Modelling and Management of Cyber Risk

Abstract

Nowadays, cyber risks are an important point on the business agenda in every company, but they are difficult to analyze due to the wide absence of reliable data and profound analyses. To improve this situation, we identify cyber losses from an operational risk database and analyze these with methods from the field of actuarial science. Specifically, we apply models from operational risk in order to yield consistent risk estimates, depending on country, industry, size, and other variables. We also test whether cyber risks are structurally identical to other operational risks or exhibit distinct characteristics. Our results show that human behavior is the main source of cyber risk and that cyber risks are very different compared to other operational risk. The results of the paper are useful for practitioners, policymakers and regulators in order to provide a better understanding of this new and important type of risk.

Keywords: Cyber risk, risk management, insurance

1 Introduction

Although cyber risk has become a crucial topic for the whole economy and society, and is reported in the media every day,[1] it has been subject of very limited academic research. This is most likely due to the wide absence of reliable data. In this paper we go one step forward and provide a thorough empirical analysis of cyber risks. For this purpose we extract cyber risk data from an operational risk dataset and analyze it with actuarial methods. We use models from operational risk on a dataset of 994 cyber risk incidents that occurred in the time period from 1971 to 2014.

The existing literature on cyber risk is mostly limited to papers from the field of technology. Within risk and insurance, our paper is closest to Biener, Eling, and Wirfs (2015)[2] who analyze the insurability of cyber risk and illustrate their statistical properties using descriptive

[1] Cyber attacks were denoted by the G20 group as a threat to the global economy (see Ackermann, 2013); the World Economic Forum (2014) estimates the probability of a critical information infrastructure breakdown with 10 percent and the financial consequences after a few days to about US$ 250 billion.

[2] The existing articles on cyber risk and cyber insurance emphasize its complexity (e.g., Hofmann and Ramaj, 2011; Öğüt, Raghunathan, and Menon, 2011) and adverse selection and moral hazard issues (e.g., Gordon, Loeb, and Sohail, 2003).

statistics. We build upon and extend their data and analyze it with a longer coverage period and a more thorough empirical analysis that goes beyond descriptive statistics.

The aim of the paper is to test whether models which prove to be useful for operational risk can also be applied to an analysis of cyber risk or whether other tools are needed. We are interested in the question whether cyber risks are structurally identical to other operational risks or exhibit distinct characteristics. Our results show that human behavior is the main source of cyber risk and that cyber risks are very different compared to other operational risk from an actuarial point of view.

These results are important for (the CFO and CRO of) every company in order to get a better understanding of cyber risks and their consequences. In the financial services sector, they are especially important since regulators require banks and insurance companies to hold risk capital for operational losses which might result from cyber risks.[3] Moreover, our results are useful for insurance companies which are developing cyber insurance policies and do not have enough data and experience with cyber risks. We illustrate the usefulness of our results for policymakers, regulators and practitioners in two applications on risk management and pricing. For the academic audience we present effective and contemporary modeling and solution approaches for the novel application area of cyber risk.

The remainder of this paper is structured as follows. In Section 2 we define the term "cyber risk" and introduce our data and methodology. Then, in Section 3 the empirical analysis is presented. We conclude in Section 4.

2 Material and Methods

Cyber risk is a dynamic loss category that has not been thoroughly discussed in academic literature yet (Biener, Eling, and Wirfs, 2015). An efficient data collection for cyber risks is just emerging. Typically, information on cyber risk is not publicly available since affected companies tend to not report it.[4] Another problem that hampers the collection of cyber risk data is the absence of a clear-cut definition.

The definition we employ here is based on how banking supervisors categorize operational risk and goes back to Cebula and Young (2010), who 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". Linking cyber risk to

[3] Also for firms outside the financial services sector, the results are important not only for internal risk management, but also in light of recent regulatory reforms. See, e.g. the regulatory approaches for new data protection (e.g. European Commission, 2012).

[4] Both in the EU and the US there is a discussion on mandatory reporting requirements. If these become reality, then more data and information would be available.

operational risk has several advantages: Firstly, it allows distinguishing cyber risk from other established risk categories.[5] Secondly, in structuring cyber risk we can use the established subcategories from operational risk (see Table 1).[6] And thirdly, linking cyber risks to operational risks allows to clearly identifying relevant data.

Table 1 Categories of cyber risk (see Cebula and Young, 2010)

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

The latter argument is exactly the empirical strategy of this paper: Having defined cyber risk as a subgroup of operational risk, we use the world's largest collection of publicly reported operational losses – the SAS OpRisk Global data – and extract cyber risk events using the search and identification strategy described in Appendix A. The database consists of 30'173 observations between March 1971 and March 2014. All losses are given in USD and adjusted for inflation to make them comparable.[7]

[5] In banking supervision (e.g. BIS, 2006) market, credit, liquidity, legal and operational risks are separated. Insurance supervisors (e.g., CEIOPS, 2009) typically consider market, insurance, credit and operational risks.

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

[7] The dataset attempts to provide an estimate of the complete costs of operational risk events (both direct as well as indirect effects); however, reputational loss due to an operational risk event is not covered since this sort of loss is typically excluded from operational risk. In this first draft of the paper, we only analyze data

To analyze the statistical properties of cyber risk and to identify the model that describes the data best we use the standard toolbox from actuarial science. After presenting descriptive statistics, we fit the cyber loss data using extreme value theory. In particular, we implement the loss distribution approach (e.g., peak-over-threshold method), which is standard in modelling operational risk. We also present an extended version of this approach where the loss data depends on covariates (following Chavez-Demoulin, Embrechts, and Hofert, 2013) and fit the loss data to various other distributions which have proven to be useful for actuarial loss analysis (e.g., the g-and-h family of distributions, the Generalized Beta distribution of the second kind, and skewed distributions; see, e.g., Eling, 2012). To identify the model that works best, we apply standard goodness of fit tests and also more tailored tests for the advanced measurement approaches.

After having identified the best modelling approach, we present two applications: Firstly, a numerical study to estimate the risk measures value at risk and tail value at risk. These measures are especially relevant for regulatory purposes in banking and insurance (Basel II, Solvency II) and show how much capital a company needs to cover the losses with a given confidence level (see Eling and Tibiletti, 2010, for definitions of the risk measures). Secondly, we use the numerical results for pricing of a typical cyber insurance policy. Here we use results from a recent market survey (Biener et al., 2015) and standard pricing methods from actuarial science (see, e.g., Bowers et al., 1997). A detailed description of the methodology is presented in Appendix B.

3 Results

3.1 Descriptive Statistics

Table 2 provides a summary of the cyber risk sample and compares its characteristics with non-cyber risk. All descriptive statistics for cyber risk are significantly smaller than those for non-cyber risk, i.e., the other operational risks.[8] The maximal loss in our sample is US$ 13 billion compared to US$ 89 billion for non-cyber risk.[9] The loss amounts for cyber risk are

until 2009 (as done in Biener, Eling, and Wirfs, 2015), since we are in the process of finishing the data identification and analysis.

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

[9] The largest cyber risk case occurred at the Bank of China in February 2005 when US$ 13,313.51 million were laundered through one of its branches, which was possible because the bank's internal money laundering controls were manipulated by employees. The largest non-cyber risk case involves the U.S. tobacco company Philip Morris, which, in November 2001, was ordered to pay US$ 89,143.99 million in punitive damages to sick smokers.

thus much smaller than for other operational risks.[10] Sorting into cyber risk subcategories (Panel B of Table 2) shows that most of the cyber risk incidents occur in the "actions of people" subcategory.[11] It thus seems that human behavior is the main source of cyber risk, while the other categories, such as external disasters, are very rare. The average losses across the different subcategories are relatively similar.

Table 2 Losses per risk type (in million US$)

Category	N	Mean	Std. dev.	Min.	Quantiles			VaR	TVaR	Max.
					25%	50%	75%	(95%)	(95%)	
Panel A: Cyber versus non-cyber risk										
Cyber risk	994	40.53	443.88	0.10	0.56	1.87	7.72	89.56	676.88	13,313
Non-cyber risk	21,081	99.65	1,160.17	0.10	1.88	6.20	25.37	248.97	1595.27	89,143
Panel B: Cyber risk subcategories										
Actions of people	903	40.69	463.25	0.10	0.55	1.83	6.87	84.36	679.04	13,313
Systems and technical failure	37	29.07	77.33	0.10	1.10	5.03	11.65	168.95	329.04	370
Failed internal processes	41	47.72	205.92	0.14	0.42	2.04	9.05	158.65	743.40	1,311
External events	13	39.40	115.73	0.28	0.56	1.03	13.77	192.88	422.71	422

Table 3 further separates the cyber and non-cyber risk loss data into several subcategories. The geographic separation (Panel A) shows that Northern American companies experience more than twice as many (51.9%) cyber risk incidents than do European firms (23.2%) and even more than twice as many as firms located on other continents. For loss severity, we find that Northern America has some of the lowest mean cyber risk and non-cyber risk losses, whereas Europe and Asia have much higher average losses. This situation may be due to North American firms being more capable of and willing to invest in risk mitigating measures for extreme losses, which results from a longer tradition of recognizing and managing cyber risks as compared to Europe or Asia.

Panel B of Table 3 provides a separation into financial and nonfinancial services industries. 78.6% of all cyber risk incidents occur in the financial services industry. This is not surprising since financial services firms, such as banks and insurance firms, store a significant amount of critical personal data.[12] However, the average loss resulting from cyber risk for firms in nonfinancial services industries is about twice as high as for financial services firms. This finding might be explained by financial services firms having a higher awareness regarding critical data and better protection against cyber risk. For non-cyber risks, firms in the

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

[11] Hacking attacks, physical information thefts, human failures, and all incidents where employees manipulate data (un-/intentionally) are included here.

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

nonfinancial services industries face higher average losses than firms in the financial services sector; however, the difference is not as substantial as it is for cyber risk.

Table 3 Cyber and non-cyber risk losses (in million US$)

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

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

An important aspect of cyber risk is contagion, and thus our next separation of the data is between incidents affecting only one single firm and those affecting multiple firms (Panel C of Table 3). If just one firm is involved (83.2% of the cyber risk cases), the average loss per firm per case is more than twice as high as if more than one firm is involved. This result may appear counterintuitive; however, in the event more than one firm is affected, cyber attacks are identified earlier and thus losses can be limited. Also, there may be economies of scale in solving the problems created by cyber incidents when multiple firms are involved (e.g., forensic investigation costs).[13]

Panel D of Table 3 separates the sample based on firm size. With increasing size, the number of incidents increases, i.e., firms with more than 250 employees have more cyber losses. Interestingly, we observe a U-shaped pattern in the mean losses both for cyber and non-cyber risk.[14] It may be that smaller firms do not have the awareness and resources to protect against cyber risk, while large firms have diseconomies of scale due to complexity.[15]

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

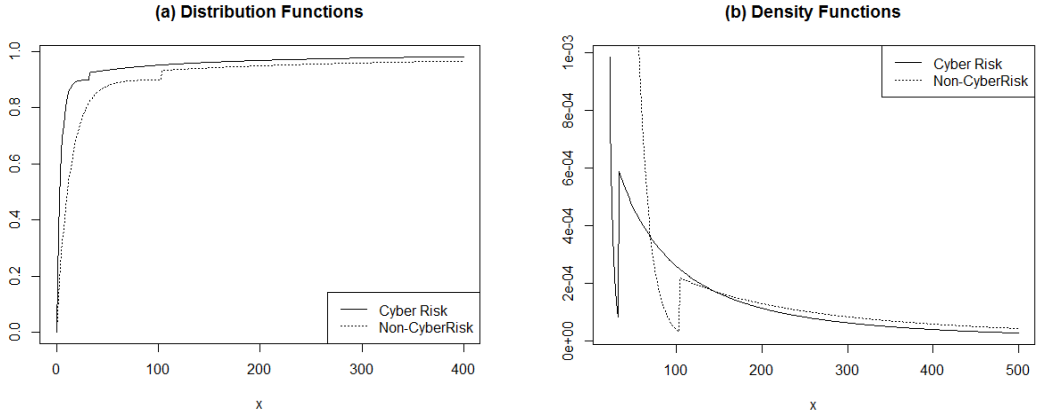
[14] The results are robust with regard to the size categorization. We estimated the values for a separation into Small: less than 100, Medium: less than 1,000, and Large: more than 1,000 employees and find no differences in this pattern.

[15] We also analyzed the development of cyber risks over time and found that the number of cyber risk incidents was relatively small before 2000. After that point, however, the number of incidents continuously increased and in the last years accounts for a substantial part of all operational risk incidents. These findings again emphasize the increasing economic importance of cyber risk in recent years. The average loss, however, has

3.2 Modelling Results and Goodness of Fit

To more closely analyze the distributional characteristics of cyber risk compared to other operational risk, we implement methods from extreme value theory when estimating the loss severity distribution (e.g., Peaks-over-Threshold method; POT). In this approach, losses above a predefined threshold are modeled by a generalized Pareto distribution (GPD) while losses below the threshold are modeled with a distribution common in loss modelling (e.g., the Exponential distribution as in Hess, 2011).[16] The estimated distributions for cyber and non-cyber risk are shown in Figures 1.

Figure 1 Estimated distribution and density function



In addition, we model losses with other parametric distributions common in actuarial science, such as the Exponential, Gamma, GPD, Log-normal, or Weibull distribution (see, e.g., Eling, 2012). Results of the goodness of fit analysis are presented in Table 4.

Table 4 Goodness of Fit Analysis

Model	Cyber Risk (N = 994)			Non-Cyber Risk (N = 21,081)		
	Log-likelihood	AIC	Kolmogorov-Smirnov-Test	Log-likelihood	AIC	Kolmogorov-Smirnov-Test
POT (threshold 90%)	CS	CS	CS	CS	CS	CS
Exponential	-4,673.87	9,349.75	0.582 ***	118,088.10	236,178.10	0.535 ***
Gamma	-3,430.25	6,864.50	0.243 ***	-95,081.78	190,167.60	0.220 ***
GPD	**-2,925.01**	**5,854.03**	0.435 ***	**-86,226.42**	**172,456.80**	0.218 ***
Log-normal	-2,938.64	5,881.28	0.062 ***	-86,256.49	172,517.00	0.030 ***
Weibull	-3,122.09	6,248.19	0.147 ***	-89,246.14	178,496.30	0.088 ***

Note: In the Kolmogorov-Smirnov-Test the first column represents the distance and the second the significance level of rejecting the null hypothesis (H_0: the given distribution is equal to the sample distribution). *, **, ***, indicate confidence levels of 10%, 5%, and 1%, respectively. AIC = Akaike information criterion, CS = coming soon.

decreased over the last several years, which might indicate the increasing use of self-insurance measures that reduce the loss amount in the event of a cyber attack. Detailed results are available from the authors upon request.

[16] We apply the bootstrap goodness of fit test by Villaseñor-Alva and González-Estrada (2009) and, based on this, choose a threshold at the 90% percentile. For purposes of comparison, we also computed results for a 92.5% threshold, with findings similar to those with 90% threshold; thresholds below reveal a non-fit for non-cyber risks according to Villaseñor-Alva and González-Estrada (2009); raising thresholds much higher makes the sample used for the fit in cyber risk too small.

The results from the Kolmogorov-Smirnov-Tests (K-S tests) indicate that none of the five single parametric distributions models the cyber risk loss data adequately. Furthermore, these distributions also do not fit the non-cyber risk data, which motivates the use of more advanced modelling approaches. From the five distributions, the GPD provides the best results, but also for this model the null hypothesis in the K-S test is rejected at a 1% confidence level.

In the following version of the paper we will also present an extended version of this POT approach where the loss distribution depends on covariates (following Chavez-Demoulin, Embrechts, and Hofert, 2013) and fit the loss data to various other distributions which have proven to be useful for actuarial loss analysis (e.g., the g-and-h family of distributions, the Generalized Beta distribution of the second kind, and skewed distributions; see, e.g., Eling, 2012).

3.3 Applications

We first conduct a numerical study to estimate the risk measures value at risk and tail value at risk. These measures are especially relevant for regulatory purposes in banking and insurance (Basel II, Solvency II). Table 5 presents the risk measurement results for cyber and non-cyber risk for the POT models and the five parametric distributions.

Table 5 Risk Measurement

Model	Cyber Risk (N = 994)		Non-Cyber Risk (N = 21,081)	
	VaR	TVaR	VaR	TVaR
POT (threshold of 90%)	**90.71**	**1,026.25**	**245.04**	**2,332.72**
Exponential	121.45	162.11	298.06	398.64
Gamma	197.00	320.95	472.03	759.73
GPD	81.80	115,792.30	**246.73**	428,691.10
Log-normal	60.95	209.92	198.84	709.35
Weibull	**83.13**	176.63	229.75	471.68
Empirical	89.56	676.88	248.97	1,595.27

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

The VaR estimator for cyber risk, applying the Exponential, Gamma, and Log-normal distribution, is significantly different from the empirical VaR, which indicates that the distribution assumption does not fit the data well in the tail. The result for the Weibull distribution is much closer to the empirical VaR than the other four parametric distributions. However, the estimate from the POT provides the best fit for the VaR. Similar results can be observed for the TVaR. The Exponential, Gamma, Log-normal, and Weibull distribution significantly underestimate the TVaR, which suggests that they are not modelling the tail-behavior appropriately. Although overestimating the tail-losses, the POT approach again provides the best fit. Moreover, a more conservative estimation might be appropriate for

regulatory purposes.[17] In the comparison of non-cyber risks, GPD and the POT approach provide the best fit for VaR, while again the POT approach shows the best approximation of the TVaR. Furthermore, the results show that the distribution of cyber risk differs significantly from the distribution of other operational risks. For example, the distribution of the non-cyber risk sample shows much higher VaR and TVaR than that of the cyber risk sample, explaining in part the much higher maximal losses in these categories.[18] This finding implies that when modeling operational risk, cyber risk needs to be considered separately.

Secondly, we will use the numerical results to yield a price for a standard cyber insurance policy. This will help to get a sense for the economic relevance of these risks. The results will be added in the next draft of the paper.

4 Conclusions

Insurance firms start to sign cyber risk policies and might not have a lot experience with cyber risks. For the pricing process of insurance contracts and the estimation of security capitals, a good understanding of the properties and behavior of the risk is vital. Furthermore, regulatory approaches for new data protection and regulation schemes are expected to come (see, e.g., a proposal for the EU; European Commission, 2012). Our findings can provide insight what parts it is most important to look at and what security levels they have to postulate in the risk management processes of their supervised companies. The results of the paper might thus offer important insights for the management of cyber risks, about their insurability and might also provide guidance for the pricing of cyber insurance policies. They are relevant for policymakers and regulators that need to develop sound policies for the treatment of this new, dynamic risk category. For the academic audience we present effective and contemporary modeling and solution approaches for the novel application area of cyber risk.

We need to highlight the limitations of the paper, which will also yield some avenues for future research opportunities. For example, the identification strategy should not be interpreted as more as a first step towards a more thorough analysis of cyber risk. What we do is extracting cases with a predefined criteria catalogue; collecting an own database with cyber risk would be a useful avenue for future research. Also our risk estimates are only a first indication of the true cyber risk; e.g. since reputational risks are not incorporated. If the models from operational risk prove to be useful for an analysis of cyber risks, then recent papers from this field can also be used to estimate the potential reputational effect (see, e.g.,

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

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

Cummins, Lewis, and Wei, 2006 or Cannas, Masala, and Micocci, 2009). We either can directly integrate it in the paper or, alternatively, place it in the conclusion of the paper as an avenue for future research.

References

Ackerman, G. (2013) 'G-20 urged to treat cyber-attacks as threat to global economy,' Bloomberg, from www.bloomberg.com/news/2013-06-13/g-20-urged-to-treat-cyber-attacks-as-threat-to-economy.html, accessed 18 January 2014.

Aue, F., and Kalkbrener, M. (2006) 'LDA at work: Deutsche Bank's approach to quantify operational risk', Operational Risk 1(4), 49-93.

Balkema, A. A., and de Haan, L. (1974) 'Residual life time at great age', Annual Probability 2, 792-804.

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

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.

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

Bowers, N., Gerber, H. U., Hickman, J., Jones, D., and Nesbitt, C. (1997) 'Actuarial Mathematics', 2nd ed., Society of Actuaries, Schaumburg, IL.

Cannas, G., Masala, G., and Micocci, M. (2009) 'Quantifying Reputational Effects for Publicly Traded Financial Institutions', Journal of Financial Transformation 27, 76-81.

Cummins, J. D., Lewis, C. M., and Wei, R. (2006) 'The Market Value Impact of Operational Loss Events for US Banks and Insurers', Journal of Banking and Finance 30(10), 2605-2634.

Cope, E., and Labbi, A. (2008) 'Operational loss scaling by exposure indicators: Evidence from the ORX database', The Journal of Operational Risk 3(4), 25-45.

Cope, E. W., Piche, M. T., and Walter, J. S. (2012) 'Macroenvironmental determinants of operational loss severity', Journal of Banking and Finance 36(5), 1362-1380.

Chavez-Demoulin, V., Embrechts, P., and Hofert, M. (2013) 'An extreme value approach for modeling Operational Risk losses depending on covariates', Working Paper.

Chavez-Demoulin, V., Embrechts, P., and Nešlehová, J. (2006) 'Quantitative models for operational risk: Extremes, dependence and aggregation', Journal of Banking & Finance 30(10): 2635-2658.

Cebula, J. J. and Young, L. R. (2010) A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

CEIOPS (2009) CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR Standard Formula – Article 111 (f): Operational Risk. CEIOPS-DOC-45/09, Frankfurt: Committee of European Insurance and Occupational Pensions Supervisors.

Dahen, H., and Dionne, G. (2010) 'Scaling models for the severity and frequency of external operational loss data', Journal of Banking and Finance 34(7), 1484-1496.

Davison, A. C. (1984) 'Modelling excesses over high thresholds, with an Application', in J. de Oliveira (ed.), Statistical Extremes and applications, D. Reidel, 461-482.

De Fontnouvelle, P., Dejesus-Rueff, V., Jordan, J. S., and Rosengren, E. S. (2006) 'Capital and risk: New evidence on implications of large operational losses', Journal of Money, Credit, and Banking 38(7), 1819-1846.

Degen, M., Embrechts, P., and Lambrigger, D.D. (2007) 'The quantitative modeling of operational risk: between g-and-h and EVT', ASTIN Bulletin 37(2), 265-291.

Dutta, K., and Perry, J. (2007) 'A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital', Working Paper No. 06-13, Federal Reserve Bank of Boston.

Eling, M. (2012) 'Fitting insurance claims to skewed distributions: Are the skew-normal and skew-student good models?', Insurance: Mathematics and Economics 51(2), 239-248.

Eling, M., and Tibiletti, L. (2010) 'Internal vs. external risk measures: How capital requirements differ in practice', Operations Research Letters 38(5), 482-488.

Embrechts, P., Klüppelberg, C., and Mikosch, T. (2003) 'Modelling Extremal Events for Insurance and Finance', Springer.

European Commission (2012) 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)', from ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf, accessed 18 January 2014.

Ganegoda, A., and Evans, J. (2013) 'A scaling model for severity of operational losses using generalized additive models for location scale and shape (GAMLSS)', Annals of Actuarial Science 7(1), 61-100.

Giacometti, R., Rachev, S., Chernobai, A., Bertocchi, M., and Consigli, G. (2007) 'Heavy-Tailed Distributional Model for Operational Losses', Working Paper.

Gourier, E., Farkas, W., and Abbate, D. (2009) 'Operational risk quantifying using extreme value theory and copulas: from theory to practice', The Journal of Operational Risk 4(3), 1-24.

Gordon, L.A., Loeb, M.P. and Sohail, T. (2003) 'A framework for using insurance for cyber-risk management', Communications of the ACM 44(9): 70–75.
Gustafsson, J, Nielsen, J. P., Pritchard, P., and Roberts, D. (2006)' Operational risk guided by kernel smoothing and continuous credibility: A practitioner's View', The Journal of Operational Risk 1(1), 43-56.
Hess, C. (2011) 'The impact of the financial crisis on operational risk in the financial services industry: Empirical evidence', Journal of Operational Risk 6(1): 23-35.
Hofmann, A. and Ramaj, H. (2011) 'Interdependent risk networks: The threat of cyber attack', International Journal of Management and Decision Making 11(5/6): 312–323.
KPMG (2013) 'e-Crime – Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz', KPMG Forensic Services, from www.kpmg.com/CH/de/Library/Articles-Publications/Seiten/e-crimesurvey-2013.aspx, accessed 18 January 2014.
McNeil,A. J., Frey, R., and Embrechts, P. (2005) 'Quantitative Risk Management: Concepts, Techniques, Tools', Princeton University Press.
Moscadelli, M. (2004) 'The modelling of operational risk: Experience with the analysis of the data collected by the Basel Committee', Technical Report 517, Banca d'Italia.
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.
Pickands, J. (1975) 'Statistical inference using extreme order statistics', Annals of Statistics 3, 119-131.
Ponemon Institute (2013) 'Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age', from www.assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf, accessed 18 January 2014.
Reiss, R.-D., and Thomas, M. (2007) 'Statistical Analysis of Extreme Values', Birkhäuser Verlag, Basel – Boston – Berlin.
Shevchenko, P. V. (2010) 'Implementing loss distribution approach for operational risk', Applied Stochastic Models in Business and Industry 26(3), 277-307.
Shih, J., Khan, A., and Medepa, P. (2000) 'Is the size of an operational loss related to firm size?', Operational Risk Magazine 2(1), 1-2.
Soprano, A., Crielaard, B., Piacenza, F., and Ruspantini, D. (2009) 'Measuring operational and reputational risk – A Practitioner's Approach', Wiley, Finance.
Villaseñor-Alva, J.A. and González-Estrada, E. (2009) 'A bootstrap goodness of fit test for the generalized pareto distribution', Computational Statistics and Data Analysis 53(11): 3835-3841.
World Economic Forum (2014) 'Global Risks 2014 – Ninth Edition', from www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf, accessed 17 April 2014.
Wilson, S. (2007) 'A Review of Correction Techniques for Inherent Biases in External Operational Risk Loss Data', Australian Prudential Regulation Authority.

Appendix

Appendix A: 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* needs to be involved in the cause of the cyber risk incident (e.g., hackers, employees, system, nature), and (3) a relevant *outcome* such as the loss of data or misuse of confidential data needs to be present (see Table A1 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 A2). The resulting dataset includes a total of 994 cyber risk incidents, or about 4.5% of the total sample of operational risks.

Table A1 Data Search Strategy

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

Table A2 Keywords per Criteria

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

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

Appendix B: Methodology

Fitting of Single Parametric Distributions

As a first insight on the distributional properties and because of its easy implementation, the data can be fitted by single parametric distributions. For operational risk, literature suggests the use of more advanced methodologies (mostly from extreme value theory) to model these kind of losses, since simple distributions were found to provide no perfect fit for the extreme events in operational risk (e.g. Moscadelli, 2004). In Section 3.1, we observed that cyber risk losses are much smaller than operational losses. Thus, there might be reasons to believe that the simple parametric distributions can provide a better fit for cyber risk than for operational risk. Thus, we fit parametric distributions first, for instance, Log-normal, Exponential, Gamma, Weibull, Log-Weibull, GPD, Burr, symmetrized alpha-stable, Log-alpha-stable (see Giacometti et al., 2007).

Approaches from Extreme Value Theory (EVT)

If the distribution fitting is used to compute risk capitals (e.g. required in Basel II and Solvency II for operational risks) the single estimation of severity distributions is not adequate, since the distribution of events over time is neglected. Furthermore, the extreme events that can occur in operational risk might not be modelled adequately. For these purposes, methods from EVT have proven to be the right choice in operational risk modelling (see, e.g., McNeil, Frey, and Embrechts, 2005; Embrechts, Klüppelberg, and Mikosch, 2003; Reiss and Thomas, 2007, for an introduction). In this area the loss distribution approach (LDA) has become the most common model, where a loss-frequency distribution and a loss-severity distribution are fitted separately on historical data. The first describes the occurrence of losses over time, while the latter provides information on the potential size of the losses. Afterwards these two distributions are combined to an aggregated loss distribution (see, e.g., McNeil, Frey, and Embrechts, 2005). Since in most of these models there are no closed-form formulas for the aggregates available, the aggregation is typically done by Monte Carlo Simulation.[19] For the modeling of frequency and severity distributions a variety of different approaches exist that we briefly introduce in the following parts.

[19] In banking this approach is applied on a yearly basis and for each business line an aggregated loss distribution is estimated. From those an overall annual loss distribution is estimated by a copula approach that enables to account for diversification effects between business lines (see, e.g., Gourier, Farkas, and Abbate, 2009). This final distribution is then used for the calculation of capital requirements. For an example in the industry we refer to Soprano et al. (2009) for UniCredit Group, or Aue and Kalkbrener (2006) for Deutsche Bank.

Loss-frequency Distribution

The loss-frequency distribution is commonly modeled as a homogeneous Poisson process. It is assumed that the mean number of events occurring in a fixed time interval is constant over time. In practice this could not be confirmed for operational risk (Giacometti et al., 2007). Thus, if it is assumed that the mean number of events in a given time period changes over time, non-homogeneous Poisson processes are used (Giacometti et al., 2007). Those processes assume that the intensity parameter (which defines the average number of events) can be expressed by a mathematical function depending on time. Giacometti et al. (2007) assumes the intensity functions to be Log-normal or Log-Weibull.

Loss-severity Distribution

For the loss-severity distributions, a variety of different approaches are discussed in the literature. For instance, the severity can be modeled by a simple parametric distribution (e.g., Pareto, Log-normal, etc.; Giacometti et al., 2007). However, those approaches do not cover the extreme events of operational risk adequately (Moscadelli, 2004). Thus, an approach that is often applied is the Peak-over-threshold (POT) approach (Embrechts, Klüppelberg, and Mikosch, 2003), in which the extreme values (losses above a predefined threshold u) of the severity distribution are modeled separately from the main body of the losses. The approach is based on the Balkema-de Haan-Pickands Theorem, which states that if the threshold u is chosen reasonably high, the distribution above the threshold can be modeled by a GPD (Pickands, 1975, and Balkema and de Haan, 1974). The body is then fitted on one of the simple parametric distributions discussed before, e.g., exponential (Hess, 2011) or Log-normal distribution (Moscadelli, 2004).[20]

More Advanced Methods from EVT

In literature, several limitations in the estimation of operational losses by the standard EVT approaches are discussed. Those in particular occur, if external data is used. Wilson (2007), for instance, provides a review on biases inherent in external operational risk loss data and discusses potential correction techniques:

- Reporting bias: occurs when different thresholds are used to report losses (e.g. the SAS OpRisk Global data covers losses above US$ 100’000 only, overestimating the losses since it has been fitted to a too large number of higher losses). An approach to correct for

[20] In Biener, Eling, and Wirfs (2015) we provide a first analysis of the loss-severity distribution using POT following Hess (2011).

reporting bias is proposed in De Fontnouvelle et al. (2006). In our case, we know the reporting threshold and can apply the method used in Hess (2011).

- Control bias: occurs because data is generated by institutions with different control mechanisms. Some losses might be irrelevant for some firms, thus not collected, while they might for others, which then cannot be used. We assume that this poses not a problem for our dataset, since we look at publicly reported incidents, reported in media.
- Scale bias: occurs because data is generated by institutions with different sizes (i.e., the loss severity of firms in external databases depends on the size of the firm). This problem can be incorporated, e.g. by adjusting the loss height depending on firm size and further covariates (e.g. business line, and event type; see Ganegoda and Evans, 2013).

Since, Ganegoda and Evans (2013) only adjust the loss-severity distribution by covariates, Chavez-Demoulin, Embrechts, and Hofert (2013) discuss an approach for loss-frequency and loss-severity. In addition, they add a time-dependence to their model, such that changes in loss-frequency / -severity can be modelled appropriately. One of the advantages of this approach is, that data can be pooled (data does not need to be separated into different groups, e.g., business lines, for which the fitting of the distribution must be done separately to figure out differences in the distributions across business lines), and by that sample size does not reduce. Furthermore, interactions between different covariates can be measured (e.g. an interaction between type of loss and change in frequency can be analyzed). The following covariates can and should be modelled by our approach:

- Time: For operational losses Chavez-Demoulin, Embrechts, and Hofert (2013) observed changes in loss-severity and loss-frequency over time. Chavez-Demoulin, Embrechts, and Nešlehová (2006) find a significant relationship between loss-frequency and time.

  Cyber risk's economic importance increased heavily in recent years and thus suggests that cyber risk losses developed over time also. In Biener, Eling, and Wirfs (2015) we observe a relatively small amount of cyber risk incidents before 2000; however, a continuous increase in the last years was shown. For loss severity, average losses decreased over the last years and gave reason to believe that increased use of self-insurance measures reduced the losses occurred.
- Size: The relationship between firm size and the loss severity is extensively discussed in the literature. For instance, Shih et al. (2000), Cope and Labbi (2008), and Ganegoda and Evans (2013) all discuss this relationship and find a positive correlation between size and loss height. This phenomenon is also called the scaling problem or scale bias, which occurs when data is collected from institutions with different sizes.

For our analysis of cyber risk, firm size might also have an influence, in particular on severity AND frequency. The larger the firm, the more sensitive data might be available, the higher the potential losses. The larger the company, the more complex the operations and the more often mistakes and incidents happen. In the descriptive analyses of Section 3.1 we observed an increasing number of incidents with increasing size (measures by number of employees). For the mean losses we observe a u-shape, which makes the inclusion of non-linear size variables in the approach appropriate.

- Business Line: The relation between business lines and loss severity has been analyzed in Dahen and Dionne (2010), Ganegoda and Evans (2013), and Chavez-Demoulin, Embrechts, and Hofert (2013). In the latter paper, the relationship has been analyzed also for the loss-frequency. The results show significant differences for business lines and suggest the analysis also for our approach.

  Unfortunately, in our approach we consider all industries and are not focused on the banking industry as the existing studies. Thus, a separation into the business lines, as, e.g. in Chavez-Demoulin, Embrechts, and Hofert (2013), is not applicable in our case. However, we can differentiate into firms from the financial and nonfinancial industry. In Section 3.1 we observed essential differences for this covariate in cyber losses (most incidents occur in the financial industry group, however, the average losses are just about half of those from the nonfinancial industry).
- Event type: The approaches in Dahen and Dionne (2010) and Ganegoda and Evans (2013) incorporate the event category for operational losses coming from the Basel regulations. As before for business lines, this was modelled for the banking industry specifically. We can easily adjust this to the cyber risk event types discussed in Cebula and Young (2010). In Section 3.1 we identified most of the incidents to fall in the category “Actions of people”, and by that showed that the human behavior is the main source of cyber risk. The average losses per category however, are very similar.
- Geographical region: To the best of our knowledge, we would be the first to differentiate by a geographical covariate. We believe that for cyber risk it is essential, since regulatory / legal responsibilities are completely different for different areas in the world and self-protection standards might be different or regulated differently. In Section3.1 we show that Northern American companies experience more than twice as many cyber risk incidents than European firms, however, for loss severity they show one of the smallest average losses. It could be worthwhile to incorporate this covariate into our analysis.

- For potential further macroenvironmental determinants, see Cope, Piche, and Walter (2012) (e.g., executive power, prevalence of insider trading, shareholder protection laws, restrictions on banking activity, supervisory power, per capita activity, and a government index).

In the further work, we might identify additional covariates that could be interesting to analyze and which could be covered by our dataset.

Further Approaches Beyond Operational Risks

In the paper we will also go beyond standard operational risk models and look at recent developments in the field of actuarial science in order to identify the model which best describes the cyber risk data.

For instance, Dutta and Perry (2007) fitted the g-and-h family of distributions and the Generalized Beta distribution of the second kind (GB2) to operational losses. These approaches were found to provide reasonable fits for non-EVT approaches. Both distributions can be used as approximations for many of the previously mentioned one- and two-parameter distributions and accommodate a wide variety of tail-thicknesses and permit skewness as well (see Dutta and Perry, 2007). Thus, on the one hand, the approach from Dutta and Perry (2007) could provide new insights on the distributional behavior of cyber risk, but on the other hand could serve as a robustness test of the results found earlier. Degen, Embrechts, and Lambrigger (2007) extend Dutta and Perry (2007)'s approach by discussing some fundamental properties of the g-and-h distribution and their link to EVT. They show that under some instances the quantile estimation by EVT approaches might be inaccurate if data is well modelled by a g-and-h distribution.

Another approach that has been applied to operational losses in literature is the one explained in Gustafsson et al. (2006). The approach is based on a non-parametric smoothing technique, utilizing the Generalized Champerowne distribution (GCD). The advantage of his approach is that the tail behavior can be modelled adequately, but unlike EVT, the modelling is done by data from the full distribution (the POT approach models body and tail separately, not considering information from the other part of the distribution). Finally, we fit skewed distributions to the loss data (e.g. skew-normal and skew-student), that have proved to be adequate in describing property-liability insurance claims (Eling, 2012).[21]

[21] All the approaches discussed before, are based in their estimation procedure on maximum-likelihood estimation. Shevchenko (2010) describes an alternative to maximum likelihood based on Bayesian Inference. This approach could be worth to implement since previous knowledge could be incorporated in this approach (e.g. properties of operational risk could be interesting for cyber risks).

Methodology for Comparison of Models

To compare the different fitting approaches with each other, and identify the one that works best, we first apply goodness-of-fit tests that compare the fitted distributions with the empirical data (Kolmogorov-Smirnov and Anderson-Darling test). These tests are standard in the fitting of parametric distributions (Moscadelli, 2004). More tailored tests, in particular for the POT approach, are given in Davison (1984), and Reiss and Thomas (2007). Further tests that provide insights about the appropriateness of estimations are severity VaR performance analyses (Moscadelli, 2004), which we will conduct in a second step. Since most of the fitting algorithms are based on maximum likelihood estimation, we can also compare Log-likelihood values and ground our analysis on the Akaike information criterion (AIC) or the Bayesian information criterion (BIC). A variety of further tests might come up during our implementation period. For the approach in Chavez-Demoulin, Embrechts, and Hofert (2013), further comparison techniques are needed. To identify the best combination of covariates (that model the cyber losses best) and to find the best model specification, Chavez-Demoulin, Embrechts, and Hofert (2013) compare models via likelihood-ratio tests. Furthermore, Ganegoda and Evans (2013) describe an information criterion that could be used to compare two competing models.[22]

Risk Measurement and Pricing of Cyber Insurance Policies

After we have identified the best modelling approach, we will present two applications: Firstly, we will conduct a numerical study to estimate the risk measures value at risk and tail value at risk. These measures are especially relevant for regulatory purposes in banking and insurance (Basel II, Solvency II). Secondly, we will use the numerical results to yield a price for a standard cyber insurance policy. This will help to get a sense for the economic relevance of these risks.

[22] Note, that Ganegoda and Evans (2013) model only the loss-severity, and not loss-frequency AND loss-severity as in the approach of Chavez-Demoulin, Embrechts, and Hofert (2013). Thus, some adjustments might be necessary.