Does insurance regulation adequately reflect cyber risk?

An Analysis of Solvency II and the Swiss Solvency Test

This Version: February 2016
Does insurance regulation adequately reflect cyber risk?

An Analysis of Solvency II and the Swiss Solvency Test

Abstract: Cyber risk is a relatively new type of risk, which might be huge in magnitude both in underwriting and in the operational risk of insurance companies. We first describe the dynamic nature of cyber risk, then analyze the current regulatory treatment and finally assess the adequacy of the current treatment. Our results indicate that the current regulatory treatment does not adequately reflect the potential risk exposure from this new type of risk. We make recommendations for an adequate assessment of cyber risk both in underwriting and operational risk.
1 Introduction

New insurance regulations and research have mainly been concentrated on operational risk in general and classical underwriting activities. In contrast, cyber risk as a new emerging risk has neither been the focus of regulators nor researchers. A major challenge for the development of adequate risk management models has been a limited understanding of the cyber risk’s properties mainly due to lacking data. Most recently, however, some new research initiatives contributed to a better understanding of cyber risk. For example Haas & Hofmann (2013), Biener, Eling & Wirfs (2015) and Eling & Wirfs (2015) extensively analyzed the properties of cyber risk.

This paper aims to shed light on this new topic by analyzing whether cyber risk is adequately accounted for by the insurance regulators. Cyber risk can affect an insurance company in two different ways. On the one hand, since an insurance relies critically on the processing of sensitive information, its IT infrastructure is highly vulnerable to cyber risk exposure. This exposure is treated by regulatory frameworks as part of the operational risk category (operational cyber risk). On the other hand, writing cyber risk policies seems to be an attractive business opportunity for insurance companies in an otherwise quite saturated market (underwriting cyber risk). These two types of cyber risk exposures not only require different risk management techniques but they are also treated differently by the regulatory frameworks.

We contribute to this emerging new research stream by analyzing how current regulatory regimes treat cyber risk and comparing it with the results of recent empirical studies on cyber risk. In order to compare the empirical properties with the regulatory frameworks, we transform incident data from Biener et al. (2015) to company specific data. The ultimate goal of the paper is to analyze whether regulations have taken cyber risk adequately into account and, if not, how it could be done in further regulation initiatives. The two regulatory models we consider are the two most recent and most often discussed in academic literature: Solvency II (SII) and the Swiss Solvency Test (SST; see Eling, Schmeiser, & Schmit, 2007; Holzmüller, 2009).

The remainder of the paper is organized as follows. In Chapter 2 we give an overview of the research done on cyber risk and its properties. Those findings are then compared in Chapter 3 & 4 with the regulatory treatment under SII and SST. Finally, we conclude by summarizing and discussing the results in Chapter 5 and also provide recommendations for an improved cyber risk assessment in regulatory models.
2 Cyber risk: Definition and Properties

In the following we define cyber risk as “operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems” (Eling & Wirfs, 2015). From the perspective of an insurance company, cyber risk can be subdivided according to the origin into operational and underwriting cyber risk. The two cyber risk sources differ fundamentally in their properties as well as in their adequate risk management techniques. At first, since an insurance and the average buyer of a cyber risk policy might not rely equally on processing sensitive information, they experience different exposures to cyber risk. As a consequence underwriting and operational cyber risk do not have the same properties (compare Eling & Wirfs, 2015). Moreover, most regulatory frameworks allow to account for risk mitigating measures and thereby a reduction in capital requirement.

The two categories differ with respect to the responsibility within the company and the available risk management techniques:

<table>
<thead>
<tr>
<th>Risk management techniques</th>
<th>Operational cyber risk</th>
<th>Underwriting cyber risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management techniques</td>
<td>Technical IT security measures</td>
<td>Reinsurance</td>
</tr>
<tr>
<td></td>
<td>Improving processes</td>
<td>Risk transfer (insurance linked securities)</td>
</tr>
<tr>
<td></td>
<td>Educating employees</td>
<td>Insurance pooling</td>
</tr>
<tr>
<td></td>
<td>Buying cyber risk policies</td>
<td>Screening &amp; controlling of policy holders</td>
</tr>
<tr>
<td>Responsibility</td>
<td>IT department</td>
<td>Actuary</td>
</tr>
</tbody>
</table>

The management of operational cyber risk is mainly directed to improve processes and employees’ education. It is strongly related to how well an insurance is managed and therefore operational cyber risk is more idiosyncratic or company specific in nature. Consequently, modelling and calibration of operational risk should be company specific and using data from a global operational risk database to calibrate RM models might not be adequate. In contrast, since underwriting cyber risk consists of a more or less diversified pool of single exposures, it might resemble the stochastic characteristics derived from global data.

---

1 The authors provide a detailed discussion of the term cyber risk.

2 When an insurance chooses to transfer its cyber risk, the exposure is partially replaced by the counterparty default risk and capital requirements might or might not decline.
Generally, as cyber risk is an emerging topic, the policy pools are usually quite small and consequently the diversification effect is limited. From a technical point of few this has the consequence that the law of large numbers is not applicable as an approximation and instead numerical techniques have to be applied to model the insurance pool behavior.

Despite the distinct nature, in an extreme event, such as a breakdown of global communication, operational and underwriting cyber risks on the insurance balance sheet will get correlated. Therefore, an adequate risk model would account for high tail correlation between the single losses. However, interconnectedness of IT systems and the use of the same technologies (software) is also causing correlation in normal circumstances and is going to increase as IT technology penetrates more and more every aspect of life (internet of things, emerging countries get more integrated in the global communication systems) (Baer & Parkinson, 2007; Haas & Hofmann, 2013).

In order to understand cyber risk even better, the frequency and severity of events should be unbundled, since they have their own fundamental structure. Changes over time might contain additional information and correlation between losses might be originated in correlation in the frequency instead of severity. The main risk driver seem to differ when considering frequency and severity:

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Frequency</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Technology</td>
<td>Processes in place to mitigate losses</td>
</tr>
<tr>
<td></td>
<td>Criminal activity (criminal law; poverty)</td>
<td>Crisis management (PR)</td>
</tr>
<tr>
<td></td>
<td>Interconnectedness (e.g. access of a country to the internet)</td>
<td>The companies dependency on the IT technology</td>
</tr>
<tr>
<td></td>
<td>Occurrence of disasters</td>
<td>Sensitivity of processed information</td>
</tr>
<tr>
<td>Mitigation</td>
<td></td>
<td>Cyber risk insurance</td>
</tr>
</tbody>
</table>

It seems that while the loss severity might be mainly determined by company specific factors, the frequency depends more on the global cybercriminal activity. Therefore, it might be the

3 Estimating the loss distribution (Precondition: iid) from an incidence database (e.g. SAS OpRisk) without unbundling of frequency and severity would give the marginal distribution given that an incidence has happened. As this distribution neglects all the periods and companies where there has been no incidences reported, directly applied to calculate risk measures (e.g. VaR, TVaR) would lead to estimates with positive bias since the distribution is shifted to the right or shows heavier tails.
case that severity needs to be estimated based on company specific data. Because it is easier to
establish that a loss has simply occurred then the exact amount of this loss, the frequency dis-
tribution can be estimated more precisely than severity.

Eling & Wirfs (2015) investigated the statistical properties of cyber risk based on the SAS
OpRisk database. Cyber risk losses show stronger skewness and kurtosis compared to P&L but
weaker than operational risk. The frequently used log normal distribution in risk management
(see Chapter SII), does not seem to be the best choice when modelling cyber risk. As the prob-
ability mass in the tail is to low, they show it tends to underestimate the VaR slightly and TVaR
quite strongly (especially problematic for SST). They find the best fit for their peaks over
threshold (POT) model, where the body consists of a log normal and the tail of a generalized
pareto (GP) distribution.4 Their GPD shows a shape parameter around 1 depending on the re-
gion, industry and time.5 This small parameter not only questions the applicability of risk
measures TVaR but can under certain circumstances (especially an underdeveloped market)
reduce the optimal risk pool size.6 The later would ask for higher capital requirement for cyber
risk.

---

4 While the author applies skewed normal and student distribution on P&L losses and finds that it fits reasonably
well, they might also suit for cyber risks (Eling, 2012).
5 Operational risks show pareto indices of less than one (Neslehová, Embrechts, & Chavez-Demoulin, 2006).
6 It can be shown that heavy tails and high correlation of risk can lead to small risk pools or no diversification as
an optimum (Ibragimov & Walden, 2007; Ibragimov, Jaffee, & Walden, 2009).
3 Data & Methodology

In order to compare later on the empirical properties with the regulatory frameworks, the SAS OpRisk data reported per cyber risk incidence needs to be transformed to company specific data. This transformation can be done by the widely applied loss distribution approach (LDA) where the company specific risk exposure is described by the frequency, \( N \), compounded severities, \( Z_i: X = \sum_{i=0}^N Z_i \) (Neslehová, Embrechts, & Chavez-Demoulin, 2006). Both random variables’ parameters and distributions can be estimated by the data at hand (compare Hess, 2011). Assuming that \( Z_i \) are iid and independent of \( N \), the parameters for the company specific risk exposure can be derived by applying the Wald’s and Blackwell-Girshick’s equations:

\[
E(X) = E(N) \cdot E(Z) \\
Var(X) = Var(N) \cdot E(Z)^2 + E(N) \cdot Var(Z)
\]

In order to derive the empirical distribution for \( X \) and more specifically its risk measures, Var and TVaR, it is assumed that the compounding is done by a Poisson process. Since there is no closed form solution, the compounding is done numerically with the Panjer recursion. 7 Table 1 summarizes the statistics and figure 1 shows the empirical distribution.

Table 1: Cyber risk parameters

<table>
<thead>
<tr>
<th></th>
<th>( n )</th>
<th>( \bar{z} )</th>
<th>( s )</th>
<th>( Var_{0.995} )</th>
<th>( TVaR_{0.99} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity (per incident)</td>
<td>( Z^s )</td>
<td>994</td>
<td>40.5</td>
<td>443.9</td>
<td>1'112</td>
</tr>
<tr>
<td>Frequency (per year)</td>
<td>( N^o )</td>
<td>0.15</td>
<td>0.39</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDA (per company)</td>
<td>( X_{op} )</td>
<td>6.1</td>
<td>172.7</td>
<td>158</td>
<td>530.5</td>
</tr>
<tr>
<td>Severity (truncated)</td>
<td>( Z_t )</td>
<td>994</td>
<td>8.4</td>
<td>14.4</td>
<td>50.0</td>
</tr>
<tr>
<td>LDA (truncated)</td>
<td>( X_t )</td>
<td>1.3</td>
<td>6.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portfolio (of 50)</td>
<td>( X_{uw} )</td>
<td>304</td>
<td>1221</td>
<td>13'349</td>
<td>10'978</td>
</tr>
<tr>
<td></td>
<td>( X_{uw,t} )</td>
<td>63.3</td>
<td>45.7</td>
<td>217.4</td>
<td>225.1</td>
</tr>
</tbody>
</table>

(Amounts in mUS$)

The first part of the table reports the statistics for \( X_{op} \) which is here taken as an estimate for the insurance company’s operational risk exposure. Clearly, for this assumption the data needs to be somewhat representative for the insurance industry. An insurance company is then expected to suffer on average a loss due to cyber risk of mUS$ 6 per year at a quite substantial uncertainty

---

7 For the Panjer recursion the function “aggregateDist{actuar}” in R has been used.
8 Compare Biener et al. (2015).
as the risk measures show. Put it differently, operational cyber risk shows extremely heavy tails. Moreover, $X_{op}$ could also represent an insurance’s underwriting risk in the extreme case where there is no diversification at all and cyber policies do not contain any coverage limits (no limits and deductibles). Again the estimation is only as good as the recorded SAS companies represent an insurance’s average cyber risk portfolio. However, it can be expected that an insurance company will usually set a coverage limit for its cyber policies that is here assumed to be mUS$ 50. With this limit the insurance would still provide full coverage for 92.5% of all occurred losses. The second part of table 1 reports the more realistic properties of a single underwriting risk $X_t = \sum_{i=0}^N \min(Z_i, 50)$. Note that this coverage limit significantly alters the tail behavior of the insurers’ exposure (see figure 1).

Since the regulatory requirements for underwriting risk are applicable for a portfolio of policies and assume implicitly some degree of diversification (depending on the LoB), it is necessary to think of the risk $X_t$ as being a component of a portfolio. We assumed that an average cyber risk portfolio contains 50 policies, $X_{uw,t} = \sum_{i=1}^{50} X_{lt}$, and that $X_{lt}$ are iid. The lower part of table 1 states the statistics for $X_{uw,t}$. Despite truncated data, the distribution still features a rather heavy tail and high (tail) value at risk.
In a later version of this paper, we are going to loosen the iid assumption and apply an estimate for the correlation between each risk’s frequency distribution.
4 Operational Cyber Risk

Generally, cyber risk is not treated as a separated risk category in regulatory risk management frameworks but instead needs to be considered as a part of the more generic operational risk category. The Solvency II (SII) framework defines operational risk as (similar to Basel II): “[...] it is the risk of loss arising from inadequate or failed internal processes, or from personnel and systems, or from external events. Operational risk should include legal risks, and exclude risks arising from strategic decisions, as well as reputation risks” (European commission, 2010, p. 102). Clearly, this definition comprises a substantial part of possible cyber risk treads. However, the exclusion of reputational risk\(^ {10} \) seems to be especially critical since leaking sensitive information could even be the main costs component for some companies.

SII requires that operational risk is assessed qualitatively (Pillar II&III) by specifying processes in order to identify, analyze and report operational risks, as well as quantitatively (Pillar I). The capital requirement \( (scr_{\text{op}}) \) for the overall operational risk is defined as (EIOPA, 2014):

\[
scr_{\text{op}} = \min\{0.3 \cdot bscr(p, r), bc(p, r)\}^{11}
\]

where \( bscr \) (Basic capital requirement) and \( bc \) (base charge)\(^ {12} \) are some functions that share the same volume measures, previous and current year premiums \( (p) \) as well as technical provisions \( (r) \) for life and non-life, as an input.

Clearly, this volume based approach is not very sensitive to the true risk exposure. However, when it might be the only way to go when there is not enough data history to calibrate more sophisticated models. For completeness it should be mentioned that, there is an ongoing discussion whether a risk more sensitive approach similar to advanced measurement approach (AMA) under the Basel framework should be implemented instead.

Analyzing the formula with respect to cyber risk and its properties shows that it captures the true value at risk only in a very crude way. Firstly, capital requirement relies on the volume measures that are only very loosely related to cyber risk exposure. Instead, to take cyber risk into account properly, capital requirement should be defined as some factor times the expected

---

\(^{10}\) EIOPA (2014, S. 11) justifies neglecting reputational risk by the lack of historical data on that risk category.

\(^{11}\) Strongly simplified formula; however it does not change fundamentally the interpretation below. Note that this approach is similar to Basel II (Basel Committee on Banking Supervision, 2005), where capital requirement is calculated as \( \beta \cdot Gross\ income \), where \( \beta \) might be chosen according to the LoB.

\(^{12}\) bscr and bc consist of several min / max operations on some factors times the volume measures.
**cyber risk losses.** Secondly, the constant factor structure does not allow to account specifically for the cyber risk, as could be measured by the volatility in cyber risk losses. Thirdly, only one capital charge is calculated for all potential source of operational risk and it is not accounted for the specifics of cyber risk. Obviously, such a measure does not adequately take into account specific factors that determine cyber risk exposure, such as the business model, target markets, size of the insurance and, more importantly, it might deteriorate the management’s incentives to take measures in order to reduce cyber risk exposure. Finally, this approach with a constant factors dose only approximate the value at risk even if a specific distribution is assumed. If it is assumed that premiums and technical provisions, as measure of the company size, is somehow related to the cyber risk exposure, considering the base charge \((bc)\) would be sufficient, since the basic capital requirement \((bscr)\) is mainly determined by underwriting and market risk and therefore is a strongly biased measure for cyber risk.

Since the factors used to calculate the required capital are given only for the overall operational risk, it is difficult to determine whether they are appropriate from a cyber risk perspective. However, it is possible to make a qualitative comparison. The value at risk for \(Y\) from table 1 can be converted to a relative measure, \(s_{CP} = \frac{SCR}{E(Y)}:\)

<table>
<thead>
<tr>
<th>(Y)</th>
<th>(VaR_{0.995})</th>
<th>SCR</th>
<th>(s_{CP})</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>158</td>
<td>152.1</td>
<td>24.9</td>
</tr>
</tbody>
</table>

\(s_{CP}\) can be interpreted as the empirical analogue to the overall but unknown risk factor, \(\delta_{OP}\), used here. However, as SII predefines the more granular risk factors, they need to be aggregated first in order to be comparable with \(s_{CP}\). Instead, here a simpler qualitative argumentation should do. The factors SII uses start from 0.0045 for reserves risk, 0.03 for premium risk, and end with 0.3 for BSCR. BSCR itself is calculated as some factors \(\delta_{bscr}\) times a volume measures. As the discussion in the next chapter shows, it is likely that that \(0.3*\delta_{bscr}<<1\). The linear combination of all these granular risk factors is an upper bound for \(\delta_{OP}\). Therefore, \(\delta_{OP}\) is always equal or smaller than the biggest granular factor. Since all factors lie way below the empirical analogue, \(s_{CP}\), it must hold that \(\delta_{OP}<<s_{CP}\). Therefore, it can be safely concluded that SII massively underestimates the treads from exposure to cyber risk and this is misjudgment is even more severe, if we recall that the factors used here should be sufficient for the overall operational risk not only cyber risk.

The SST framework does not consider operational risk quantitatively but qualitatively under
SST (SQA; Swiss Qualitative Assessment). However, according to Art. 98 of the Swiss supervisory act (AVO), it is possible that the supervisory body requests in certain circumstances an additional margin on top of the required capital.
5 Underwriting Cyber Risk

The options, how to treat cyber risk originated by policies an insurance has written, can be categorized similarly as in operational cyber risk. While SII standard approach relies more on a volume based approach, SST employs as a risk based model. However, each approach allows more or less for company specific adjustments. In the discussion of both approaches it is assumed that the insurance retains all liabilities since reinsurance contracts are not of special interest for cyber risk.

5.1 Underwriting Cyber Risk in SII

Generally, the total capital requirement is the aggregation of the required capital for more granular risk categories, such as (sub-) modules, segments and LoBs. If $X$ is a random vector of dimension $m$ for all risk categories, each contribution to the required capital is defined as (compare article 115 in European Commission, 2014):

$$
scr(X) = 3 \cdot \delta^e(X) \cdot v(X) \quad (2)
$$

Hence, the loss volatility, $\delta (X)$, is equal to the coefficient of variation, $\delta^e(X)$, times the volume measure, $v(X)$. A major problem with this approach is that it does not accounted for the statistical properties of cyber risk. Since $X$ already represents the total loss on a portfolio, diversification properties nor the size of the portfolio play a role. Besides that, volatility is generally not a very useful risk measure when the distribution is asymmetric as it is usually the case in non-life-insurance and it is not very sensitive to the tail distribution. Finally, for some distribution with extreme heavy tails the volatility does not exist at all. (compare McNeil, Frey, & Embrechts, 2005)

In order to attain the aggregated capital, the granular risks are added together, $S = 1^T \cdot X$. SII requires using the formula (compare article 87, 114 in European Commission, 2014):

$$
scr(S) = \sqrt{scr(X)^T \Sigma scr(X)} \quad (3)
$$

---

13 Until QIS5 the required capital was defined as $scr(X) = VaR_{0.995}(X) - v(X)$, assuming a log normal distribution, (European commission, 2010) and the capital requirement can be interpreted as the unexpected risk exceeding the expected loss. The current definition (2) does not make explicit distribution assumption but approximates the old one.
where $\Sigma$ is the correlation matrix $n \times n$. In order to facilitate the aggregation, the granular volume measures is defined here as a fraction of the aggregated value:

\[ v(X) = a \cdot v(S) \]

where $I^T \cdot a = 1$. Combining the equations (2), (3) and (4) would yield:

\[ scr(S) = 3 \cdot v(S) \cdot \sqrt{(a \cdot \delta^S(X))^T \cdot \Sigma \cdot (a \cdot \delta^S(X)a)} = 3 \cdot \delta^S(S) \cdot v(S) \]  

(5)

Note that as equation (5) resembles the variance-covariance-approach, the risk measure is coherent and, more specifically, sub-additively, $scr(S) \leq I^T \cdot scr(X)$. For the empirical analysis below, it is required to relate the volume measure to the expected loss. Therefore it is assumed that the volume measure equals the expected loss divided by the loss ratio:

\[ v(S) = b^{-1} \cdot E(S) \]  

(6)

Put it differently, it says that the sum of premiums and reserves reduced by the calculative cost and profit margin approximates the expected loss. Applying (6) to (5) would yield:

\[ scr(S) = 3 \cdot \delta^S(S) \cdot b^{-1} \cdot E(S) \]  

(7)

While $b$ and $E(S)$ are calibrated for cyber risk empirically, $\delta^S(S)$ needs to be derived from the SII correlation and risk factor tables. From a bottom up perspective, the relative volatility per segment $\delta^S_{pr}$ is composed of premium, $\delta^S_p$, and reserve, $\delta^S_r$, risk according to (5):

\[ \delta^S_{pr} = \left( \frac{\delta^S_p}{\delta^S_r} \right); \Sigma_{pr} = \begin{pmatrix} 1 & p \\ p & 1 \end{pmatrix}, p = 0.5 \]

To derive the volatilities it is possible to rely on predefined or company-specific estimates. This in principle enables to account for cyber risk specifics. It is additionally assumed that half of the expected losses are reserved:

\[ a_{pr} = \left( \frac{a_r}{1-a_r} \right); a_r = 0.5 \]

---

14 While this definition is in most circumstances equivalently to the requirements of SII, for the aggregation of premium & reserves, it neglects the geographic diversification: $v_{PR} = (v_P + v_R) \cdot (0.75 + 0.25 \cdot c)$

15 The same would not be true if the equation is interpreted as an aggregation of VaRs (compare foot note 15). For a detailed discussion of risk measures’ properties refer to McNeil, Frey & Embrechts (2005).

16 The exact definitions of the volume measures for premium & reserves would be (article 116 in European Commission, 2014):

\[ v_{PR} = v_P + v_R, v_p = \max(E(P_{CV}), P_{PV}) + c, v_R = E(R) + c \]
Then the volatilities over all segments \( s \) are again aggregated, \( \delta_s^s \), according to (5). However, as the tables do not contain volatilities specific to cyber risk, the obligations have to be allocated according to their true nature of risk, even if it is needed to be unbundled into several LoBs (article 55 abs. 6). Relevant segments for cyber risk are general liability, legal expenses and miscellaneous financial loss and their correlation matrix is \( \Sigma_s \). Additionally, it is assumed that:

\[
a_s^i = a_s^j \forall i, j
\]

Conducting the aggregations for all segments with the numerical values specified would yield:

<table>
<thead>
<tr>
<th>LoBs</th>
<th>( \langle \delta_P \rangle )</th>
<th>( \langle \delta_R \rangle )</th>
<th>( \langle \delta_{PR} \rangle )</th>
<th>( \langle \alpha_s \rangle )</th>
</tr>
</thead>
<tbody>
<tr>
<td>General liability</td>
<td>0.14</td>
<td>0.11</td>
<td>0.11</td>
<td>1/3</td>
</tr>
<tr>
<td>Legal expenses</td>
<td>0.07</td>
<td>0.12</td>
<td>0.08</td>
<td>1/3</td>
</tr>
<tr>
<td>Miscellaneous financial loss</td>
<td>0.13</td>
<td>0.20</td>
<td>0.14</td>
<td>1/3</td>
</tr>
</tbody>
</table>

Finally, non-life risk, \( \delta_{nl}^s \), is the aggregation of the two relevant modules, catastrophic (cat) as well as the segment risk according to (5) (Article 114): \( ^{18} \)

\[
\delta_{nl}^s = \left( \begin{array}{c}
\delta_s^{cat} \\
\delta_s^s
\end{array} \right); \quad \Sigma_{nl} = \begin{pmatrix}
1 & p \\
\frac{p}{1}
\end{pmatrix}, \quad p = 0.25
\]

Consequently, the cyber risk is divided fundamentally into normal and extreme events, mimicking the EV approach discussed above. Similarly \( scr_{cat} \) is composed of several sources of catastrophic risks that are aggregated according to formula (5). Again while there is no specific category for cyber risk, man-made cat (MC), especially the category liability, and other cat (OC), seem to be relevant. The aggregation is done with the trivial correlation matrix \( I \):

<table>
<thead>
<tr>
<th>NL cat risk</th>
<th>( \delta_{(\cdot)}^c )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liability</td>
<td>1.0</td>
</tr>
<tr>
<td>Other</td>
<td>0.4</td>
</tr>
<tr>
<td>cat</td>
<td>1.1</td>
</tr>
</tbody>
</table>

Now the derived SII statistics can be compared to the empirical findings:

---

\( ^{17} \) Refer to appendix for the correlations used.

\( ^{18} \) Laps risk has been neglected since the data available for testing do not contain any information about this category.
It seems that the SII approach takes underwriting cyber risk adequately into account. However, the result is highly sensitive to the assumptions in chapter 2 concerning the diversification and coverage limits.

The cumulative empirical distribution has been fitted to the SII distribution and the Kolmogorov-Smirnov test statistic evaluated.

<table>
<thead>
<tr>
<th></th>
<th>$\bar{x}$</th>
<th>$\nu_{(.)}$</th>
<th>$\delta_{(.)}^z$</th>
<th>$\delta_{(.)}$</th>
<th>$scr_{(.)}$</th>
<th>$VaR_{(.)}^{0.995}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s$</td>
<td></td>
<td></td>
<td>0.11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cat</td>
<td></td>
<td></td>
<td>1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$nl$</td>
<td></td>
<td>79.1$^{19}$</td>
<td>1.1</td>
<td>87.0</td>
<td>261</td>
<td>340.1</td>
</tr>
<tr>
<td>Empirical $^{20}$</td>
<td>63.3</td>
<td></td>
<td>0.72</td>
<td>45.8</td>
<td></td>
<td>271.4</td>
</tr>
</tbody>
</table>

(amounts in mUS$)

The cumulative empirical distribution has been fitted to the SII distribution and the Kolmogorov-Smirnov test statistic evaluated.

<table>
<thead>
<tr>
<th>Test</th>
<th>$d_{max}$</th>
<th>$d_{0.05}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>KS</td>
<td>0.17</td>
<td>0.04</td>
</tr>
</tbody>
</table>

$^{19}$ Assumption: $b = 0.8$

$^{20}$ Refer to p.6
5.2 Underwriting Cyber Risk in SST

In SST the capital requirement, SCR, is derived by calculating the expected shortfall, ES, of the loss, \(X\), distribution and subtracting the expected values (Bundesamt für Privatversicherungen, 2006). In the following, market, credit risk and even discounting is completely neglected; only the ceteris paribus effect of underwriting risk, \(u\), is of interest:

\[
SCR(X_u) = ES_{0.99}(X_u) - E(X_u)
\]

Generally, the expected tail value shows nicer properties than for example the value at risk as it is a coherent risk measure and therefore sub-additive (McNeil, Frey, & Embrechts, 2005). Moreover, it is more sensitive to the tail behavior of a distribution than for example the volatility. Quite similar as for SII, the total loss is subdivide into several LoBs and (sub-) modules and for the aggregation the same formulas are applicable. In terms of random variables the total loss is defined (simplification) as:

\[
X_u = (X^N_p + X_r) + X^{EX}_p
\]

where the reserve risk, \(X_r\), and the normal losses, \(X^N_p\), together are assumed to be log normally distributed and extreme events, \(X^{EX}_p\), are described by a Poisson compounded Pareto distribution (CPois). The later summand facilitates to take cyber risk specifics, such as heavy tails, appropriate into account. Especially, the shape parameter of the PD can be chosen accordingly (compare chapter 2). However, a drawback of the PC is that it requires risks to be independent. This is generally not true for cyber risk, and certainly not for extreme events.

For the analysis the data sample is divided in 686 normal losses (< 5 Mio.) and 308 extreme losses. The aggregation starts by aggregating random and parameter risk for each LoB, premium risk and reserve risk. As in SII there is no specific category for cyber risk but the need to be allocated according to their risk nature.

<table>
<thead>
<tr>
<th>LoB</th>
<th>(a)</th>
<th>(\delta^T_{(pa)})</th>
<th>(\delta^T_{(er)})</th>
<th>(\lambda)</th>
<th>(\delta^T_{(pr)})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liability</td>
<td>1/4</td>
<td>3.5%</td>
<td>11%</td>
<td>5.2</td>
<td>44%</td>
</tr>
<tr>
<td>Financial losses</td>
<td>1/4</td>
<td>5%</td>
<td>5%</td>
<td>5.2</td>
<td>44%</td>
</tr>
<tr>
<td>Legal costs</td>
<td>1/4</td>
<td>5%</td>
<td>5%</td>
<td>5.2</td>
<td>44%</td>
</tr>
<tr>
<td>others</td>
<td>1/4</td>
<td>4.5%</td>
<td>5%</td>
<td>5.2</td>
<td>44%</td>
</tr>
</tbody>
</table>
\[
\begin{array}{cccc}
\delta^{\text{pr}} & E(X^{\text{pr}}) & \delta^{(\text{pr})} & ES_{0.99}(X^{\text{pr}}) \\
44\% & 1.4 & 0.6 & \\
\end{array}
\]

(amounts in mUS$)

Therefore, SST assumes that the normal losses are: \(X^{N}_u \sim LN(1.4, 0.6)\). Finally, the extreme events have to be considered as well. Again it is assumed that those losses can be allocated to the same LoBs and the given pareto parameters are:

<table>
<thead>
<tr>
<th>LoB</th>
<th>(\alpha_{(\cdot)})</th>
<th>(\lambda_{(\cdot)})</th>
<th>(\alpha_{(\cdot)})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liability</td>
<td>1/4</td>
<td>2.3</td>
<td>2</td>
</tr>
<tr>
<td>Financial losses</td>
<td>1/4</td>
<td>2.3</td>
<td>0.75</td>
</tr>
<tr>
<td>Legal costs</td>
<td>1/4</td>
<td>2.3</td>
<td>1.5</td>
</tr>
<tr>
<td>others</td>
<td>1/4</td>
<td>2.3</td>
<td>1.5</td>
</tr>
</tbody>
</table>

SST assumes extreme events to be independent and proposes a Panjer recursion in order to aggregate them. 24 Finally, the excess and normal losses are again assumed to be independent and are convoluted together. 25 The aggregated loss probability function is plotted in figure 1 (dotted line). As expected, the excess losses increase the heaviness of the right tail and shifts the distribution to the right. The risk measure as suggested by SST and the empirical counterparts are:

<table>
<thead>
<tr>
<th>(\delta^{(u)})</th>
<th>(E(X^{(u)}))</th>
<th>(\delta^{(u)})</th>
<th>(ES_{0.99}(X^{(u)}))</th>
<th>(SCR(X^{(u)}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>SST</td>
<td>63.3</td>
<td>63.3</td>
<td>45.8</td>
<td>225.1</td>
</tr>
<tr>
<td>Empirical\textsuperscript{26}</td>
<td>63.3</td>
<td>45.8</td>
<td>225.1</td>
<td>161.8</td>
</tr>
</tbody>
</table>

(amounts in mUS$)

Since the loss data from SAS is incident based, again a Panjer recursion is used to poisson compound the empirical loss severities to derive the total loss on a cyber policy pool. In figure 1 the theoretical SST model is compared with the empirical distribution (black line). Note that as the data contains a few very high losses (maximum value is US$ 13 bill) not the whole distribution is plotted.

---

24 For the Panjer recursion the function “aggregateDist{actuar}” in R has been used.

25 For the convolution the function “convolve{stats}” has been used.

26 Refer to p.7
As can be seen, the SST assumption strongly underestimates the occurrence of extremely high losses and the expected shortfall lower than suggested by the data. Also the Kolmogorov-Smirnov-test confirms that it can be safely rejected that the SST distribution has generated this data (d=0.65). Moreover, the graph suggest that the appropriate pareto distribution would have a shape of <1 and therefore the mean cannot be calculated. While this would suggest that the capital requirement for cyber risk under the standard approach does not ensure the ruin probability aimed for, it is important to remark that most parameter used above could potentially be adapted to cyber risk specifics. Especially the location and dispersion of the distribution can be calibrated differently.
6 Discussion and Conclusion

The analysis in this paper shows that SII and SST only account for cyber risk in a very crude way since neither of them uses specific cyber risk categories and factors. While SST only requires that operational cyber risk is considered qualitatively, SII employs a simple factor approach. However, empirical testing shows that SII might massively underestimate the trends from operational cyber risk. With respect to underwriting cyber risk we showed that the requirements under SII and SST are only sufficient if we assume a well-diversified pool of cyber risk policies (more than 50 and no correlation) and a coverage limit at a rather low level (mUS$ 50). However, those assumptions might not be fulfilled in many cases.

Consequently, the current regulations have some shortcomings with respect to cyber risk. The risk insensitivity and the “one fits it all” approach might disturb risk mitigating behavior and does not reward sound risk management. However, in certain cases, especially for operational cyber risk, the capital requirement should be increased in order to maintain the soundness of the insurance industry. This will become even more important as industry gets more and more penetrated by new technologies. Moreover, governmental or private initiatives directed at enhancing the availability and quality of data on cyber risk would be highly appreciated.
References


Appendix

<table>
<thead>
<tr>
<th></th>
<th>5</th>
<th>7</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.5</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0.5</td>
<td>0.5</td>
<td>1</td>
</tr>
</tbody>
</table>