ERGO Center of
Excellence in Insurance

Eine Einrichtung der TUM gefördert von der ERGO Group

Cyber Risk and Cyber Insurance: Actuarial Challenges and Modelling Accumulation Risk with Marked Point Processes

based on joint work with Matthias Scherer

Gabriela Zeller
Technische Universität München
Fakultät für Mathematik
Lehrstuhl für Finanzmathematik

DGVFM-eWeiterbildungstag 2021, 18 March 2021

ERGO Center of Excellence in Insurance

Eine Einrichtung der TUM gefördert von der ERGO Group

Agenda

1. Introduction

2. A Holistic View on Cyber Risk

3. Actuarial Model

4. Simulation Study

5. Conclusion

Introduction - Academic Literature Review

Numerous contributions from the **academic literature** divided into:

- Development of frameworks and taxonomies (e.g. *Agrafiotis et al. (2018)*)
- Game-theoretic study of interdependent security (e.g. *Bolot and Lelarge (2008)*, *Shetty et al. (2010)*)
- (Empirical) Insurability analysis (e.g. *Biener et al. (2015)*)
- Modelling of attack rates (stochastic processes, time series analysis) (e.g. *Xu et al. (2018)*)
- Dependence modelling of attacks (copula approaches) (e.g. *Herath and Herath (2011)*)
- Models of epidemic spreading on networks (e.g. *Fahrenwaldt et al. (2018)*)
- Statistical analysis of empirical loss data, often using extreme value theory approaches (e.g. *Edwards et al. (2016)*, *Eling and Wirfs (2019)*)

Introduction - Academic Literature Review

Numerous contributions from the academic literature divided into:

- Development of frameworks and taxonomies (e.g. *Agrafiotis et al. (2018)*)
- Game-theoretic study of interdependent security (e.g. *Bolot and Lelarge (2008)*, *Shetty et al. (2010)*)
- (Empirical) Insurability analysis (e.g. *Biener et al. (2015)*)
- Modelling of attack rates (stochastic processes, time series analysis) (e.g. *Xu et al. (2018)*)
- Dependence modelling of attacks (copula approaches) (e.g. *Herath and Herath (2011)*)
- Models of epidemic spreading on networks (e.g. *Fahrenwaldt et al. (2018)*)
- Statistical analysis of empirical loss data, often using extreme value theory approaches (e.g. *Edwards et al. (2016)*, *Eling and Wirfs (2019)*)

Summary:

- Cyber risk and insurance much discussed in academia and practice, but:

→ **Established modelling approach** capturing properties of this new risk type still elusive

Agenda

1. Introduction

2. A Holistic View on Cyber Risk

3. Actuarial Model

4. Simulation Study

5. Conclusion

Cyber Risk - Definition

Problem: **Lack of established definition**

Cyber Risk - Definition

Problem: Lack of established definition

The Geneva Association (2016) suggests the following:

> *Any risk emerging from the use of information and communication technology (ICT) that* ***compromises the confidentiality, availability, or integrity of data or services****.*

The definition includes **origins**,

Cyber Risk - Definition

Problem: Lack of established definition

The Geneva Association (2016) suggests the following:

*Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to **business disruption, (critical) infrastructure breakdown, and physical damage to humans and property**.*

The definition includes origins, **effects**

Cyber Risk - Definition

Problem: Lack of established definition

The Geneva Association (2016) suggests the following:

Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure breakdown, and physical damage to humans and property. Cyber risk is either caused ***naturally or is man-made****, where the latter can emerge from* ***human failure, cyber criminality (e.g. extortion, fraud), cyberwar, and cyber terrorism****. [...]*

The definition includes origins, effects and **causes**.

ERGO Center of Excellence in Insurance

Eine Einrichtung der TUM gefördert von der ERGO Group

Cyber Risk - Definition

Problem: Lack of established definition

The Geneva Association (2016) suggests the following:

Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure breakdown, and physical damage to humans and property. Cyber risk is either caused naturally or is man-made, where the latter can emerge from human failure, cyber criminality (e.g. extortion, fraud), cyberwar, and cyber terrorism. [...]

The definition includes origins, effects and causes.

→ Cyber risk is **dynamic and complex**.

→ The application of **traditional actuarial approaches faces various challenges**.

→ Comprehensive study of cyber risk requires a **multitude of perspectives**.

Cyber Risk - Key Characteristics

Key **challenging properties** of cyber risk (*Eling and Wirfs (2016), Marotta et al. (2017)*):

- Lack of historical data
- Dynamic risk type & strategic threat actors
- Interdependence / accumulation risk
- Difficult impact determination
- Information asymmetry (adverse selection / moral hazard) (?)

Cyber Risk - Key Characteristics

Key **challenging properties** of cyber risk (*Eling and Wirfs (2016), Marotta et al. (2017)*):

- Lack of historical data
- Dynamic risk type & strategic threat actors
- Interdependence / accumulation risk
- Difficult impact determination
- Information asymmetry (adverse selection / moral hazard) (?)

Insurability analysis of cyber risk (*Biener et al. (2015)*):
Most problematic features (in practice) are

- Lack of independence of loss occurrence
- Presence of information asymmetries
- Lack of adequate cover limits

Cyber Risk - Key Characteristics

Key **challenging properties** of cyber risk (*Eling and Wirfs (2016), Marotta et al. (2017)*):

- Lack of historical data
- Dynamic risk type & strategic threat actors
- Interdependence / accumulation risk
- Difficult impact determination
- Information asymmetry (adverse selection / moral hazard) (?)

Insurability analysis of cyber risk (*Biener et al. (2015)*):
Most problematic features (in practice) are

- Lack of independence of loss occurrence
- Presence of information asymmetries
- Lack of adequate cover limits

From now on: formal definition of risk as combination of **threat, vulnerability** and **impact**.

Cyber Risk - Threats

Distinguish **threats** according to **type** and **root cause**:

	Idiosyncratic incidents		*Systemic events*	
	Targeted attack	Individual failure	Untargeted attack	Mass failure
Data Breach (DB)	Targeted data theft	Individual unintended data disclosure	Data theft through widespread malware / phishing	Unintended data disclosure at cloud service provider
Business Interruption (BI)	Targeted (D)DoS / Ransomware Attack	Disruption of IT system or process through accidental malfunction	Widespread ransomware attack	Cloud service outage disrupting business services
Fraud / general (FR)	CEO fraud through targeted (spear-)phishing attack	Accidental compromise of database by employee	Widespread ransomware attack or social engineering fraud	Accidental compromise of data stored at cloud service provider

- **Types** are distinguished along their compromise of confidentiality, availability or integrity.
- **Systemic events** stem from the existence of a common vulnerability and cause multiple simultaneous **incidents**.
- **Idiosyncratic incidents** are connected to the characteristics of the affected / targeted company.

ERGO Center of Excellence in Insurance

Eine Einrichtung der TUM gefördert von der ERGO Group

Cyber Risk Model - Company Characteristics

Companies are viewed as **heterogeneous**

→ different exposure and resilience to identified threats

→ different impact of a given combination of threat and vulnerability

Relevant characteristics:

Covariate	Abbreviation	Type	Scope	Information Availability
Industry Sector	b	Categorical	FI: Finance and Insurance BR: Businesses (Retail) HC: Healthcare EDU: Education GOV: Government and Military MAN: Manufacturing	Public data
Size	s	Ordinal	1 Small 2 Medium 3 Large	Public data or questionnaire, use revenue and/or number of employees.
Data	d	Ordinal	1 Low risk 2 Medium risk 3 High risk	Self-report via questionnaire, use combination of number of stored records and type of data.
IT Security Level	c	Numerical	$[c_{min}, c_{max}] \overset{\text{w.l.o.g.}}{=} [0, 1]$	Self-report via questionnaire or assessment by insurer's service provider.
Number of suppliers	$nsup$	Ordinal	1 Low 2 Medium 3 High	Self-report via questionnaire or estimation from industry sector and company size.

Eine Einrichtung der TUM gefördert von der ERGO Group

Agenda

1. Introduction
2. A Holistic View on Cyber Risk
3. **Actuarial Model**
4. Simulation Study
5. Conclusion

Insurance Portfolio

Assume K **insured firms** with **covariates** $x_j = (x_{j1}, \cdots, x_{j5})' = (b_j, s_j, d_j, c_j, nsup_j)', \quad j \in \{1, \ldots, K\}$

Examples for **covariate ranges**:

- Industry sector $b_j \in$ {FI, HC, BR, EDU, GOV, MAN}
  (FI = Finance and Insurance, HC = Healthcare, BR = Business (Retail), EDU = Education, GOV = Government and Military, MAN = Manufacturing)
- Size $s_j \in \{$small, medium, large$\}$ (by annual revenue and/or number of employees)
- Data $d_j \in \{$1 = Low risk, 2 = Medium risk, 3 = High risk$\}$ (by number of stored records and whether sensitive data (e.g. PII, PHI) is stored)
- IT Security Level $c_j \in [0, 1]$ (measured on a standardized scale)
- Number of suppliers $nsup_j \in \{$1 = Low, 2 = Medium, 3 = High$\}$

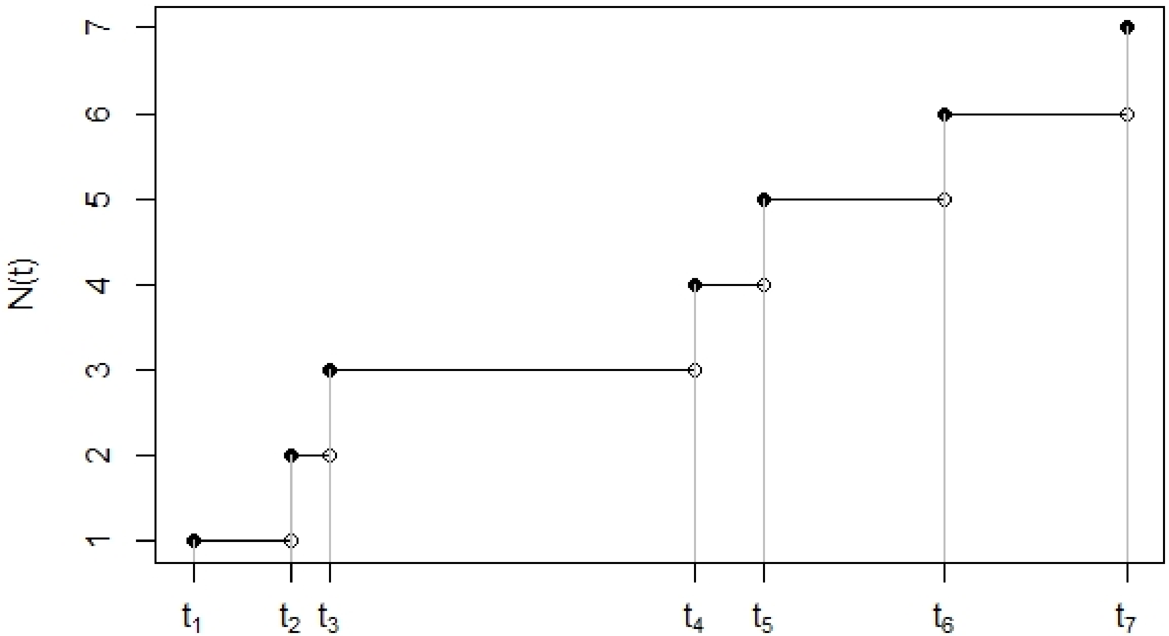
→ $K \times 5$ **covariate matrix** given by

$$\mathbf{X} = \begin{pmatrix} x_1' \\ \vdots \\ x_K' \end{pmatrix} = \begin{pmatrix} x_{11} & \cdots & x_{15} \\ \vdots & \ddots & \vdots \\ x_{K1} & \cdots & x_{K5} \end{pmatrix}.$$

ERGO Center of Excellence in Insurance

Eine Einrichtung der TUM gefördert von der ERGO Group

Excursus: A (Simple) Point Process



Loss Frequency - Idiosyncratic Incidents

Occur **independently** across firms with rate **depending on covariates** $\rightarrow$ **simple point processes**

Loss Frequency - Idiosyncratic Incidents

Occur independently across firms with rate depending on covariates $\to$ simple point processes

Specifically, a **non-homogeneous Poisson process** on $[0,\infty)$ with rate:

$$\lambda_j^{\cdot,idio}(t) := \lambda^{\cdot,idio}(x_j,t) = \exp(f_{\cdot}(x_j) + g_{\cdot}(t))$$

with $\cdot \in \{DB, BI, FR\}$, $f_{\cdot}(x_j) = \alpha_{\lambda,\cdot} + \sum_k f_{\lambda,\cdot,k}(x_{jk})$ and measurable $g_{\cdot} : [0,\infty) \to \mathbb{R}$ (standard GAM).

Loss Frequency - Idiosyncratic Incidents

Occur independently across firms with rate depending on covariates $\rightarrow$ simple point processes

Specifically, a non-homogeneous Poisson process on $[0,\infty)$ with rate:

$$\lambda_j^{\cdot,idio}(t) := \lambda^{\cdot,idio}(x_j,t) = \exp(f_\cdot(x_j) + g_\cdot(t))$$

with $\cdot \in \{DB, BI, FR\}$, $f_\cdot(x_j) = \alpha_{\lambda,\cdot} + \sum_k f_{\lambda,\cdot,k}(x_{jk})$ and measurable $g_\cdot : [0,\infty) \rightarrow \mathbb{R}$ (standard GAM).

For some time point $T > 0$ let

- $N_j^{DB,idio}(T)$ be the **number of idiosyncratic DBs at firm j** during $[0,T]$
- $N^{DB,idio}(T)$ be the **number of idiosyncratic DBs in the whole portfolio** during $[0,T]$

Loss Frequency - Idiosyncratic Incidents

Occur independently across firms with rate depending on covariates $\rightarrow$ simple point processes
Specifically, a non-homogeneous Poisson process on $[0, \infty)$ with rate:

$$\lambda_j^{\cdot,idio}(t) := \lambda^{\cdot,idio}(x_j, t) = \exp(f_\cdot(x_j) + g_\cdot(t))$$

with $\cdot \in \{DB, BI, FR\}$, $f_\cdot(x_j) = \alpha_{\lambda,\cdot} + \sum_k f_{\lambda,\cdot,k}(x_{jk})$ and measurable $g_\cdot : [0, \infty) \rightarrow \mathbb{R}$ (standard GAM).
For some time point $T > 0$ let

- $N_j^{DB,idio}(T)$ be the number of idiosyncratic DBs at firm j during $[0, T]$
- $N^{DB,idio}(T)$ be the number of idiosyncratic DBs in the whole portfolio during $[0, T]$

- On **individual firm level**:

$$N_j^{DB,idio}(T) \sim Poi\left(\Lambda_j^{DB,idio}(T)\right), \quad \text{where } \Lambda_j^{DB,idio}(T) = \int_0^T \lambda_j^{DB,idio}(t)dt, \; \forall j \in \{1, \dots, K\}.$$

- On **portfolio level** (by superposition):

$$N^{DB,idio}(T) \sim Poi\left(\Lambda^{DB,idio}(T)\right), \quad \text{where } \Lambda^{DB,idio}(T) = \int_0^T \Big(\sum_{j=1}^K \lambda_j^{DB,idio}(t)\Big)dt.$$

Loss Frequency - Incidents from Systemic Events

Common vulnerability causes **multiple simultaneous arrivals** $\rightarrow$ **marked point processes**

Loss Frequency - Incidents from Systemic Events

Common vulnerability causes multiple simultaneous arrivals $\rightarrow$ marked point processes

Specifically, start with a **non-homogeneous Poisson process** $N_g^{\cdot}$ (**ground process** for the whole system) with rate:

$$\lambda^{\cdot,g}(t) = \exp(g_{\lambda^{\cdot,g}}(t)).$$

Each arrival of the ground process, $\{t_i\}_{i\in\mathbb{N}}$, carries a **two-dimensional mark** with components

$$m_i \in \mathscr{M} := [m_{min}, m_{max}] \overset{\text{wlog.}}{=} [0,1], \qquad (\textit{strength})$$
$$S_i \in \mathscr{S} := \mathscr{P}_K, \qquad (\textit{affected subset})$$

$\rightarrow$ **marked point process** $\{t_i, (m_i, S_i)'\}_{i\in\mathbb{N}}$ on $[0,\infty) \times (\mathscr{M} \times \mathscr{S})$.

Loss Frequency - Incidents from Systemic Events

Common vulnerability causes multiple simultaneous arrivals $\to$ marked point processes

Specifically, start with a non-homogeneous Poisson process $N_g^{\cdot}$ (ground process for the whole system) with rate:

$$\lambda^{\cdot,g}(t) = \exp(g_{\lambda^{\cdot,g}}(t)).$$

Each arrival of the ground process, $\{t_i\}_{i\in\mathbb{N}}$, carries a two-dimensional mark with components

$$m_i \in \mathscr{M} := [m_{min}, m_{max}] \overset{\text{wlog.}}{=} [0,1], \qquad (\textit{strength})$$

$$S_i \in \mathscr{S} := \mathscr{P}_K, \qquad (\textit{affected subset})$$

$\to$ marked point process $\{t_i, (m_i, S_i)'\}_{i\in\mathbb{N}}$ on $[0,\infty) \times (\mathscr{M} \times \mathscr{S})$.

Assumptions on conditional mark distribution:

- marks $\{(m_i, S_i)\}_{i\in\mathbb{N}}$ iid., joint mark distribution independent of location $t \in [0,\infty)$
- mark components $\{m_i\}_{i\in\mathbb{N}}$ and $\{S_i\}_{i\in\mathbb{N}}$ independent

Loss Frequency - Incidents from Systemic Events

Common vulnerability causes multiple simultaneous arrivals $\rightarrow$ marked point processes

Specifically, start with a non-homogeneous Poisson process $N_g^{\cdot}$ (ground process for the whole system) with rate:

$$\lambda^{\cdot,g}(t) = \exp(g_{\lambda^{\cdot,g}}(t)).$$

Each arrival of the ground process, $\{t_i\}_{i\in\mathbb{N}}$, carries a two-dimensional mark with components

$$m_i \in \mathscr{M} := [m_{min}, m_{max}] \overset{\text{wlog.}}{=} [0,1], \qquad (\textit{strength})$$

$$S_i \in \mathscr{S} := \mathscr{P}_K, \qquad (\textit{affected subset})$$

$\rightarrow$ marked point process $\{t_i, (m_i, S_i)'\}_{i\in\mathbb{N}}$ on $[0,\infty) \times (\mathscr{M} \times \mathscr{S})$.

Assumptions on conditional mark distribution:

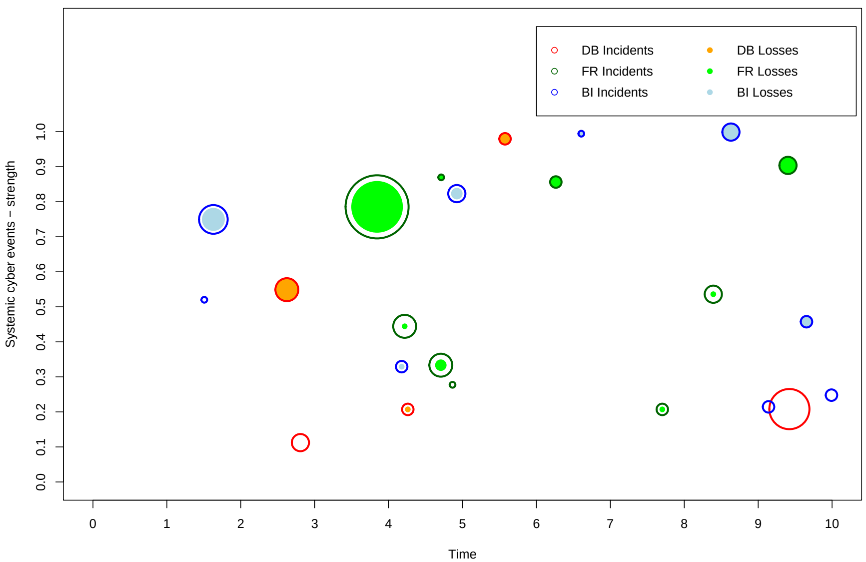
- marks $\{(m_i, S_i)\}_{i\in\mathbb{N}}$ iid., joint mark distribution independent of location $t \in [0,\infty)$
- mark components $\{m_i\}_{i\in\mathbb{N}}$ and $\{S_i\}_{i\in\mathbb{N}}$ independent

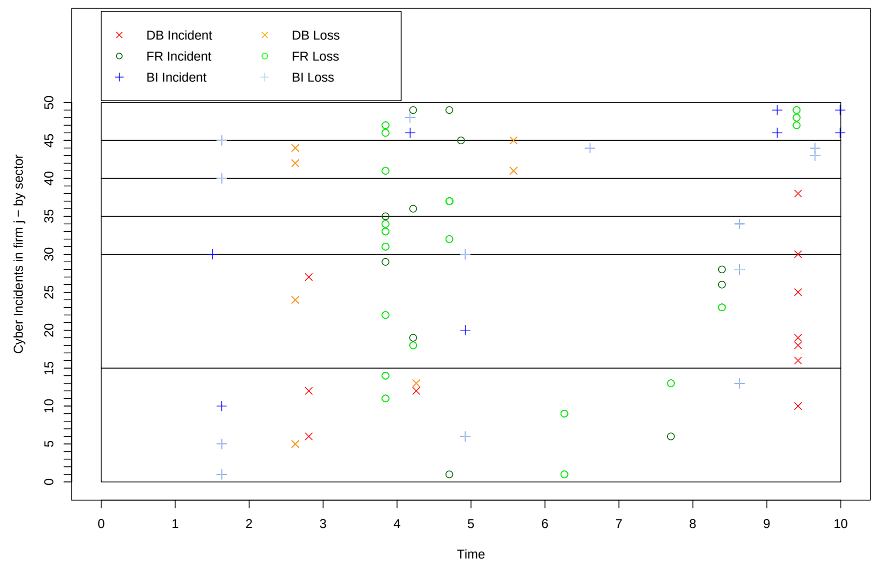
Example:

- An event $\{2,(0.4,\{1,4,7,24,29\})\}$ occurs at "timepoint 2", affects firms indexed $\{1,4,7,24,29\}$ across all industries and causes a loss in any of these firms with IT security level < 0.4 (on a standardized scale)

Loss Frequency - Incidents from Systemic Events

- Event $\{t_i, (m_i, S_i)'\}$ **reaches** firms $\{j \in S_i\}$
- Event $\{t_i, (m_i, S_i)'\}$ **causes a loss** in firms $\{j \in S_i, c_j < m_i\} =: \{j \in S_i^*\}$





Loss Frequency - Incidents from Systemic Events

For some time point $T > 0$ let

- $\bar{N}_j^{DB,syst}(T)$ $(N_j^{DB,syst}(T))$ be the number of systemic DB incidents (losses) at firm j during $[0, T]$
- $\bar{N}^{DB,syst}(T)$ $(N^{DB,syst}(T))$ be the cumulative number of systemic DB incidents (losses) in the whole portfolio during $[0, T]$

Then, given $\{t_i, (m_i, S_i)'\}_{i \in \mathbb{N}}$ and $\mathbf{X}$:

▶ **Individual firm level:**

$$\bar{N}_j^{DB,syst}(T) = \sum_{i=1}^{N^{DB,g}(T)} \mathbb{1}_{\{j \in S_i\}} \sim Poi\Big(\Lambda^{DB,g}(t) \cdot \mathbb{P}(j \in S_i)\Big)$$

$$N_j^{DB,syst}(T) = \sum_{i=1}^{N^{DB,g}(T)} \mathbb{1}_{\{j \in S_i^*\}} \sim Poi\Big(\Lambda^{DB,g}(t) \cdot \mathbb{P}(j \in S_i) \cdot \mathbb{P}(m_i > c_j)\Big)$$

▶ **Portfolio level:**

$$\bar{N}^{DB,syst}(T) = \sum_{i=1}^{N^{DB,g}(T)} |S_i|, \qquad \textit{compound Poisson}$$

$$N^{DB,syst}(T) = \sum_{i=1}^{N^{DB,g}(T)} |S_i^*| \qquad \textit{compound Poisson}$$

Loss Frequency - Incidents from Systemic Events

How to choose assumptions for the distribution of $|S_i|$ and $|S_i^*|$?
(Translation: Which companies in the portfolio might typically be affected jointly?)

- Common vulnerability is often **sector-specific**
  - Distinguish between sector-specific events and general events
  - In either case, assume firms to be affected with equal probability independently from each other

$\rightarrow$ $|S_i|$ and $|S_i^*|$ will follow a **Binomial mixture** distribution

Loss Frequency - Incidents from Systemic Events

How to choose assumptions for the distribution of $|S_i|$ and $|S_i^*|$?
(Translation: Which companies in the portfolio might typically be affected jointly?)

- Common vulnerability is often sector-specific
- ▶ Distinguish between sector-specific events and general events
- ▶ In either case, assume firms to be affected with equal probability independently from each other

$\rightarrow$ $|S_i|$ and $|S_i^*|$ will follow a Binomial mixture distribution

Simultaneous arrivals from systemic events allow the model to capture

- ▶ **lack of independence** between cyber losses in a realistic fashion
- ▶ **overdispersion** of claim counts typically found in empirical data
- ▶ effect of **knowledge about incident / loss** in one firm in the portfolio on incident probabilities in other (similar) firms

Loss Severity

Characteristics of **cyber loss severities**:

- Different types of incidents (DB, FR, BI) differ w.r.t. severity distribution
- Time- and covariate-dependence
- Typically heavy-tailed, body and tail of distribution modelled separately

ERGO Center of Excellence in Insurance

Eine Einrichtung der TUM gefördert von der ERGO Group

Loss Severity

Characteristics of cyber loss severities:

- Different types of incidents (DB, FR, BI) differ w.r.t. severity distribution
- Time- and covariate-dependence
- Typically heavy-tailed, body and tail of distribution modelled separately

▶ Promising approach for all types of incidents (*Eling and Wirfs (2019)*): model cost distribution directly using a **log-normal** distribution for the body and a **GPD** for the tail

Let L_{ij} be the cost of a cyber incident at firm j at time t_i, then assume:

$$(L_{ij} \mid L_{ij} \leq u_{ij}^{\cdot}) \sim TruncLN(\mu_{ij}^{\cdot}, \sigma^{\cdot}, 0, u_{ij}^{\cdot}), \qquad \text{(\textit{cyber incidents of daily life})}$$

$$(L_{ij} \mid L_{ij} > u_{ij}^{\cdot}) \sim GPD(u_{ij}^{\cdot}, \beta_{ij}^{\cdot}, \xi_{ij}^{\cdot}), \qquad \text{(\textit{extreme cyber incidents})}$$

where $TruncLN(\mu, \sigma, x_{\min}, x_{\max})$ denotes a truncated log-normal distribution on the interval $[x_{\min}, x_{\max}]$ and $GPD(u, \beta, \xi)$ denotes a generalized Pareto distribution with location u, scale β, and shape ξ.

Loss Severity

Characteristics of cyber loss severities:

- Different types of incidents (DB, FR, BI) differ w.r.t. severity distribution
- Time- and covariate-dependence
- Typically heavy-tailed, body and tail of distribution modelled separately

▶ Promising approach for all types of incidents (*Eling and Wirfs (2019)*): model cost distribution directly using a log-normal distribution for the body and a GPD for the tail

Let L_{ij} be the cost of a cyber incident at firm j at time t_i, then assume:

$$
\begin{aligned}
(L_{ij} \mid L_{ij} \leq u_{ij}^{\cdot}) &\sim \mathit{TruncLN}\left(\mu_{ij}^{\cdot}, \sigma^{\cdot}, 0, u_{ij}^{\cdot}\right), && \textit{(cyber incidents of daily life)} \\
(L_{ij} \mid L_{ij} > u_{ij}^{\cdot}) &\sim \mathit{GPD}\left(u_{ij}^{\cdot}, \beta_{ij}^{\cdot}, \xi_{ij}^{\cdot}\right), && \textit{(extreme cyber incidents)}
\end{aligned}
$$

where $\mathit{TruncLN}(\mu, \sigma, x_{\text{min}}, x_{\text{max}})$ denotes a truncated log-normal distribution on the interval $[x_{\text{min}}, x_{\text{max}}]$ and $\mathit{GPD}(u, \beta, \xi)$ denotes a generalized Pareto distribution with location u, scale β, and shape ξ.

Alternatives:

- **DB**: Model severity as **number of breached records** using log-normal distribution (*Edwards et al. (2016)*) and **convert into cost** of breach using results by *Jacobs (2014)* or *Farkas et al. (2019)*
- **BI**: Use **PERT** distribution for the body (*Hashemi et al. (2015)*) and GPD for the tail

Agenda

1. Introduction

2. A Holistic View on Cyber Risk

3. Actuarial Model

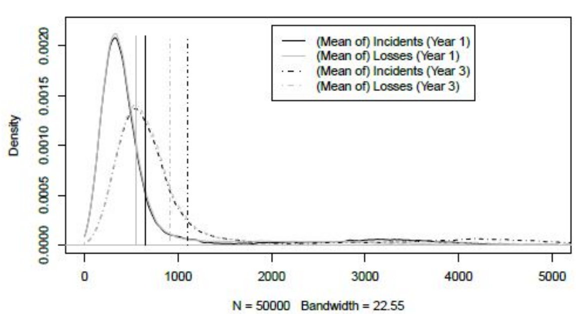
4. Simulation Study

5. Conclusion

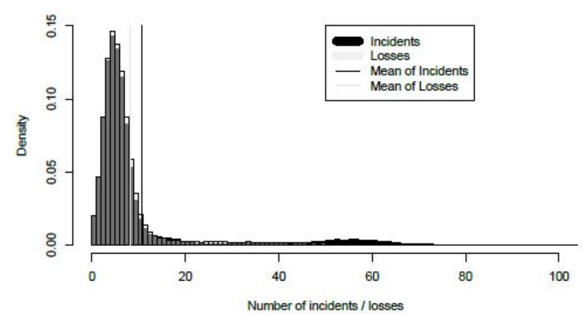
Simulation Study - Setting and Loss Distribution

Simulation setting:

- Fictitious insurance portfolio of $K = 500$ firms from $B = 6$ sectors
- Ten sub-portfolios ($K = 50$) of equal IT security level
- $T = 5$-year observation period, policy duration of one year
- Uniform distribution of systemic events over sectors
- Uniform distribution of event strengths
- Presented results based on 50.000 simulation runs



(a) Density of cumulative loss (whole portfolio).



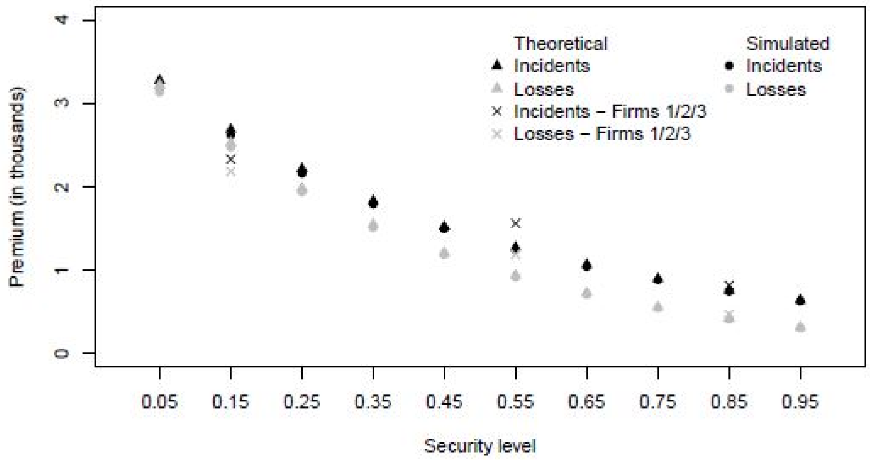
(b) Histogram of incident / loss numbers.

Simulation Study - Results - Premium

- Premiums for three exemplary firms*

Premium based on Expected Value Principle ($\rho = 0.2$) (in thousands)				
	Based on Losses		Based on Incidents	
	Theoretical	Simulated	Theoretical	Simulated
Firm 1	2.1665	2.0814	2.3174	2.2338
Firm 2	0.4610	0.4451	0.8107	0.7746
Firm 3	1.1777	1.1732	1.5557	1.5164

- Premiums according to sub-portfolio losses (equal IT security level)



*Firm 1: Small manufacturing business with low data risk, supplier risk and IT security, Firm 2: Medium-sized financial company with medium data and supplier risk and high IT security, Firm 3: Large health care provider with high data risk, medium supplier risk, and average IT security

Simulation Study - Results - Risk Measurement

Compare $VaR_{0.99}$ and $AVaR_{0.99}$ using the

- Historical estimate

$$\widehat{VaR}_{1-\alpha}(\mathbf{L}) = \hat{F}_L^{-1}(1-\alpha) = L_{(i)},$$
$$\widehat{AVaR}_{1-\alpha}(\mathbf{L}) = \frac{1}{n-i+1}\sum_{j=i}^{n} L_{(j)},$$

where $L_{(1)} < L_{(2)} < \ldots < L_{(n)}$ are the order statistics of a realisation of losses $\mathbf{L} = (L_1, \ldots, L_n)$, $(1-\alpha) \in \left(\frac{i-1}{n}, \frac{i}{n}\right]$, and $\hat{F}$ denotes the empirical c.d.f..

- Peak-over-threshold estimate

$$\widehat{VaR}_{1-\alpha}(\mathbf{L}) = u + \frac{\hat{\beta}}{\hat{\xi}}\left(\left(\frac{\alpha}{\frac{n'}{n}}\right)^{-\hat{\xi}} - 1\right),$$
$$\widehat{AVaR}_{1-\alpha}(\mathbf{L}) = \begin{cases} \frac{\widehat{VaR}_{1-\alpha}+\hat{\beta}-\hat{\xi}u}{1-\hat{\xi}}, & \text{if } \hat{\xi} < 1, \\ \infty, & \text{if } \hat{\xi} \geq 1, \end{cases}$$

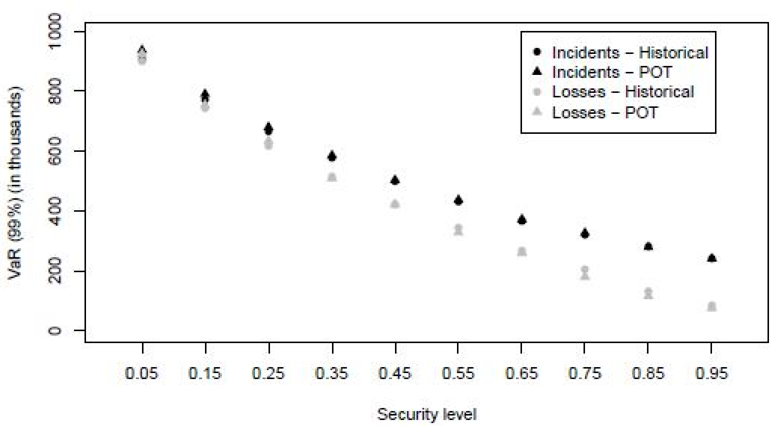
assuming that for a large threshold u, the excesses follow a GPD with parameter estimates $\hat{\beta}$ and $\hat{\xi}$ and n' is the number of threshold exceedances.

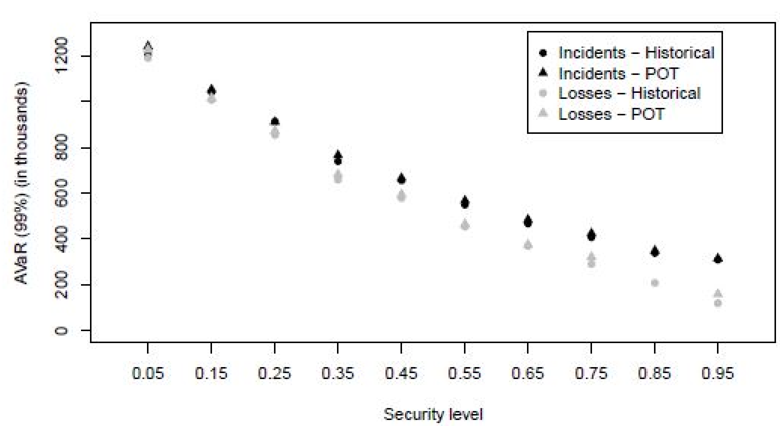
Simulation Study - Results - Risk Measurement

- Risk measures for three exemplary firms and two sub-portfolios

Risk Measures	$VaR_{0.99}$				$AVaR_{0.99}$			
	Losses		Incidents		Losses		Incidents	
	Hist	POT	Hist	POT	Hist	POT	Hist	POT
Firm 1	82.03	63.54	82.61	69.20	90.66	130.04	92.00	135.02
Firm 2	30.15	3.58	33.53	24.19	34.65	30.46	36.81	43.54
Firm 3	54.66	33.04	56.10	47.07	60.48	78.16	62.27	89.30
Portfolio 1	899.81	924.42	906.65	937.77	1189.22	1225.41	1203.32	1239.45
Portfolio 6	344.61	328.84	430.39	436.58	454.74	464.24	548.10	566.73

- Risk measures on sub-portfolio level

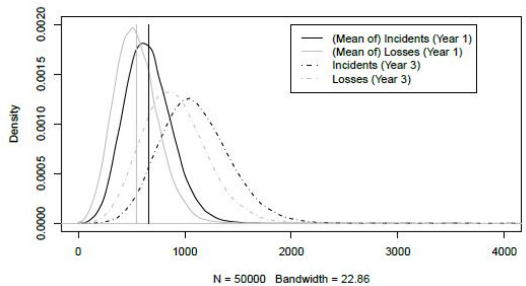




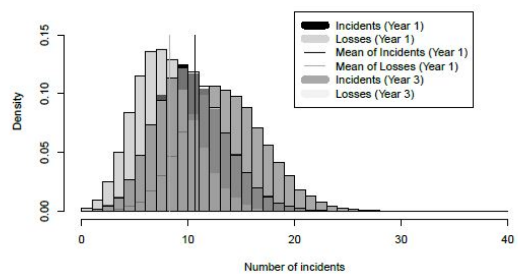
Simulation Study - Results - Accumulation Risk

To emphasize the importance of capturing **accumulation risk**, compare the case with completely independent incidents (same marginal frequency for each company, no systemic events)

- Cumulative loss distribution

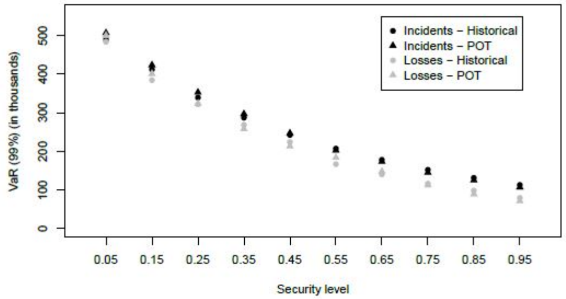


(a) Density of cumulative losses; Independence Case.

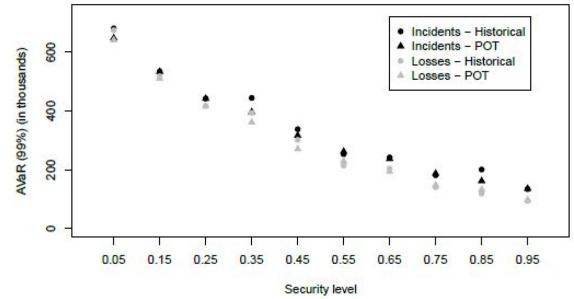


(b) Histogram of incident numbers; Independence Case.

- Risk measures



(a) $VaR_{0.99}$; Independence Case

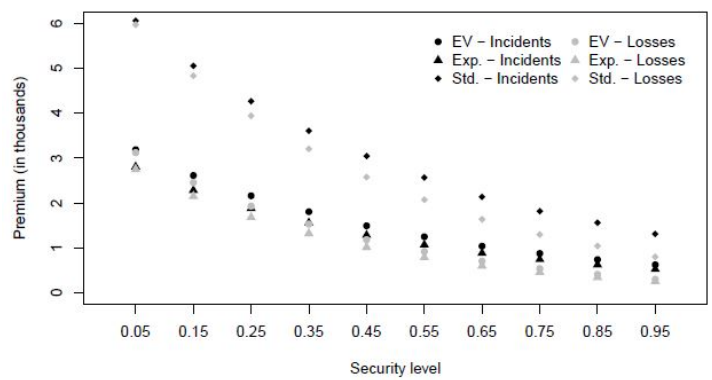


(b) $AVaR_{0.99}$; Independence Case

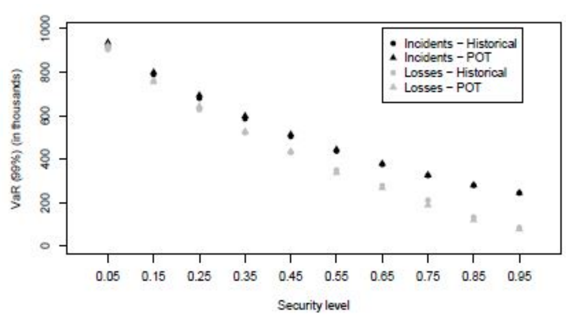
Simulation Study - Results - Cover Limit

To include **realistic policy design** and alleviate effects of extremely heavy-tailed severity distributions, compare to the case with **cover limit** (truncated loss severities)

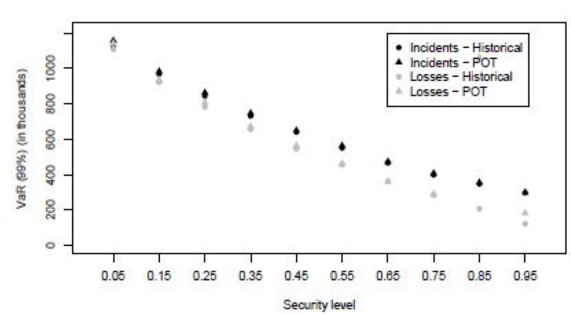
- Premium according to sub-portfolio losses



- Risk measures



(a) $VaR_{0.99}$; Cover Limit $\bar{M}_2$.



(b) $AVaR_{0.99}$; Cover Limit $\bar{M}_2$.

ERGO Center of Excellence in Insurance

Eine Einrichtung der TUM gefördert von der ERGO Group

Agenda

1. Introduction

2. A Holistic View on Cyber Risk

3. Actuarial Model

4. Simulation Study

5. Conclusion

Conclusion

Summary:

- Cyber risk poses many **challenges** to traditional actuarial approaches, one of the most severe concerns for (re-)insurers being interdependence and resulting **accumulation risk**
- The **academic literature offers many vantage points** on the modelling of cyber risk and particularly interdependence, not all of them applicable to real-world portfolios
- In our view, one of the main sources of interdependence are **common vulnerabilities** (e.g. operating systems, cloud service providers), which may not be easy to understand and diversify in a portfolio

Conclusion

Summary:

- Cyber risk poses many challenges to traditional actuarial approaches, one of the most severe concerns for (re-)insurers being interdependence and resulting accumulation risk
- The academic literature offers many vantage points on the modelling of cyber risk and particularly interdependence, not all of them applicable to real-world portfolios
- In our view, one of the main sources of interdependence are common vulnerabilities (e.g. operating systems, cloud service providers), which may not be easy to understand and diversify in a portfolio

Future challenges & chances for academia and practice include:

- Arrangements and standards to facilitate **data / information sharing** to overcome scarcity of (publicly) available, reliable data on cyber incidents and related losses
- **Interdisciplinary research** on properties of cyber risk (mathematical, economic, legal viewpoints) and **continuing cooperations** between academia, industry, and government agencies needed
- **Design of cyber insurance products** that transcend mere risk transfer and promote network resilience, e.g. by including services using knowledge about portfolio interdependence

ERGO Center of Excellence in Insurance

Eine Einrichtung der TUM gefördert von der ERGO Group

Thank you for your attention!

Zeller, Gabriela and Scherer, Matthias, A Comprehensive Model for Cyber Risk based on Marked Point Processes and its Application to Insurance (February 12, 2021).

Available at SSRN: https://ssrn.com/abstract_id=3668228

References

- Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., and Upton, D. *A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate.* Journal of Cybersecurity, 4(1), 2018.
- Biener, C., Eling, M., and Wirfs, J.H. *Insurability of cyber risk: An empirical analysis.* The Geneva Papers on Risk and Insurance - Issues and Practice, 40(1):131-158, 2015.
- Bolot, J. and Lelarge, M. *A new perspective on internet security using insurance.* In IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, p. 1948-1956.
- Edwards, B., Hofmeyr, S., and Forrest, S. *Hype and heavy tails: A closer look at data breaches.* Journal of Cybersecurity, 2(1):3-14, 2016.
- Eling, M. and Wirfs, J.H. *Cyber risk: too big to insure? Risk transfer options for a mercurial risk class*, Volume 59 of IVW-HSG-Schriftenreihe, 2016.
- Eling, M. and Wirfs, J.H. *What are the actual costs of cyber risk events?* European Journal of Operational Research, 272(3):1109-1119, 2019.
- Farkas, S., Lopez, O., and Thomas, M. *Cyber claim analysis through Generalized Pareto Regression Trees with applications to insurance pricing and reserving.*, 2019. `https://hal.archives-ouvertes.fr/hal-02118080`

References

- Fahrenwaldt, M., Weber, S., and Weske, K. *PRICING OF CYBER INSURANCE CONTRACTS IN A NETWORK MODEL.* ASTIN Bulletin, 48(3), 1175-1218, 2018.
- Hashemi, S.J., Ahmed, S., and Khan, F. *Probabilistic modeling of business interruption and reputational losses for process facilities.* Process Safety Progress, 34(4):373-382, 2015.
- Herath, H. and Herath, T. *Copula-based actuarial model for pricing cyber-insurance policies.* Insurance Markets and Companies, 2(1), 2011.
- Jacobs, J. *Analyzing Ponemon cost of data breach.* `https://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/`, 2014.
- Marotta, A., Martinelli, F., Nanni, S., Orlando, A., and Yautsiukhin, A. *Cyber-insurance survey.* Computer Science Review, 24:35-61, 2017.
- Shetty, N., Schwartz, G., Felegyhazi, M., and Walrand, J. *Competitive cyber-insurance and internet security.*, Economics of Information Security and Privacy, volume 5, p. 229-247, 2010.
- The Geneva Association, Eling, M., and Schnell, W. 2016, *Ten Key Questions on Cyber Risk and Cyber Risk Insurance.* `https://www.genevaassociation.org/sites/default/les/research-topics-documenttype/pdf_public/cyber-risk-10_key_questions.pdf`, 2016.
- Xu, M., Schweitzer, K., Bateman, R., and Xu, S. *Modeling and predicting cyber hacking breaches.*, IEEE Transactions on Information Forensics and Security, 13(11):2856–2871, 2018.