Modelling and Management of Cyber Risk

Martin Eling and Jan Hendrik Wirfs
University of St. Gallen, Switzerland
Institute of Insurance Economics

IAA Colloquium 2015
Oslo, Norway
June 7th – 10th, 2015

Institute of Insurance Economics
University of St.Gallen

Contact Information

Title:

Modelling and Management of Cyber Risk

Authors:

Martin Eling and Jan Hendrik Wirfs

Institute of Insurance Economics

University of St. Gallen

Corresponding Author:

Jan Hendrik Wirfs

Rosenbergstrasse 22

9000 St. Gallen

Switzerland

Tel.: +41 (0)71 / 244 7971

eMail: jan.wirfs@unisg.ch

Modelling and Management of Cyber Risk

Martin Eling[a], Jan Hendrik Wirfs[a,*]

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

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

* Corresponding author. Tel.: +41 71 244 7971.
E-mail address: jan.wirfs@unisg.ch (J. H. Wirfs).

1

Introduction I

"Cyber Risk is the Operational Risk to information and technology assets that have consequences affecting the Confidentiality, Availability or Integrity of information and information systems"

(Cebula and Young, 2010).

Introduction II

Objective

- Provide a thorough empirical analysis of cyber risk
- 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
- Illustrate usefulness of our results for policyholders, regulators, and practitioners in two applications

Contribution

- Practitioners: provide a better understanding of cyber risks and their consequences
- Academic audience: present effective and contemporary modeling and solution approaches for the novel application area of cyber risk

Data and Methodology

Data

- SAS OpRisk Gobal Data (22,075 incidents between March 1971 and September 2009)
- Identification of 994 cyber risk incidents
- Sorting of extended dataset in process (30,173 incidents between March 1971 and March 2014)

Methodology

- Approaches from Extreme-Value-Theory
  - Loss distribution approach (e.g., peak-over-threshold method; POT)
  - Extension of POT where loss data depends on covariates (e.g., time, business line, region etc.) → Chavez-Demoulin, Embrechts, and Hofert (2013)
- Comparison
  - Standard goodness of fit tests and tailored test for more advanced models

Empirical Results I

Descriptive Analysis – Losses per Risk Type (in million US$)

Category	N	Mean	Median	VaR	TVaR	Max.
Panel A: Cyber versus non-cyber risk						
Cyber Risk	994	40.53	1.87	89.56	676.88	13,313
Non-Cyber Risk	21,081	99.65	6.20	248.97	1,595.27	89,143
Panel B: Cyber risk subcategories						
Actions of people	903	40.69	1.83	84.36	679.04	13,313
Systems and technical failure	37	29.07	5.03	168.95	329.04	370
Failed internal processes	41	47.72	2.04	158.65	743.40	1,311
External events	13	39.40	1.03	192.88	422.71	422

<u>Summary:</u>

- All descriptive statistics for cyber risk are smaller than those for non-cyber risk
- Human behavior is the main source of cyber risk
- However, average losses are similar
- Further separation into region of domicile, industry, relation to losses in other firms and company size

Empirical Results II

Descriptive Analysis – Cyber risk losses by subcategories (in million US$)

	N	Share of cyber risk incidents	Mean	Median
Panel A: Region of domicile				
Africa	19	1.91%	38.99	3.20
Asia	180	18.11%	122.18	2.63
Europe	231	23.24%	28.06	1.85
North America	516	51.91%	19.86	1.68
Other	48	4.83%	17.18	1.38
Panel B: Industry				
Nonfinancial	213	21.40%	61.74	5.00
Financial	781	78.60%	34.75	1.44
Panel C: Relation to losses in other firms				
One firm affected	827	83.20%	44.51	1.83
Multiple firms affected	167	16.80%	20.84	2.04
Panel D: Company size by number of employees[*]				
Small	40	4.02%	27.81	1.30
Medium	51	5.13%	10.33	1.33
Large	754	75.86%	46.39	1.50

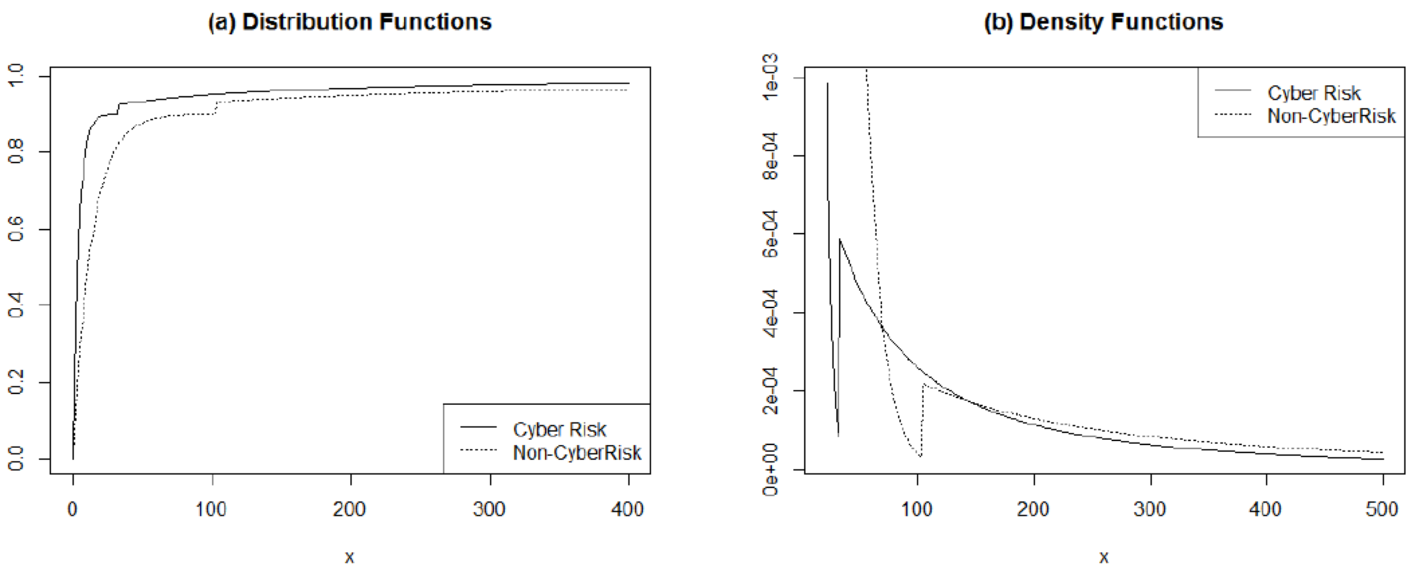
[*] Small: Less than 50 employees; Medium: Less than 250; Large: More than 250. For a few incidents, the number of employees is not available so that the total in each size group does not add up to the total sample number.

Institute of Insurance Economics
University of St.Gallen

Empirical Results III

Peak-over-Threshold Approach

- Losses above a predefined threshold are modeled by a generalized Pareto distribution
- Losses below the threshold are modeled with a distribution common on loss modelling (e.g., exponential distribution)



Empirical Results IV

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%)	**-1,993.81**	**3,989.82**	TC		**-62,836.99**	**125,676.16**	TC	
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	***

Summary:

- None of the 5 single parametric distributions models cyber losses adequately
- GPD provides best fit for single parametric distributions
- POT approach provides best fit for cyber and non-cyber losses

➔ Motivation for extended version of POT and implementation for further approaches

TC = to come, AIC = Akaike information criterion

Institute of Insurance Economics
University of St.Gallen

Empirical Results V

Extended POT Approach

- Distributional parameters of GPD can be described by a function that depends on covariates
- Subgroup-specific distributions without restricting data-sample

Model	Cyber Risk (N = 994)		Non-Cyber Risk (N = 21,081)	
	Log-likelihood	AIC	Log-likelihood	AIC
POT (threshold 90%)	-613.21	1,230.43	-14,606.69	29,217.39
POT Extension (threshold 90%)	**-602.35**	**1,208.70**	**-14,597.50**	**29,199.00**

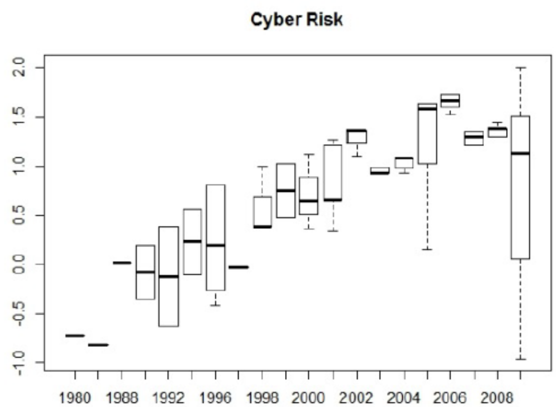
<u>Summary:</u>

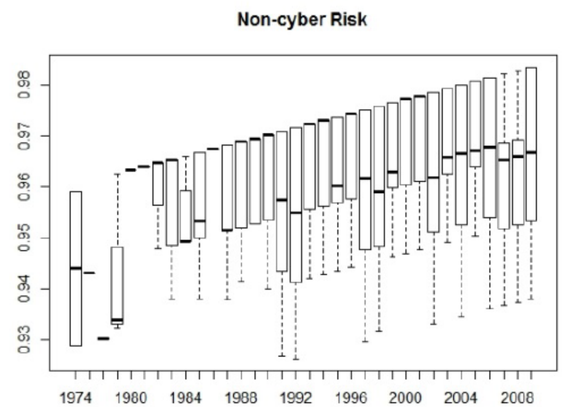
- Approach by Chavez-Demoulin, Embrechts, and Hofert (2013) seems appropriate

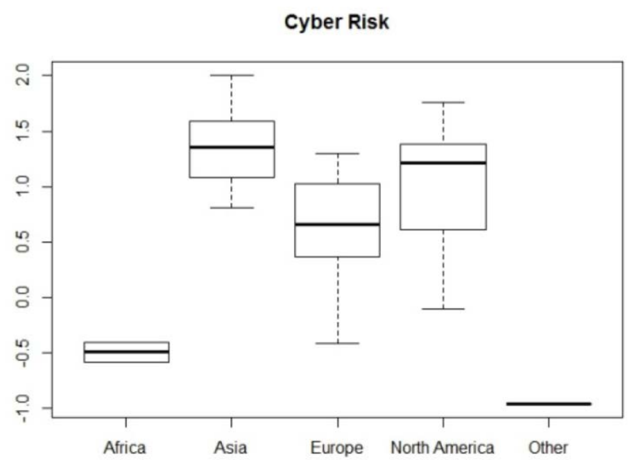
➔ Motivation for more detailed analysis

Empirical Results VI

Examples of Preliminary Results







Plots for the shape parameter
→ indication of heavy-tailedness

Empirical Results VII

Application I – Risk Management

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.

<u>Summary:</u>

- Estimates for single parametric distributions seem inappropriate
- Best fit for VaR with POT, but still not ideal for TVaR
- Cyber losses and non-cyber losses significantly different → cyber risk needs to be considered separately

Conclusion

Summary

- Human behavior is main source of cyber risk
- Cyber risks are very different compared to other operational risks
- Cyber risks become more severe over time

Limitations

- Identification strategy only a first step towards a more thorough analysis of cyber risk → collecting an own database
- Reputational risks are not incorporated → see, e.g., Cannas, Masala, and Micocci (2009) or Cummins, Lewis, and Wei (2006)

References

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

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

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

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.

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.

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.

Modelling and Management of Cyber Risk

Martin Eling and Jan Hendrik Wirfs
University of St. Gallen, Switzerland
Institute of Insurance Economics

IAA Colloquium 2015
Oslo, Norway
June 7th – 10th, 2015

Institute of Insurance Economics
University of St.Gallen

Back-up
Modelling and Management of Cyber Risk

Martin Eling and Jan Hendrik Wirfs
University of St. Gallen, Switzerland
Institute of Insurance Economics

IAA Colloquium 2015
Oslo, Norway
June 7th – 10th, 2015

Institute of Insurance Economics
University of St.Gallen

Further To-Do's

Established Model

- Implementation of loss-frequency → aggregated distribution
- Implementation of pricing example
- Implementation of additional goodness-of-fit tests
- Updating of the dataset (period 1971-2014)

Additional Modelling Opportunities

- Gustafsson et al. (2006): non-parametric smoothing technique, utilizing the generalized Champerowne distribution
- Dutta and Perry (2007): g-and-h family of distributions and Generalized Beta distribution of the second kind
- Eling (2012): skewed distributions (e.g., skew-normal, skew-student)