A Bonus-Malus Framework for Cyber Risk Insurance and Optimal Cybersecurity Provisioning

Qikun Xiang

Nanyang Technological University (NTU), Singapore

July 5, 2021

Joint work with:

Ariel Neufeld (NTU)

Ido Nevat (TUMCREATE)

Gareth W. Peters (UCSB)

Anwitaman Datta (NTU)

The ever-increasing threat of cyber crimes

- The frequency and severity of cyber attacks have been increasing significantly globally.
- Recently, Cybersecurity Ventures estimated the cost of cyber crimes to rise to 10.5 trillion USD annually by 2025.
- The world economic forum's annual global risk report regularly puts cyber attacks and theft of data in its "Top 5 global risks in terms of likelihood".
- Cyber crime affects a large array of different organisations worldwide:
  - government agencies, financial sectors, important infrastructure units, etc.
- Cyber crime can incur severe damages:
  - business interruption, data breach, reduced reputation, potential loss of life.

Cyber risk insurance

- Many different security solutions have been developed and implemented in order to detect and prevent cyber attacks (i.e. risk reduction/mitigation).
- Despite this, achieving a complete security protection is not feasible. Hence, there is an increasing demand to develop the market for cyber risk insurance (i.e. risk transfer).

$\Rightarrow$ **Risk reduction should be considered in tandem with risk transfer.**

- An organization can enjoy a reduction in the cost of risk transfer as a result of its upfront expenses in risk reduction.
- An insurer can benefit from a contract that encourages good security posture among the insureds.

Cyber risk-based Bonus-Malus framework

- We introduce the **Bonus-Malus system** to cyber risk insurance.
  - Common for automobile insurance.
  - Divide insureds into different levels:
    no claim $\Rightarrow$ low Bonus-Malus level $\Rightarrow$ premium/deductible discounts;
    claim $\Rightarrow$ high Bonus-Malus level $\Rightarrow$ premium/deductible surcharges.
- We analyze the balance between risk reduction and risk transfer via an optimal cybersecurity provisioning process.
- We adopt a realistic compound loss model under the Loss Distributional Approach (LDA) and examine heavy-tailed loss distributions.

Cyber loss model

- We consider:
  - T consecutive years.
  - Random number $N_t \in \mathbb{N}$ of cyber loss events (loss frequency).
  - Random amounts of loss $X_1^{(t)}, \ldots, X_{N_t}^{(t)} \in \mathbb{R}_+$ (loss severity).
  - $D+1$ available risk mitigation measures, with annual expenses $\beta(d) \in \mathbb{R}_+$ and risk mitigation effect $\gamma(d) \in \mathbb{R}_+$ for $d = 0, 1, \ldots, D$ ($\beta(0) = \gamma(0) = 0$).
- The cumulative annual cyber loss in year t

  without risk mitigation measure: $\sum_{k=1}^{N_t} X_k^{(t)}$;

  with risk mitigation measure d: $L_t := \sum_{k=1}^{N_t} \left(X_k^{(t)} - \gamma(d)\right)^+$.

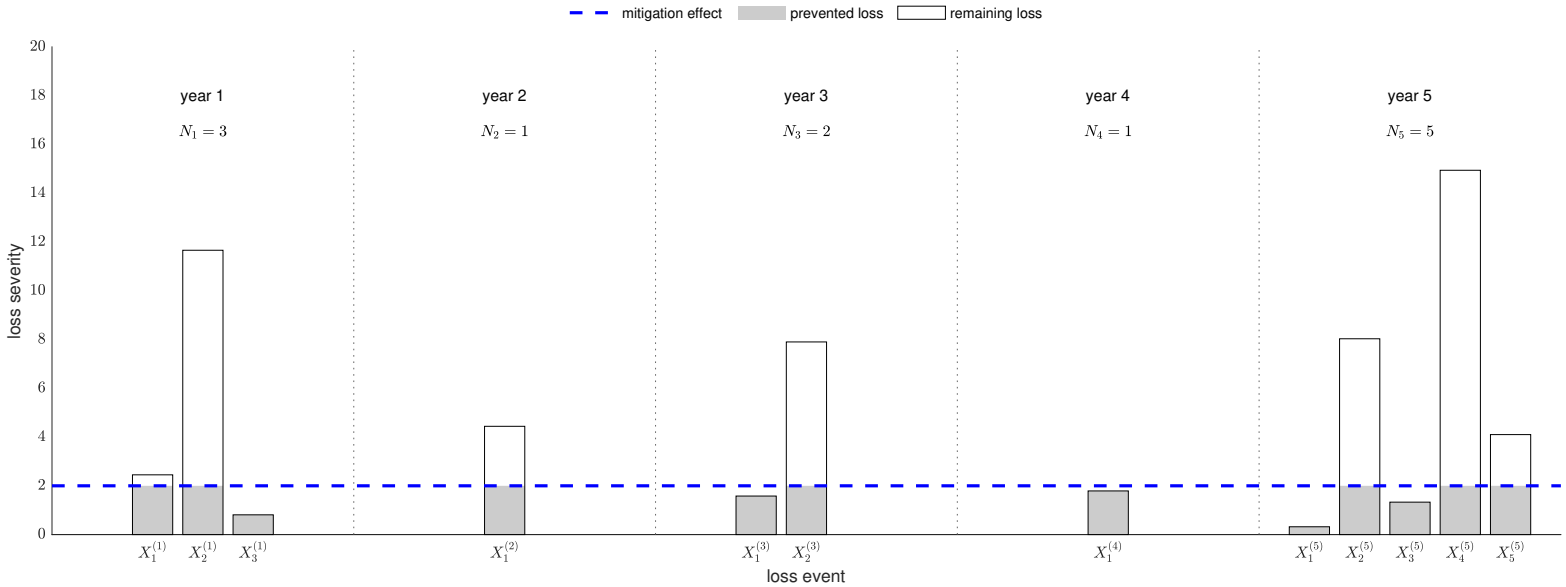
Cyber risk insurance model

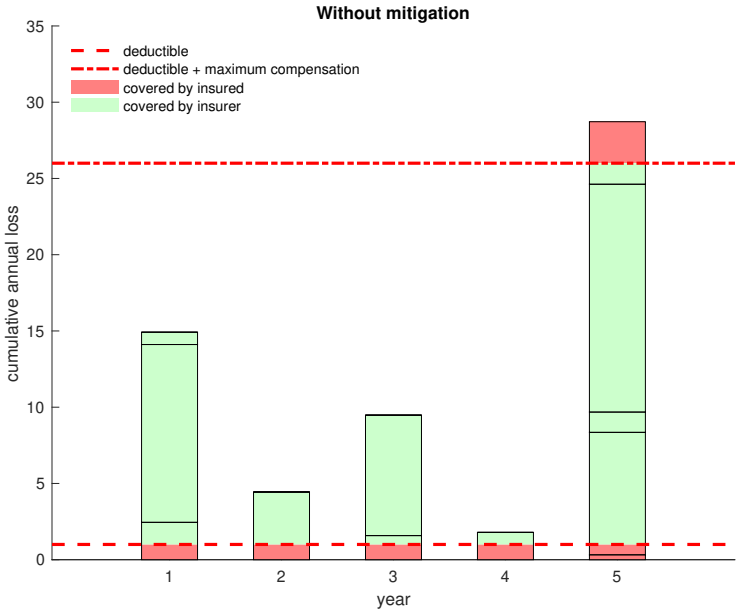
- We consider a **cyber risk insurance** contract that lasts for T years, with a variable annual premium $p^{\mathcal{BM}}$.
- At the beginning of each year, the insured decides whether to:
  - activate/continue the contract,
  - withdraw from the contract $\Rightarrow$ no premium and no insurance coverage.
- For a cumulative annual cyber loss L, if the insured:
  makes a claim $\Rightarrow$ compensation of $(L - I^{\mathcal{BM}}_{\text{dtb}})^+ \wedge I^{\mathcal{BM}}_{\text{max}}$;
  does not make a claim $\Rightarrow$ no compensation.

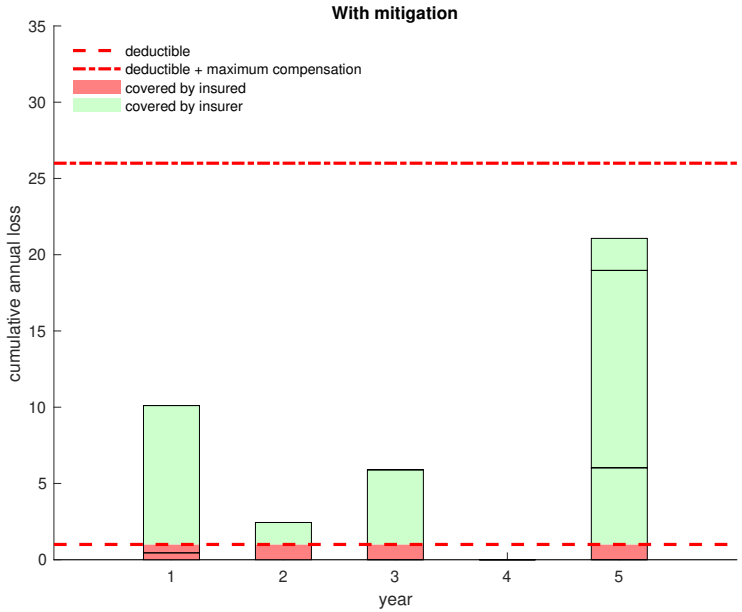
  $I^{\mathcal{BM}}_{\text{dtb}}$ is the deductible,

  $I^{\mathcal{BM}}_{\text{max}}$ is the maximum compensation.

Illustration of the cyber risk insurance model







Bonus-Malus system

- Bonus-Malus levels: $\mathcal{B} := \{-\underline{B}, \ldots, -1, 0, 1, \ldots, \overline{B}\}$.
- $b_0 = 0$, $b_t = \mathcal{BM}(b_{t-1}, C_t)$, where C_t is the amount of insurance claim in year t, $\mathcal{BM} : \mathcal{B} \times \mathbb{R}^+ \to \mathcal{B}$ is the deterministic migration rule.
- The annual premium $p^{\mathcal{BM}}(b_{t-1}, t)$, the deductible $l_{\text{dtb}}^{\mathcal{BM}}(b_{t-1}, t)$, and the maximum compensation $l_{\text{max}}^{\mathcal{BM}}(b_{t-1}, t)$ depend on the Bonus-Malus level and time.

Cybersecurity provisioning process

1. **Provision stage.** At the beginning of each year t, the insured decides:
   - the risk mitigation measure $d_t \in \{0, 1, \ldots, D\}$;
   - whether to continue the cyber risk insurance contract $\iota_t \in \{0, 1\}$ and pay the premium $p^{\mathcal{BM}}(b_{t-1}, t)$.

2. **Operation stage.** Throughout each year t, the random cumulative annual cyber loss $L_t := \sum_{k=1}^{N_t} \left(X_k^{(t)} - \gamma(d_t)\right)^+$ is realized from the compound loss model.

3. **Claim stage.** At the end of each year t,
   - the insured decides whether to make a claim $j_t \in \{0, 1\}$ and receives $C_t := j_t \left[\left(L_t - l_{\text{dtb}}^{\mathcal{BM}}(b_{t-1}, t)\right)^+ \wedge l_{\max}^{\mathcal{BM}}(b_{t-1}, t) \right]$ as compensation;
   - the insured's Bonus-Malus level is updated by $b_t = \mathcal{BM}(b_{t-1}, C_t)$.

Dynamic programming algorithm

- We model the cybersecurity provisioning process as a finite horizon stochastic optimal control problem, where the objective is to minimize the expected value of the discounted total cybersecurity cost including:
  - expenses for adopting risk mitigation measures,
  - premium and various costs of the cyber risk insurance,
  - uncompensated cyber losses.
- The stochastic optimal control problem can be solved efficiently via the **dynamic programming algorithm**.

Cyber loss severity distribution

- We adopt the **g-and-h distribution** (truncated to $\mathbb{R}_+$) introduced by Tukey (1977) as the severity distribution. In g-and-h(α, σ, g, h):
  - $\alpha \in \mathbb{R}$ controls the location;
  - $\sigma > 0$ controls the scale;
  - $g > 0$ controls the skewness; larger g means more positively skewed;
  - $h \geq 0$ controls the tail; the m-th moment exists when $h < \frac{1}{m}$.
- As studied by Dutta and Perry (2006), the g-and-h distribution:
  - allows a wide range of skewness and kurtosis;
  - fits well to real Operational Risk data;
  - produces realistic estimations of the Operational Risk capital.

Cyber loss severity distribution

- We adopt the fast Fourier transform (FFT) approach with exponential tilting to efficiently approximate $\mathbb{P}[L_t \leq l]\ \forall l \in \mathbb{R}_+$ (the distribution function of the cumulative annual cyber loss).
  - See e.g. Embrechts and Frei (2009); Cruz, Peters, and Shevchenko (2015).
  - Subsequently, quantities in the dynamic programming algorithm can be efficiently and accurately approximated.

Numerical experiments

- **Setting**:
  - $T = 20$, discount factor $= 0.95$;
  - $N_t \sim$ Poisson(0.8), $X_k^{(t)} \sim$ Tr-g-and-h($\alpha = 0, \sigma = 1, g = 1.8, h = 0.15$);
  - $D = 1$, $\beta(0) = 0$, $\beta(1) = 0.5$, $\gamma(0) = 0$, $\gamma(1) =$ 70th percentile of $X_k^{(t)}$;
  - $\mathcal{B} = \{-2, -1, 0, 1\}$, let $p_{\text{base}}^{\mathcal{BM}} \in [0, 7]$ be the base premium,

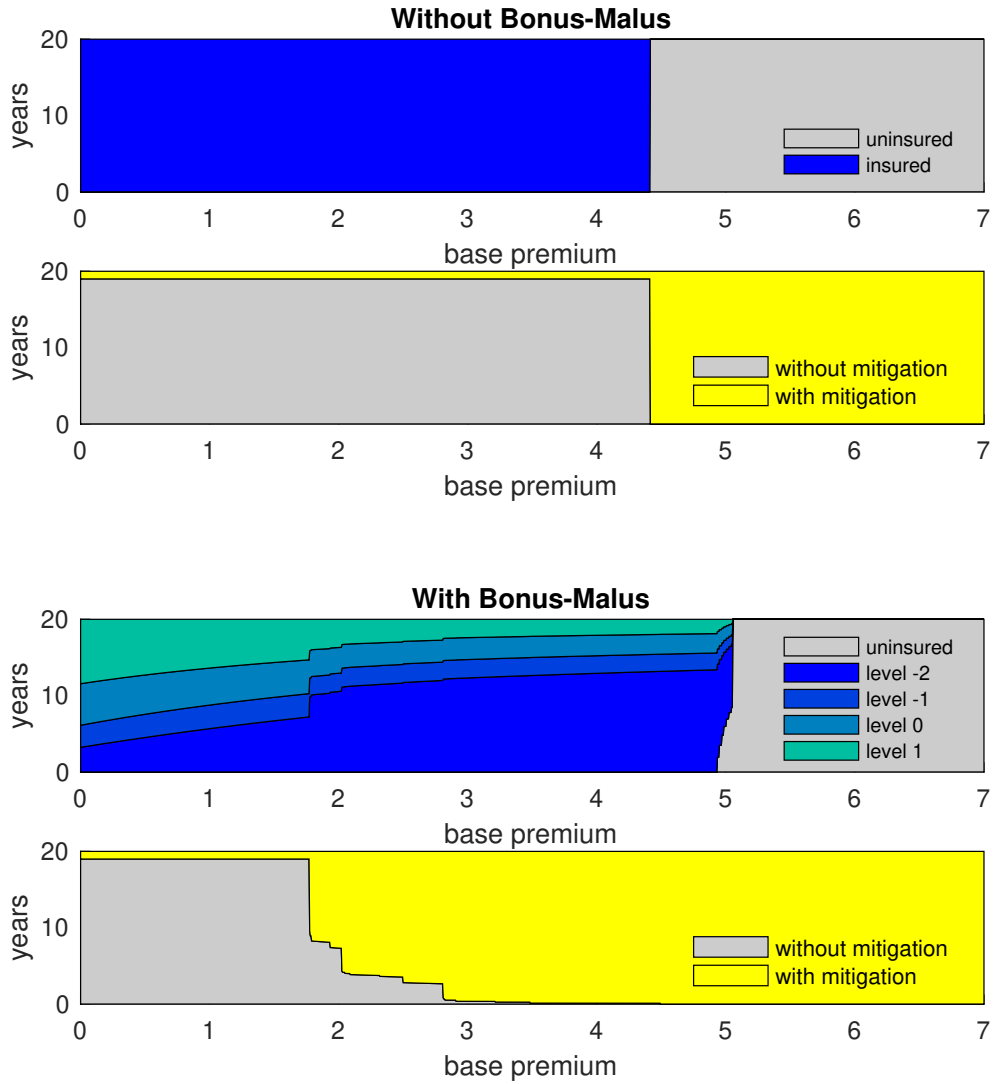
$\mathcal{BM}(b_{t-1}, C_t)$		C_t	
		$= 0$	> 0
b_{t-1}	-2	-2	1
	-1	-2	1
	0	-1	1
	1	0	1

		$p^{\mathcal{BM}}(b, t)$
b	-2	$0.6p_{\text{base}}^{\mathcal{BM}}$
	-1	$0.8p_{\text{base}}^{\mathcal{BM}}$
	0	$p_{\text{base}}^{\mathcal{BM}}$
	1	$1.5p_{\text{base}}^{\mathcal{BM}}$

  - $l_{\text{dtb}}^{\mathcal{BM}}(b, t) = 0.5$ for $t = 1, \ldots, T-1$, $l_{\text{dtb}}^{\mathcal{BM}}(b, T) = 5$ for $b \in \mathcal{B}$;
  - $l_{\text{max}}^{\mathcal{BM}}(b, t) = 1000$ for $t = 1, \ldots, T$, $b \in \mathcal{B}$.

Numerical experiments

The retention of the cyber risk insurance policy and the expected years of adoption of the risk mitigation measure vs. $p_{\text{base}}^{\mathcal{BM}}$:



References

1. Qikun Xiang, Ariel Neufeld, Gareth W. Peters, Ido Nevat, and Anwitaman Datta. **A Bonus-Malus Framework for Cyber Risk Insurance and Optimal Cybersecurity Provisioning.** Preprint, arXiv:2102.05568, 2021.

2. Marcelo G. Cruz, Gareth W. Peters, and Pavel V. Shevchenko. Fundamental aspects of operational risk and insurance analytics: A handbook of operational risk. John Wiley & Sons, 2015.

3. Paul Embrechts and Marco Frei. Panjer recursion versus FFT for compound distributions. Math. Methods Oper. Res., 69(3):497–508, 2009.

4. John W. Tukey. Exploratory data analysis, volume 2. Reading, MA: Addison-Wesley, 1977.