0.5/0.25m	(a) Case with Moral Hazard (b) Instruments for risk mitigation in place	Parameters chosen such that effects are observable in the analysis. Robustness test are available upon request.

Note: m = million.

The results for the risk owner indicate that if cover limits are included in the insurance contract, risk owners will accept deductibles. Initial verification tests indicate that the maximum deductible (with respect to a fixed cover limit), under which insurance contracts are still bought, increases with higher premiums and greater risk aversion. Furthermore, the maximal acceptable deductible decreases with a growing cover limit (significant changes are only observable if higher values for the cover limits are plotted). All these effects are in line with the findings of papers that also analyze insurance contracts of the form I^{PI} (e.g., Cummins and Mahul, 2004). The primary insurer, would only offer insurance contracts with cover limits of maximal US$100 million, which is close to the values in the market (see, e.g., Finkle, 2015). The final result shows that only insurance contracts with deductibles up to about US$200 million and cover limits of about US$100 million are acceptable for both parties. Thus, an insurance market is possible only for constellations within these limits.

Figure 1 depicts our analysis of the simulation approach. We evaluate the impact of the risk transfer instruments, discussed in Sections 2.3-2.5, on the cyber insurance market development. We analyze how the solution sets (Figure 1) change if a reinsurer or capital market investor provides risk transfer for the primary insurer. We measure this by the ratio of feasible insurance policy designs (area in Figure 1(c)) to the total number of contract designs tested. In addition, we estimate the average and total premiums that can be generated by these feasible solutions. The results for the example in Figure 1 are presented in the reference model, Panel A of Table 3. This table also depicts the further analyses.

The results in Panel A of Table 3 show that the insurance market without any further risk transfer opportunities for the primary insurer is very small. If we introduce reinsurance contract or capital market solutions the market size increases only slightly, measured by the number of feasible insurance policies. However, average premiums increase significantly (from US$204,000 to US$518,000 in the case of a capital market solution issued by the primary insurer). This indicates that the new feasible contract designs – although there are only a few – cover significantly higher losses from the risk owner than the contracts that would be offered without further risk transfer for the primary insurer. Thus, the inclusion of a reinsurer or a capital market increase primary insurer’s ability to offer insurance contracts with higher cover limits and/or lower deductibles, compared to the situation without those risk transfer opportunities.

Table 3 Market Development with Reinsurance and Capital Market Solutions under Challenges in the Insurability

	Reference		**Reinsurance**		**Capital Market (a)**		**Capital Market (b)**	
	Total Solutions (in %)	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**
Panel A: Reference Setup								
Scenario 1 (Base)	12.279	0.204 (24.065)	13.215	0.271 (34.471)	13.632	0.518 (67.830)	12.279	0.295 (34.774)
Panel B: Scenario Analysis – Dynamic Nature of Cyber Risk								
Scenario 2 (Extreme)	9.781	0.308 (28.914)	10.510	0.377 (38.045)	10.926	0.629 (66.093)	9.990	0.392 (37.595)
Scenario 3 (Worst-case)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
Panel C: Correlation in Portfolios								
PI – Low (q = 5%)	9.469	0.262 (23.841)	10.406	0.341 (34.050)	10.718	0.584 (60.199)	9.469	0.351 (31.957)
PI – Medium (q = 20%)	8.741	0.354 (29.706)	8.949	0.479 (41.237)	9.886	0.685 (65.046)	9.053	0.441 (38.344)
PI – High (q = 50%)	6.452	0.711 (44.066)	6.868	0.919 (60.654)	7.284	0.920 (64.417)	6.556	0.730 (46.011)
Panel D :Information Asymmetry – Moral Hazard[15]								
r = US$ -0.5m invested	15.505	0.181 (26.960)	---	---	---	---	---	---
r = US$ -0.25m invested	13.424	0.197 (25.472)	---	---	---	---	---	---
r = US$ 0.25m invested	12.279	0.204 (24.065)	---	---	---	---	---	---
r = US$ 0.5m invested	10.302	0.218 (21.571)	---	---	---	---	---	---
Panel E: Effect of Primary Insurer's Portfolio Size								
Medium (100 contracts)	20.812	0.286 (57.208)	20.916	0.317 (63.786)	20.916	0.409 (82.170)	20.916	0.294 (59.159)
Large (500 contracts)	78.148	0.692 (519.723)	81.790	0.707 (555.739)	78.148	0.269 (202.375)	78.148	0.570 (428.312)

Note: PI = primary insurer, m = million.

[15] Since the primary insurer is not able to observe changes in the risk owner's exposure, the cash-flows at the primary insurer level are equal to the reference setup under Panel A. Thus, results for reinsurance, capital market models (a) and (b) are equal to this setup, and thus not shown or discussed here.

We also observe that with increasing severity of losses (Panel B), market size decreases. In particular, for the worst-case scenario in which no simulated insurance contract is appropriate, a cyber insurance market is non-existent. Although reinsurance and capital market solutions can increase market size for the extreme scenario, they cannot compensate for the complete decrease in market size. This makes risk transfer mechanisms that have not been analyzed in the first four models vital; in other words, governmental intervention. It indicates that the appropriateness of risk transfer solutions depends on the dynamic nature of cyber risk and underlines the importance of this challenge in insurability.

The analysis of correlations in the primary insurer's portfolio (Panel C) indicates that correlation shrinks market size and is harmful to market development. This finding is in line with Böhme and Kataria (2006) who find that cyber insurance markets can thrive only when there are small correlations in insurance portfolios (low global correlation).[16] The risk transfer by reinsurance and capital market solutions cannot fully offset these declines. The correlation of cyber risk incidents is thus a serious problem for the development of a mature cyber insurance market.

Asymmetric information is another obstacle to cyber risk's insurability. On the one hand we observe (Panel D) that the reduction of risk by mitigation decreases market size. This is explained by the fact that these measures reduce the risk owner's exposure, but because primary insurers cannot observe these changes, premiums are not adjusted and thus remain too high for the risk owner's exposure. Furthermore, we observe that investments must surpass a critical value (e.g., investments of US$ 0.5 million change market size, while US$ 0.25 million do not). On the other hand if risk owners disinvest (i.e., they reduce or fail to update their security standards) insurance markets increase, because the premiums are too low compared to the actual risk owner's exposure. Therefore, moral hazard increases demand for cyber risk insurance.

According to Biener, Eling, and Wirfs (2015) risk pools are too small and thus efficient diversification is impaired. The analysis shows (Panel E) that increases in primary insurance portfolios significantly increase market size. As for the base scenario (Panel A) the introduction of reinsurance or capital market solutions does not significantly increase the number of feasible contract designs, but it does increase the insurance premiums charged. This indicates the generation of potentially more feasible contracts for the risk owner (i.e., lower deductibles and/or higher cover limits). The results also show that the growth in risk pools has a greater impact on

[16] This result is also in line with the findings of Böhme (2005) who shows that a large part of the market cannot be supplied because of correlated claims.

market development than does the introduction of additional risk transfer mechanisms. The results are based on the law of large numbers, according to which the variance of mean losses decreases if portfolios of mutually independent risks increase. Independence is given for the analysis in Panel E and is the crucial assumption for the observed result (that any increase in portfolio size is beneficial for market development). However, correlation between cyber risk incidents is a challenge to the insurability of cyber risk and independence is not necessarily given. The next section gives a detailed analysis of increased portfolios by the means of an insurance pool solution with respect to the challenges of insurability.

3.3 Impact of Governmental Intervention

In our model, the government can intervene in the cyber insurance market in two ways: (1) the state provides the framework for the implementation of an insurance pool; and (2) it sets a minimum standard for mitigation. For the analysis of (1) we define a primary insurance pool consisting of a merger of ten of our exemplary insurance companies; they generate a portfolio of 500 policies. From Table 3, Panel E, we know that an increase in portfolio size is conducive to market development. Furthermore, due to the expanded collective and, thus, potentially more experience, uncertainties with cyber risk decrease and lower security loadings for insurance premiums are possible (see, e.g., Gatzert and Schmeiser, 2012). Therefore, we further reduce the security loading factor from $\lambda^{RO} = 0.5$ to $\lambda^{RO} = 0.3$. The effect of smaller loading factors can be twofold. First, if loadings are smaller, premiums decrease, which makes some insurance contract designs more attractive for risk owners. Second, smaller loadings lead to smaller revenues for the primary insurer, making some insurance contracts unattractive to underwrite. The effect on the market development is thus ambiguous. In combination with an increasing portfolio size, we cannot provide a hypothesized effect for the market development at all.

For the given definition of an insurance pool, the results in Table 4 show that the installment fosters market development. However, its effect on market development is smaller in total solutions than for a single increase in portfolios size (see Panel E of Table 3 for 500 contracts). This indicates that the effects of decreasing loading factors described for the primary insurer outweigh the effect for the risk owner. However, under the insurance pool approach average premiums rise, indicating that insurance contracts with higher cover limits and/or lower deductibles can be offered to risk owners. The insurance pool solution can also foster market development for extreme scenarios. These diversification effects work only in cases when losses are independent (law of large numbers). If losses in the portfolio correlate, the benefits of the diversification effect diminish (Panel C in Table 4). Nevertheless, markets are still bigger for an insurance pool solution and correlated losses than in the reference insurance market with correlated losses (Panel C, column (1) of Table 4).

Table 4 Market Development with an Insurance Pool Solution

	(1) Reference (analog to Table 3)		**(2) Insurance Pool** (Primary insurance market without further risk transfer opportunities)	
	Total Solutions (in %)	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**
Panel A: Reference Setup				
Scenario 1 (Base)	12.279	0.204 (24.065)	64.152	1.514 (938.613)
Panel B: Scenario Analysis – Dynamic Nature of Cyber Risk				
Scenario 2 (Extreme)	9.781	0.308 (28.914)	47.555	1.904 (870.352)
Scenario 3 (Worst-case)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
Panel C: Correlation in Portfolios				
PI – Low (q = 5%)	9.469	0.262 (23.841)	53.798	1.674 (865.539)
PI – Medium (q = 20%)	8.741	0.354 (29.706)	44.121	2.091 (886.531)
PI – High (q = 50%)	6.452	0.711 (44.066)	37.357	3.160 (1134.294)

Note: PI = primary insurer, m = million.

The analysis in Table 4 shows that a pool solution is well suited to foster the growth of the cyber insurance market. However, high correlations and increases in severity of losses reduce their effectiveness (Panel B and C of Table 4). Nevertheless, our analysis shows that market size still increases even under correlation compared to the reference market. In addition, the installment of an insurance pool has advantages that have not yet been incorporated into this model. For instance, the pool could encourage information and data sharing, and facilitate the definition of standards and best practices (see, e.g., Long Finance, 2015). All these would reduce uncertainty, and eventually lead to an increase in market size.

For the analysis of minimum mitigation standards, the primary insurer can monitor the status of the mitigation measures, and adjust the premiums accordingly. For the analysis of a minimum mitigation standard we assume a government that forces every risk owner to invest US$ 0.5 million in risk mitigation. The analysis in Panel D of Table 3 shows that security investments decrease market size, since the risk owner's exposure and the charged premiums for insurance do not align for some contract designs. If the insurer adjusts the premium to the risk owner's lower exposure, the market size further decreases in number of total solutions (see Table 5, Panel A). The adjustment decreases primary insurer's revenues to the point that some contract designs might cease to be feasible. However, markets increase slightly with respect to the average premium measure. We observe a similar effect for the extreme scenario (see Panel

B of Table 5). Thus, the installment of a minimum standard for mitigation could increase premiums. Furthermore, in Panel C of Table 5 we observe that the installment of a minimum mitigation standard is beneficial in the presence of correlated losses in portfolios.

Table 5 Market Development with Minimum Mitigation Standards

	(1) Mitigation Model (Mitigation Unknown to PI)		**(2) Minimum Mitigation Standard**	
	Total Solutions (in %)	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**
Panel A: Reference Setup				
r = US$ 0.5m invested in Scenario 1 (Base)	10.302	0.218 (21.571)	9.781	0.220 (20.656)
Panel B: Scenario Analysis – Dynamic Nature of Cyber Risk				
Scenario 2 (Extreme)	6.660	0.363 (23.201)	6.660	0.369 (23.640)
Scenario 3 (Worst-case)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
Panel C: Correlation in Portfolios				
PI – Low (q = 5%)	9.469	0.262 (23.841)	9.261	0.262 (23.362)
PI – Medium (q = 20%)	5.619	0.432 (23.330)	5.931	0.442 (25.179)
PI – High (q = 50%)	6.243	0.622 (37.302)	6.452	0.711 (44.065)

Note: PI = primary insurer, m = million.

4 Conclusion

This paper investigates potential risk transfer schemes for cyber risk that can improve its insurability and foster market development. To the best of our knowledge, we are the first to use a simulation to compare different risk transfer options for cyber risk, incorporating all relevant stakeholders and most of the challenges in the insurability of cyber risk.

Our results show that the current market is relatively small. Furthermore, we observe that the incorporation of reinsurance and capital market solutions can increase market size. It is thus interesting to promote those layers for cyber risk in the future. For instance, a better understanding of cyber risk, its aggregation and modeling is necessary to securitize cyber risks by cyber cat bond products (see, e.g., Traynor, 2016). The analysis also shows that challenges in insurability have a significant impact on the market size, especially the risk of change and correlations in portfolios. Insurance pools could be an effective instrument to increase market size, also under extreme scenarios. Unfortunately, insurance pools become less effective in the presence of correlation in portfolios. Nevertheless, the introduction of an insurance pool can have further advantages. For instance, the pool could encourage information and data sharing, and facilitate the definition of standards and best practices (see, e.g., Long Finance, 2015). The incorporation and discussion of insurance pools should thus be impelled by insurance companies and regulators. Similar approaches already proven useful for other risk categories (e.g., natural catastrophes, terrorism, or D&O insurance) that also exhibited significant challenges in insurability. The installment of a minimum standard for mitigation proved to be useful in the presence of correlation in portfolios, albeit to a very small extent. Thus, regulators should start discussing their introduction. The interplay of minimum standards for mitigation and insurance pools to account for the challenges in insurability of cyber risk needs to be on the agenda in such discussions. Finally, debates over solutions for worst-case scenarios, as discussed in WEF (2010) and Ruffle et al. (2014), are inevitable. Those discussions should also involve an active role of the government in the risk transfer for such a worst-case scenario (e.g., discussions about a governmental backstop; see Long Finance, 2015).

Our model takes all stakeholders into account. For the sake of simplicity, we have to accept some limitations. Certain aspects and assumptions in the model framework in addition to the analytical approach require discussion. First of all, we assume all policyholders to be identical in risk exposure (all face the same losses) and in initial capital. Based on this assumption we can offer standardized insurance contracts (i.e., same cover limits, deductibles, and premiums). However, this assumption of homogeneity is simplistic and does not coincide with market observations. According to Biener et al.'s (2015) study of cyber insurance contracts in Switzerland, policies are constructed of different modules, from which policyholders can select the coverage that best satisfies their needs. In addition, insurance companies offer different cover limits based on up-front assessments of IT security systems. Furthermore, under the assumption of heterogeneity, we would have to expect problems of adverse selection. Therefore, simplification results in a conservative estimation since adverse selection would lead only to further decreases in market size (see, e.g., the lemons problem described in Akerlof, 1970).

Second, we simplified the modeling of the cyber cat bond: (i) cat bonds are a multi-year protection (see, e.g., Ben Ammar, Braun, and Eling, 2015), but the assumption of a one-year contract as common in reinsurance might not be feasible; (ii) investors do not solely price the value of a cat bond by a Sharpe ratio. They might also incorporate metrics like the spread as a measure of expected loss in their decision processes. Future research is needed to model cat bonds for cyber risk in more detail.

Third, under the paper's model setup, insurance and reinsurance companies have no opportunity to invest in alternative assets when no insurance is offered; the reference values (e.g., $E[U^{PI}(A_{0,PI})]$ in constraint (2)) could be too small. This could lead to estimators for market size that are potentially too high. One way to adjust the model is to replace the fixed initial capital by a stochastic process (see, e.g., Hong et al., 2011). This would complicate the model and future research is needed to examine ways to incorporate stochastic processes within such a model.

Finally, the interaction of minimum standards for mitigation and insurance pools was not evaluated in this model and creates an avenue of future research. The incorporation of self-protection measures (instruments to reduce the probability of loss occurrence; see Ehrlich and Becker, 1972) have been analyzed in comparison with insurance by Öğüt et al. (2011). The effect of self-protection measures on the cyber insurance market has not been tested in detail (see Eling and Wirfs, 2016a, for a first indication) and their interplay with mitigation standards could be another important topic for future analyses.

References

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

Akerlof, G. A. (1970) 'The Market of "Lemons": Quality Uncertainty and the Market Mechanism', The Quarterly Journal of Economics 84(2): 488-500.

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

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

Artemis (2016) 'Credit Suisse operations risk cat bond SPI, Operational Re, registered', published May 4th, 2016, http://www.artemis.bm/blog/2016/05/04/credit-suisse-operational-risk-cat-bond-spi-operational-re-registered/, last accessed: August 23, 2016.

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.

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

Biener, C., Eling, M., Matt, A., and Wirfs, J. H. (2015) 'Cyber Risk: Risikomanagement und Versicherbarkeit', I.VW Schriftenreihe, Band 54, St. Gallen.

Biener, C., Eling, M., and Wirfs, J. H. (2015) 'Insurability of Cyber Risk – An Empirical Analysis', The Geneva Papers on Risk and Insurance – Issues and Practice 40(1): 131-158.

Böhme, R. (2005), ‚Cyber-Insurance Revisited,' 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, Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006), University of Cambridge, U.K..

Böhme, R., and Schwartz, G. (2010) 'Modeling Cyber-Insurance: Towards A Unifying Framework', Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA.

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.

Carmona, R. (2009) 'Indifference Pricing: Theory and Applications', Princeton University Press.

Chavez-Demoulin, V., Embrechts, P., and Hofert, M. (2015) 'An Extreme Value Approach for Modeling Operational Risk Losses Depending on Covariates', The Journal of Risk and Insurance, forthcoming.

Cirillo, P., and Taleb, N. N. (2015) 'Expected shortfall estimation for apparently infinite-mean models of operational risk', Quantitative Finance, forthcoming.

Cossette, H., Gaillardetz, P., Marceau, E., and Rioux, J. (2002) 'On two dependent individual risk models', Insurance: Mathematics and Economics 30(2): 153-166.

Cummins, J. D., and Mahul, O. (2004) ‘The Demand for Insurance with an Upper Limit on Coverage’, The Journal of Risk and Insurance 71(2): 253-264.

Doherty, N., and Schlesinger, H. (1990) ‘Rational Insurance Purchasing: Consideration of Contract Nonperformance. Quarterly Journal of Economics 105(1): 243-253.

Ehrlich, I., and Becker, G. S. (1972) ‘Market Insurance, Self-Insurance, and Self-Protection‘, Journal of Political Economy 80(4): 623-648.

Eling, M., and Wirfs, J. H. (2016a) ‘Cyber Risk: Too Big to Insure? – Risk Transfer Options for a Mercurial Risk Class’, I.VW Schriftenreihe, Band 59, St. Gallen.

Eling, M., and Wirfs, J. H. (2016b) ‘Cyber Risk is Different’, Working Paper Series on Risk Management and Insurance, Institute of Insurance Economics, University of St. Gallen, August 2016.

Embrechts, P. (2000) ‘Actuarial versus Financial Pricing of Insurance’, The Journal of Risk Finance 1(4), 17-26.

European Union (2016) ‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)’, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, last accessed: June 24, 2016.

Finkle, J. (2015) ‘Ace offers $100 million cyber policies with added services, scrutiny’, http://www.reuters.com/article/2015/09/24/us-ace-ltd-cyberinsur-anceidUSKCN0RO2LD20150924#epgXi5Y5uU11kXSA.97, last accessed: November 05, 2015.

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

Golubin, A. Y. (2014) ‘Optimal insurance and reinsurance policies chosen jointly in the individual risk model’, Scandinavian Actuarial Journal, http://dx.doi.org/10.1080/03461238.2014.918696, last accessed: December 02, 2015.

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

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.

Hong, S. K., Lew, K. O., MacMinn, R., and Brockett, P. (2011) ‘Mossin’s Theorem given Random Initial Wealth’, The Journal of Risk and Insurance 78(2), 309-324.

Ikefuji, M., Laeven, R. J. A., Magnus, J. R., and Muris, C. (2014) ‘Expected Utility and Catastrophic Risk’, Working Paper.

Insurance Information Institute (III) (2003) ‘Cyber Insurance’, http://www.iii.org/media/hottopics/insurance/cyberinsurance/content.print/, last accessed: June 10, 2015.

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

Kelly, M., and Kleffner, A. E. (2003) ‘Optimal Loss Mitigation and Contract Design’, The Journal of Risk and Insurance 70(1): 53-72.

Kleindorfer, P. R., and Klein, R. W. (2003) ‚Regulation and Markets for Catastrophe Insurance‘, in: M. R. Sertel, S. Koray (eds.), Advances in Economic Design, Berlin: Springer, 263-280.

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

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

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

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

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

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

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

McAfee (2014) ‘Net Losses – Estimating the Global Cost of Cybercrime’, http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf, last accessed: October 16, 2015.

Mossin, J. (1968) ‘Aspects of Rational Insurance Purchasing’, Journal of Political Economy 76(4): 553-568.

Müller, K., Schmeiser, H., and Wagner, J. (2011) ‘Insurance Claims Fraud: Optimal Auditing Strategies in Insurance Companies’, Working Papers on Risk and Insurance No. 92.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. (2013), 'Cyber-risk decision models: To insure IT or not?', Decision Support Systems 56(1): 11-26.

OECD (2005) 'Terrorism Risk Insurance in OECD Countries, Policy Issues in Insurance No. 9', OECD Publishing.

Öğüt, 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.

Outreville, J.-F. (2013) 'Insurance Markets in Developing Countries: Economic Importance and Retention Capacity', in: G. Dionne (ed.), Handbook of Insurance, New York: Springer Science+Business Media, 941-956.

Pandey, P., and Snekkens, E. (2016) 'Using Financial Instruments to Transfer the Information Security Risk', Future Internet 8(20), doi:10.3390/fi8020020.

Ruffle, S. J., Bowman, G., Caccioli, F., Coburn, A. W., Kelly, S., Leslie, B., and Ralph, D. (2014) 'Stress Test Scenario: Sybil Logic Bomb Cyber Catastrophe', Cambridge Risk Framework series; Center for Risk Studies, University of Cambridge.

Schlesinger, H. (2013) 'The Theory of Insurance Demand', in: G. Dionne (ed.), Handbook of Insurance, New York: Springer Science+Business Media, 167-184.

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.

Traynor, P., Crisp, D., Wagstaff, R., Cruickshank, C., and Mulvihill, K. (2016) 'Insurance Linked Securities – Cyber Risk, Insurers and the Capital Markets', https://www.bnymellon.com/emea/en/our-thinking/insurance-linked-securities-cyber-risk-and-the-capital-markets.jsp, last accessed: August 23, 2016.

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

Appendix A: Loss Modeling Approach

Risk Owner

For the simulation approach defined in Section 2, the definition of risk exposure for each layer is vital. The risk owner's exposure to cyber risk X is generated from cyber risk loss data. We use the *SAS OpRisk Global data* and identify cyber incidents by the search and identification strategy described in Appendix B. For descriptive statistics on the data sample and a motivation to use OpRisk data for cyber risk we kindly refer the reader to Eling and Wirfs (2016b).

Assume the distribution function F_Y to describe the identified loss data ($X_1, X_2, X_3, \ldots$). So far F_X does not incorporate the possibility of a risk owner to have no loss. We compute a mixed distribution, by assuming that a company faces a loss Y which is defined by

$$Y = X \cdot Z \,,$$

where Z is a random variable, with values $Z = 1$ (a loss has occurred) or $Z = 0$ (no loss occurred). Further, we define $p = P[Z = 1]$, with $0 \leq p \leq 1$ fixed. Under these assumptions, we can define the distribution of the risk owner by

$$F_Y\left(x\right) = p \cdot F_X(x) + (1-p) \cdot \delta\left(0\right),$$

where $\delta(0)$ is the delta distribution (Dirac) which is equal to 1 if $x = 0$ and 0 in all other cases. Based on this loss distribution, we generate random loss numbers by standard random number generators (e.g., given in the statistical software packages of R). In a first step we generate losses for X by resampling with replacement on the original loss data from the SAS OpRisk Global database (see Eling and Wirfs, 2016b, for descriptive statistics). Second, as a robustness test, we fit the loss data to a log-normal distribution and generate losses thereof (see Appendix C).

While the risk owner faces having either a cyber risk loss of a particular size or no loss at all, the primary insurer (reinsurer) faces losses in a portfolio of losses. Something similar applies to the capital market, which takes over risks from a primary insurer's (model (a)) or a reinsurer's (model (b)) portfolio. The loss simulation approach for each of the other layers is described in the following paragraphs.

Primary Insurer

There are two ways to derive a distribution for the loss portfolio of the primary insurer from the risk owner's loss distribution: individual risk model and collective risk model. For an extensive review see Kaas et al. (2008) or Klugman, Panjer, and Willmot (2012). We will follow the individual risk model. The model is based on the loss distribution of the risk owner F_X. Because of the simulation approach, we will not need the exact distribution for the primary insurer's loss L^{PI}. Thus, we generate random losses on risk owner level by the distribution F_Y and apply the indemnity function I^{PI} to them. By aggregating n^{PI} of these losses, we yield an aggregated random loss for L^{PI}.

Reinsurer

The loss distribution of a reinsurer is similar to that of the primary insurer. The only difference is that the total loss of the reinsurer's portfolio L^{RE} is based on losses in the primary insurers' portfolio L^{PI}. As before, we generate random losses L^{PI}, apply I^{RE} to it, and aggregate them to a loss of a reinsurer's loss portfolio L^{RE} with n^{RE} contracts.

Capital Markets

Losses for the capital market layer depend on the model in which they are incorporated. In model (a) the capital market loss is equal to the loss in a primary insurer portfolio and is modelled analogously. For model (b), the capital market covers losses in a reinsurer's portfolio, and thus is modelled analogous to the reinsurer losses. Depending on the layer, the losses are determined analogously to the primary insurer's loss L^{PI} or the reinsurer's loss L^{RE}.[17]

Comments

Note, that we do not assume independent and identically distributed losses on each layer, as we would if we wanted to determine the actual loss distribution on each layer (see, e.g., individual risk model). The first advantage of this approach is, that we are able to generate correlated losses. The approach used to generate correlated losses is given by Cossette et al. (2002). Moreover, since we do not require the losses to be identically distributed, the approach enables the aggregation of losses for different underlying risks. For instance, the modeling of a portfolio consisting of different policyholders (e.g., different with respect to firm characteristics) can be done by Chavez-Demoulin, Embrechts, and Hofert (2015). However, we leave the latter for future research.

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

Appendix B: Search and Identification Strategy

To be categorized as a cyber risk incident, a loss event must meet three criteria: (1) a *critical asset* such as a company server or database needs to be affected, (2) a relevant *actor* (e.g., hackers, employees, system, nature) needs to be involved in causing the incident, and (3) a relevant *outcome* such as the loss of data or misuse of confidential data needs to be present (see Table B.1 for more information). 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 Table B.2). The resulting dataset includes 1,579 cyber risk incidents, or about 5.9% of the total sample of operational risks.

Table B.1 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 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 B.2 Keywords per Criterion

Critical Asset	Actor	Actor (cont.)	Outcome
account	*(1) Actions by people*	*(2) Systems and technical failure*	availability
accounting system	administrator	defect	available
address	deadline	hardware	breach
code	denial of service, DoS	loading	breakdown
communication	destruction	malicious code	confidential
computer	devastation	software	congestion
computer system	employee	stress	constrain
confidential	extortion	system crash	control
confidential document	forgot, forget, forgotten		delete
consumer information	hacker, hacked	*(3) Failed internal processes*	deletion
data	hacking	unauthorized access	disclosure
disk	human error		disorder
document	infect	*(4) External events*	disruption
file	infection	blizzard	disturbance
hard-disk	infiltrate	earthquake	encryption
hard-drive	infiltrated	eruption	espionage
homepage	key logger	explosion	failure
info(rmation)	lapse	fire	false
information system	logic bomb	flood	falsification
internet site	maintenance	hail	falsified
names	malware	heat wave	falsifying
network	manager	hurricane	incompatibility
numbers	manipulate	lightning	incompatible
online banking	miscommunication	natural catastrophe	incomplete
payment system	mistake	outage	integrity
PC	misuse	pipe burst	interruption
personal information	omission	riot	limit
phone	online attack	smoke	lose
purchase information	oversight	storm	loss
record	phish	thunder	lost
reports	phishing	tornado	malfunction
server	spam	tsunami	missing
site	Trojan	typhoon	modification
social security number	vandalism	unrest	modified
stored information	virus	utilities	modify
tablet	worm	war	overload
trade secret		weather	publication
webpage		wind	restrict
website			sabotage
			steal
			stole
			theft

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

Appendix C: Analysis of Robustness

This part of the appendix focuses on the robustness of the findings generated in the main part of this paper. We show results for solvency-constrained models, verify the assumption of risk-neutrality in insurer's decision-making, and the analysis with an alternative loss distribution assumption.

Solvency-constrained Models

The model in Section 2 assumes that all participants in the market are able to cover any (potentially residual) loss and pay any premium necessary. This is because we did not make any assumptions on the initial wealth/capital. However, this analysis is necessary since small companies in particular might not be able or willing to offer or by (re-)insurance products. In this section we test the robustness of our results with respect to company size by adding solvency constraints for each risk transfer layer. For all stakeholders we define the same constraints.

In constraint (1) we assume that the expected utility in the case with insurance must be greater than the expected utility without insurance. In addition to constraint (1) we define a second criterion for the risk owner based on a solvency requirement. This is in line with approaches discussed in Kleindorfer and Klein (2003) or Böhme and Schwartz (2010). We assume that the risk owner's ruin probability must be less than a target ruin probability TRP^{RO}. The constraint can thus be formalized as follows:

$$P\left[W_0 - X - P^{RO} + I^{PI}\left(X\right) < 0\right] \leq TRP^{RO}. \text{ (C.1)}$$

Only in cases that constraints (1) and (C.1) are satisfied, we define a market for the risk owner to be feasible. Similar constraints are defined for the primary insurer and the reinsurer. For example, for the primary insurer:

$$P\left[A_{0,PI} + P^{PI,earned} - L^{PI} < 0\right] \leq TRP^{PI}. \text{ (C.2)}$$

With these additional constraints, the definition of the initial wealth and capital becomes essential. We compute the models of Table 3 with the additional constraints and assume the following parameters in addition to those in Table 2: initial wealth of the risk owner is W_0 = US\$3 million with a TRP^{RO} = 5%; the primary insurer's initial capital is $A_{0,PI}$ = US\$100 million with a TRP^{PI} = 0.5% (motivated by Solvency II requirements), and the reinsurer's initial capital $A_{0,RE}$ = US\$100 million with TRP^{PI} = 0.5%. The results with solvency constraints are presented in Table C.1.

Further, note that under this setup an insolvency is still possible (e.g., in the example an insolvency of a primary insurer equals 0.5%). This chance of a contract non-performance of the insurer should be included in the risk owner's decision to buy insurance. There are already approaches that account for this; for instance, Doherty and Schlesinger (1990). We leave this to future research.

Risk-neutrality Assumption in Insurance Companies

The results for the risk-neutrality assumption in the primary insurer's and reinsurer's decision process are based on the solvency-constrained model. Furthermore, we define risk-neutrality for the primary insurer and reinsurer by the assumption of $\alpha^{PI} = \alpha^{RE} = 0$. Initial wealth and capitals are chosen as in the solvency-constrained model, all other parameters are defined in Table 2. We present the results in Table C.2.

Loss Distribution Assumption

The assumption for the loss distribution of X (risk owner's risk exposure) is an important factor in the analysis of our model. According to Eling and Wirfs (2016b) the generalized Pareto distribution (GPD), provides the best fit for the loss modeling by single parametric distributions. However, we do not use this distributional assumption here, because the use of a GPD for the loss data at hand provides an infinite-mean model (see results of Eling and Wirfs, 2016b), which results in relatively unstable estimates if samples are drawn from it (see, e.g., Cirillo and Taleb, 2015). For a robustness test we thus use the log-normal distribution that proved to have the second best fit in Eling and Wirfs (2016b). Nevertheless, for the main part of the paper we resample losses from the original loss data with replacement. An advantage of this approach is that the maximal possible loss is bounded by the largest value in the sample. See Table C.3 for the results, analogous to Table 3.

Further Robustness Tests

Further robustness tests are available upon request (e.g., variations for the loss probability p, effects connected to the fixed risk loading factors λ_{fix}, as well as risk aversion parameters, and the utility function were analyzed and are available). We also investigated the effect of changes in reinsurance portfolio sizes (variable n^{RE}). Market size increases with increasing n^{RE}, but only to a small extent. This might be due to relatively small primary insurance portfolios that have to be increase first.

Table C.1 Robustness Test for Solvency-constrained Models

	Reference		**Reinsurance**		**Capital Market (a)**		**Capital Market (b)**	
	Total Solutions (in %)	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**
Panel A: Reference Setup								
Scenario 1 (Base)	12.071	1.198 (138.969)	13.007	1.267 (158.330)	12.279	1.510 (178.228)	13.007	1.295 (161.913)
Panel B: Scenario Analysis – Dynamic Nature of Cyber Risk								
Scenario 2 (Extreme)	0.104	2.687 (2.687)	0.104	2.748 (2.748)	0.104	2.874 (2.874)	0.104	2.477 (2.477)
Scenario 3 (Worst-case)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
Panel C: Correlation in portfolios								
PI – Low (q = 5%)	0.104	2.164 (2.164)	0.104	2.227 (2.227)	0.208	2.517 (5.033)	0.104	2.230 (2.230)
PI – Medium (q = 20%)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
PI – High (q = 50%)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
Panel D :Information asymmetry – Moral Hazard								
r = US$ -0.5m invested	28.928	1.308 (363.524)	---	---	---	---	---	---
r = US$ -0.25m invested	25.806	1.307 (324.218)	---	---	---	---	---	---
r = US$ 0.25m invested	8.949	1.221 (105.088)	---	---	---	---	---	---
r = US$ 0.5m invested	0.416	2.201 (8.804)	---	---	---	---	---	---
Panel E: Effect of Primary Insurer's Portfolio Size								
Medium (100 contracts)	19.459	1.262 (236.007)	19.771	1.315 (249.902)	19.459	1.389 (259.779)	19.771	1.289 (244.837)
Large (500 contracts)	27.055	1.336 (347.459)	27.471	1.346 (355.330)	27.055	1.200 (312.104)	27.471	1.249 (329.755)

Note: PI = primary insurer, m = million.

Table C.2 Analysis for Risk-Neutral Insurers

	Reference		Reinsurance		Capital Market (a)		Capital Market (b)	
	Total Solutions (in %)	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**
Panel A: Reference Setup								
Scenario 1 (Base)	22.060	1.299 (273.387)	22.268	1.353 (289.540)	22.060	1.557 (330.173)	22.268	1.352 (289.292)
Panel B: Scenario Analysis – Dynamic Nature of Cyber Risk								
Scenario 2 (Extreme)	0.104	2.687 (2.687)	0.104	2.748 (2.748)	0.104	2.874 (2.874)	0.104	2.477 (2.477)
Scenario 3 (Worst-case)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
Panel C: Correlation in portfolios								
PI – Low (q = 5%)	0.416	2.533 (10.132)	0.416	2.604 (10.415)	0.416	2.664 (10.657)	0.416	2.333 (9.334)
PI – Medium (q = 20%)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
PI – High (q = 50%)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
Panel D :Information asymmetry – Moral Hazard								
r = US$ -0.5m invested	28.928	1.308 (363.524)	---	---	---	---	---	---
r = US$ -0.25m invested	25.806	1.307 (324.218)	---	---	---	---	---	---
r = US$ 0.25m invested	9.053	1.222 (106.322)	---	---	---	---	---	---
r = US$ 0.5m invested	0.520	2.269 (11.345)	---	---	---	---	---	---
Panel E: Effect of Primary Insurer's Portfolio Size								
Medium (100 contracts)	23.517	1.299 (293.656)	23.621	1.337 (303.560)	23.517	1.405 (317.433)	23.621	1.295 (294.001)
Large (500 contracts)	26.951	1.336 (346.083)	27.367	1.345 (353.781)	26.951	1.200 (310.919)	27.367	1.250 (328.724)

Note: PI = primary insurer, m = million.

Table C.3 Robustness Test for Distributional Assumption

	Reference		Reinsurance		Capital Market (a)		Capital Market (b)	
	Total Solutions (in %)	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**	**Total Solutions (in %)**	**Average (Total) Premium (in million US$)**
Panel A: Reference Setup								
Scenario 1 (Base)	20.395	0.129 (25.273)	21.748	0.199 (41.559)	29.344	0.435 (122.624)	21.952	0.227 (47.708)
Panel B: Scenario Analysis – Dynamic Nature of Cyber Risk								
Scenario 2 (Extreme)	12.591	0.253 (30.606)	13.944	0.325 (43.571)	14.776	0.570 (80.911)	13.944	0.349 (46.827)
Scenario 3 (Worst-case)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)	0.000	0.000 (0.000)
Panel C: Correlation in portfolios								
PI – Low (q = 5%)	16.337	0.159 (25.010)	16.337	0.221 (34.630)	22.476	0.462 (99.893)	16.753	0.250 (40.266)
PI – Medium (q = 20%)	11.655	0.268 (30.028)	12.071	0.408 (47.370)	13.528	0.581 (75.552)	12.279	0.393 (46.335)
PI – High (q = 50%)	8.741	0.512 (43.038)	9.157	0.697 (61.376)	9.990	0.748 (71.806)	9.573	0.612 (56.357)
Panel D :Information asymmetry – Moral Hazard								
r = US$ -0.5m invested	23.725	1.120 (255.364)	---	---	---	---	---	---
r = US$ -0.25m invested	21.748	1.129 (235.936)	---	---	---	---	---	---
r = US$ 0.25m invested	19.147	1.135 (208.837)	---	---	---	---	---	---
r = US$ 0.5m invested	18.106	1.139 (198.237)	---	---	---	---	---	---
Panel E: Effect of Primary Insurer's Portfolio Size								
Medium (100 contracts)	35.796	0.186 (64.106)	36.108	0.230 (79.804)	35.796	0.306 (105.236)	36.108	0.208 (72.031)
Large (500 contracts)	93.236	0.408 (365.213)	93.236	0.414 (371.240)	93.236	0.184 (164.788)	93.236	0.325 (291.122)

Note: PI = primary insurer, m = million.