Extreme data breach losses: An alternative approach to estimating probable maximum loss for data breach risk

개인정보 유출 리스크로 인한 최대가능 손실 추정모형

발표자: 정 광 민

포스텍 산업경영공학과 /
드레이크 대학교 경영대학 (겸직)

보험연구원 산학세미나 / 2020년 8월 21일

Market Overview (1 / 2)

Status-quo of the cyber-insurance market

Status-quo

- Market growth: **37%** per annum between 2016 and 2017 (11% over 2019)
- Global premium volume (2018): $ 4.9bn ($ 2,373 bn of total non-life premium globally)
- 80% of the premium volume from the U.S. and the rest from Europe and Asia.
- 528 cyber-insurers in the U.S. in 2018 (6,000 insurers in total in the U.S.)

Korean market

- Market size: ₩ 32.2 bn in 2016 (₩ 84.5 tn of total non-life premium in 2016)
- Coverage is highly limited compared to those in the U.S. market.
- Big players are present in the market (Samsung, KB, Hyundai Marine, DB, AIG, Meritz).

Source: “Cyber Overview”, Munich Re
“sigma 03/2019”, Swiss Re
“Ten key questions on cyber risk and cyber risk insurance”, Eling and Schnell (2017) with Geneva Association
“Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?”, Romanosky et al. (2017)
“전자금융과 금융보안 제 19호”, 금융보안원 (2020)

Market Overview (2 / 2)

Challenges of the cyber-insurance market

Challenges

Demand side	Supply side
1. Lack of understanding of risk 2. Purchasing behavior relative to effect of risk control measures	1. Lack of data 2. Challenge in modeling and pricing 3. Limited coverage (Cover limit)

사이버 보험 시장이 활성화되지 않는 원인

사이버보험 시장이 활성화되지 않는 원인	1순위	2순위	3순위	합계
1) 기업의 실질적인 잠재 리스크는 작아서 보험 수요가 낮음	19.2%	6.1%	7.1%	32.4%
2) 사이버보험에 가입해도 사이버보험이 기업의 니즈를 충족시키지 못함	18.2%	17.2%	20.2%	55.6%
3) 까다로운 가입조건과 가입절차로 인해 가입 니즈를 저해함	1.0%	4.0%	2.0%	7.0%
4) 사이버보험 가입 시 얻는 혜택이 낮아서 보험 수요가 낮음	4.0%	26.3%	9.1%	39.4%
5) 사고발생 시 보장에 대한 확신이 없어서 보험 수요가 낮음	30.3%	14.1%	16.2%	60.6%
6) 가입하고 싶은 사이버보험 상품이 없어서 보험 수요가 낮음	0%	6.1%	7.1%	13.2%
7) 상품 개발에 필요한 전문 인력이 없어서 다양한 상품이 부족함	6.1%	6.1%	13.1%	25.3%
8) 정부의 적극적인 시장 육성 의지가 없음	6.1%	9.1%	14.1%	29.3%
9) 기타	7.1%	1.0%	0%	8.1%
무응답	8.1%	10.1%	11.1%	29.3%

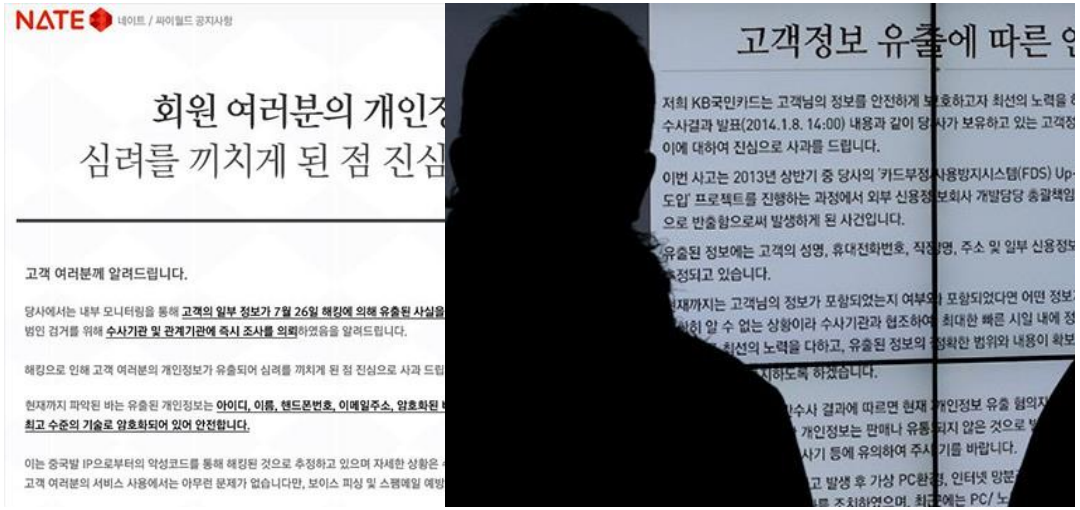
개인정보 배상책임보험 최저가입금액 기준

적용대상 사업자의 가입금액 산정요소		최저가입금액 (최소적립금액)
이용자수	매출액	
100만명 이상	800억원 초과	**10억원**
	50억원 초과 800억원 이하	**5억원**
	5천만원 이상 50억원 이하	**2억원**
10만명 이상 100만명 미만	800억원 초과	**5억원**
	50억원 초과 800억원 이하	**2억원**
	5천만원 이상 50억원 이하	**1억원**
1천명 이상 10만명 미만	800억원 초과	**2억원**
	50억원 초과 800억원 이하	**1억원**
	5천만원 이상 50억원 이하	**5천만원**

Source: “KISA Report 2018 Vol. 6”, KISA (한국인터넷진흥원)
“개인정보 손해배상 보장제도 안내서”, 방송통신위원회 및 한국인터넷진흥원, 2019

Motivation of the Study (1 / 4)

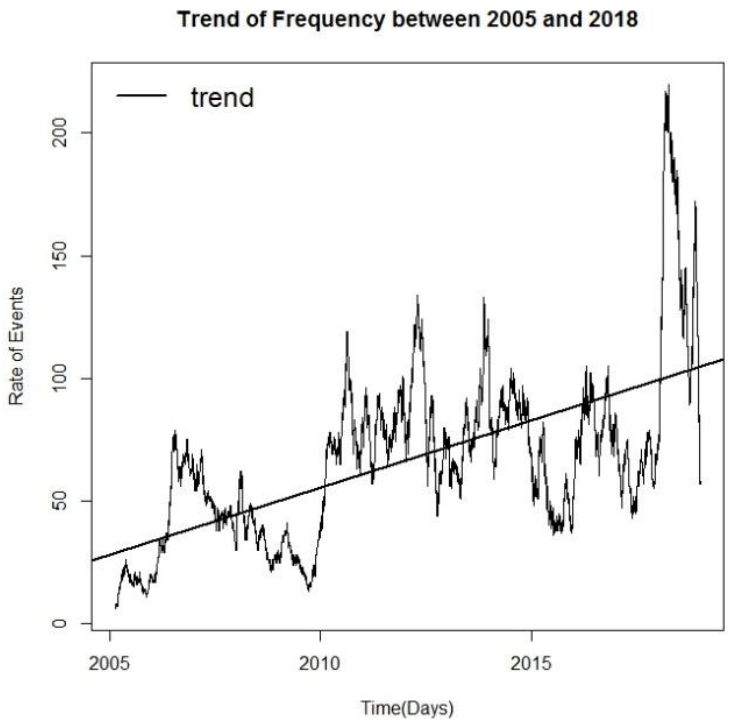
Extreme data breach events



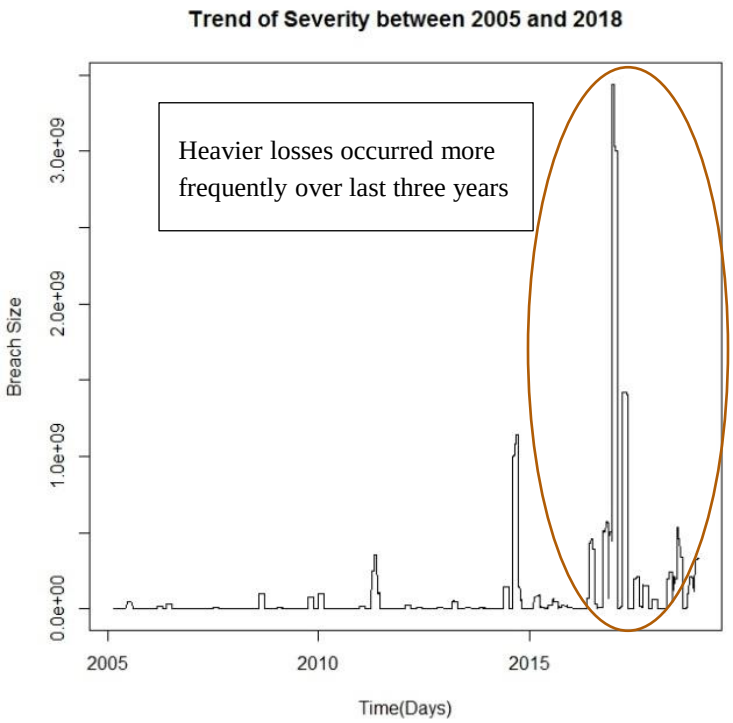
Motivation of the Study (2 / 4)

Trends of data breach loss frequency and severity (2005 – 2018)

Frequency trend



Severity trend



Motivation of the Study (3 / 4)

Literature review on extreme data breach/cyber loss estimation

Probabilistic model: The evaluation of the loss process

	Maillart & Sornette (2010)	Edwards, Hofmeyr & Forrest (2016)	Wheatley, Maillart & Sornette (2016)	Eling & Jung (2018)	Eling & Wirfs (2019)	Hofmann, Wheatley & Sornette (2020)
Data period	2000-2008 (breach loss)	2005-2015 (breach loss)	2007-2015 (breach loss)	2005-2016 (breach loss)	1995-2014 (monetary loss)	2007-2017 (breach loss)
Methodology	Threshold-based (power-law distribution)	Lognormal	Threshold-based (double-truncated Pareto)	Lognormal & threshold-based with dependence modeling	Threshold-based (Pareto distribution)	Threshold-based (truncated Pareto)
Estimate of maximum loss	NA	130 million	300 million	1.1 billion (99.5%)	NA	NA

Dragon king beyond the estimation
(Sornette and Ouillon, 2012)

Motivation of the Study (4 / 4)

List of extreme data breach losses (2005 – 2018)

Date	Breached entity	Risk type	Industry	Breach records (million)
Dec 14, 2016	Yahoo	HACK	Business	3,000.0
Mar 8, 2017	Multiple entities	DISC	Business	1,370.0
Aug 5, 2014	Multiple entities	HACK	Business	1,000.0
Sep 22, 2016	Yahoo	HACK	Business	500.0
Nov 16, 2016	FriendFinder	HACK	Business	412.0
May 31, 2016	MySpace	HACK	Business	360.0
Jul 3, 2018	Exactis	DISC	Business	340.0
Nov 30, 2018	Marriott International	HACK	Business	327.0
Apr 2, 2011	Epsilon	HACK	Business	250.0
Jun 19, 2017	DeepRootAnalytics	DISC	Business	198.0
Dec 28, 2015	Multiple entities	DISC	Business	191.0
Jun 6, 2012	LinkedIn	HACK	Business	167.0
Mar 30, 2018	Under Armour	HACK	Business	150.0
Sep 7, 2017	Equifax	HACK	Financial service	145.5
May 21, 2014	Ebay	HACK	Business	145.0
Jan 20, 2009	Multiple entities	HACK	Financial service	130.0
Jun 27, 2018	NameTests	DISC	Business	120.0
May 17, 2016	LinkedIn	HACK	Business	117.0
Oct 11, 2018	MindBody - FitMetrix	DISC	Business	113.5
Apr 27, 2011	Sony	HACK	Business	101.6

Research Questions & Contributions

Research questions

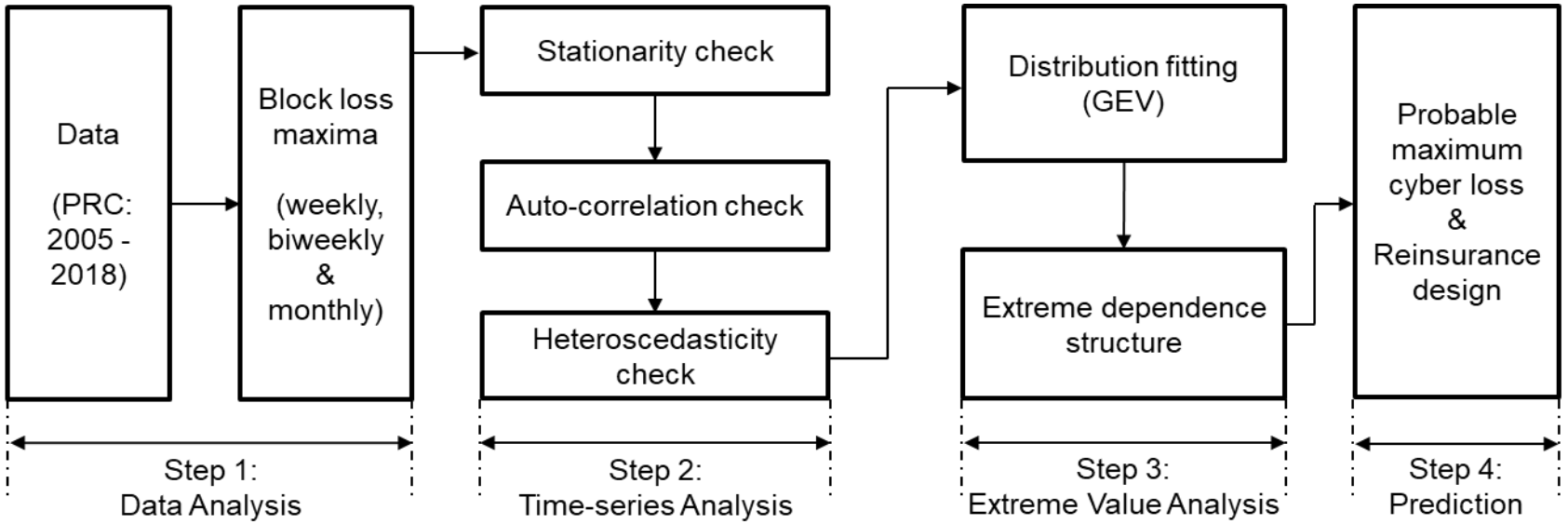
- Can one statistically estimate the size of dragon king by data breach risk?
- If one can estimate the size of dragon king, how can she **apply this to the current insurance market** and what could be a **solution to manage a catastrophe data breach loss**?

Contributions

- An alternative approach to modeling extreme cyber loss
- A definition of probable maximum loss for data breach risk
- An empirical benchmark on reinsurance with public-private partnership (PPP)

Methodology

Overview of modeling



Data: Overview (1 / 2)

Privacy Rights Clearinghouse (PRC)

- Non-profit corporation compiling “chronology of data breaches” in the U.S. from 2005 onwards (9,002 losses as of Jan 31, 2019) -> the largest public database for data breach losses
- Updating day-by-day based on reports from a government agency or verifiable media source
- Date made public, Company, Industry, Breach type, Location and Total breach records.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Date Made Public	Company	City	State	Type of breach	Type of organization	Total Records	Description	Information	Source UR	Year of Breach	Latitude	Longitude
2	21-Oct-09	Bullitt Cour	Shepherds	Kentucky	DISC	EDU	676	A Bullitt	Dataloss DB		2009	37.9884	-85.7158
3	21-Oct-09	Roane Sta	Harriman	Tennessee	PORT	EDU	14,783	Roane	Dataloss DB		2009	35.93396	-84.5524
4	15-Oct-09	Halifax Hea	Daytona B	Florida	PORT	MED	33,000	A laptop	Dataloss DB		2009	29.21082	-81.0228
5	04-Oct-09	Suffolk Co	Selden	New York	DISC	EDU	300	Suffolk	Dataloss DB		2009	40.86649	-73.0357
6	28-Sep-09	Penrose H	Colorado S	Colorado	PHYS	MED	175	Officials at	Dataloss DB		2009	38.83388	-104.821
7	23-Sep-09	Eastern Ke	Richmond	Kentucky	DISC	EDU	5,045	The	Dataloss DB		2009	37.74786	-84.2947
8	22-Sep-09	Bernard M	Dallas	Texas	PORT	BSF	2,246	More than	Dataloss DB		2009	32.80296	-96.7699
9	22-Sep-09	Sagebrush	Bakersfield	California	PHYS	MED	31,000	Thousand	Dataloss DB		2009	35.37329	-119.019
10	21-Sep-09	Rocky Mou	Pinedale	Wyoming	DISC	BSF	1,325	A	Dataloss DB		2009	42.86661	-109.861
11	14-Sep-09	University	Gainesville	Florida	DISC	EDU	25	In August,	Dataloss DB		2009	29.65163	-82.3248
12	14-Sep-09	Jones Gen	Boulder	Colorado	PHYS	BSR	0	Boulder	Dataloss DB		2009	40.01499	-105.271
13	02-Sep-09	Bluegrass	Danville	Kentucky	UNKN	EDU	100	A file	Dataloss DB		2009	37.64563	-84.7722
14	02-Sep-09	Naval Hosp	Pensacola	Florida	PORT	MED	38,000	Naval	Dataloss DB		2009	30.42131	-87.2169
15	21-Aug-09	University	Amherst	Massachu	HACK	EDU	0	Nearly a	Dataloss DB		2009	42.38037	-72.5231
16	15-Aug-09	Northern K	Highland H	Kentucky	PORT	EDU	200	A	Dataloss DB		2009	39.03312	-84.4519
17	14-Aug-09	Calhoun A	Battle Cree	Michigan	DISC	EDU	455	Personal	Dataloss DB		2009	42.32115	-85.1797
18	03-Aug-09	National Fi	Washingto	District Of	DISC	GOV	27,000	An	Media		2009	38.89511	-77.0364
19	22-Jul-09	A Honolulu	Honolulu	Hawaii	INSD	MED	0	In June	Media		2009	21.30694	-157.858
20	14-Jul-09	Canyons S	Cottonwoo	Utah	PORT	EDU	6,000	Canyons	Dataloss DB		2009	40.61967	-111.81
21	14-Jul-09	Leander Si	Leander	Texas	UNKN	EDU	0	School	Media		2009	30.57881	-97.8531
22	09-Jul-09	Mountain M	Salt Lake	Utah	PHYS	MED	0	Names,	Media		2009	40.76078	-111.891
23	08-Jul-09	AT&T	Chicago	Illinois	INSD	BSO	2,100	A	Dataloss DB		2009	41.85003	-87.6501
24	24-Jun-09	Florida Dep	Tallahasse	Florida	PORT	GOV	2,828	The	Dataloss DB		2009	30.43826	-84.2807
25	24-Jun-09	Battle Cree	Battle Cree	Michigan	DISC	GOV	65	Some	Media		2009	42.32115	-85.1797

Data: Overview (2 / 2)

Data in this study

Period: Jan 1st, 2005 – Dec 31st, 2018

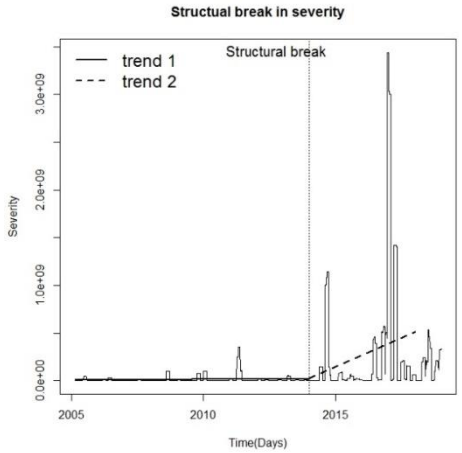
# of obs: 6,780 in total without zero-values

Risk classification (Edwards et al., 2016):

Risk type	Variable	Explanation
Malicious	Hacking (HACK)	Hacking attack by outsiders or infection by malware
	Insider (INSD)	Breached by an insider (e.g., employee or contractor)
	Payment card fraud (CARD)	Fraud involving debit and credit cards
Negligent	Portable device (PORT)	Lost, discarded or stolen portable devices
	Stationary device (STAT)	Lost stationary computers
	Unintended disclosure (DISC)	Privacy information disclosed unintentionally
	Physical loss (PHYS)	Lost, discarded or stolen non-electronic information

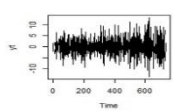
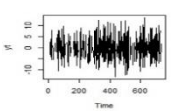
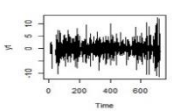
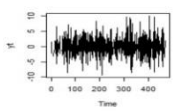
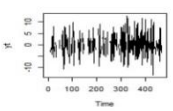
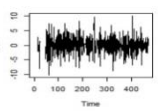
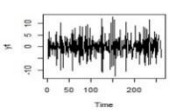
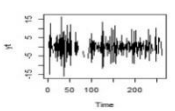
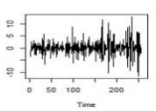
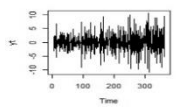
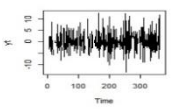
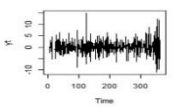
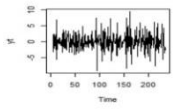
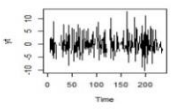
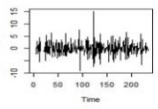
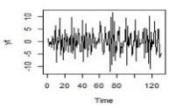
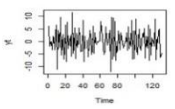
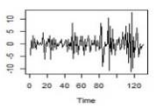
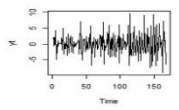
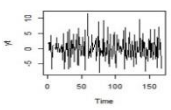
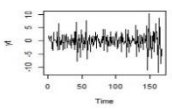
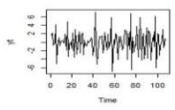
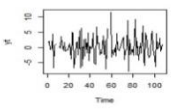
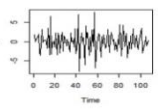
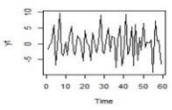
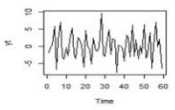
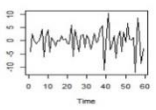
Empirical Estimation (1 / 4)

A break in loss severity



		Test			Trend	
	Structural break	OLS-CUSUM	Rec-CUSUM	Chow	Intercept	Slope
Severity	Jan, 2014	5.890***	3.851***	73.059***	1: -42m 2: -1.9b	1: 3,888 2: 0.1m

Split the dataset into two periods: **pre-2014** and **post-2014**

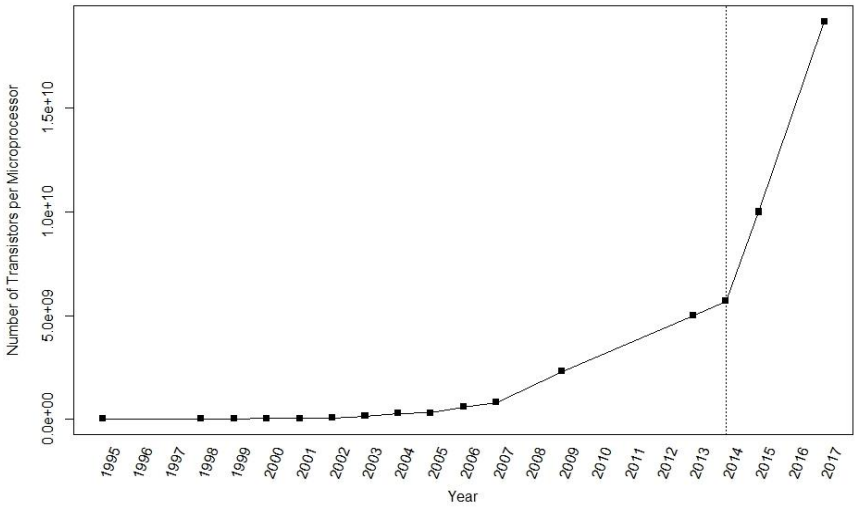
	Entire period			Pre-2014			Post-2014		
	Comp	Mal	Neg	Comp	Mal	Neg	Comp	Mal	Neg
Weekly									
Biweekly									
Monthly									

Empirical Estimation (2 / 4)

A break in loss severity: What could have driven it?

1. State-level acts of data breach notification?
   - Five states have enacted this law since 2014.
   - Borderless businesses in different states, where this law gets more effective.

2. Significant advance in the information technology?
   - 10 out of 15 most extreme loss events from fully online-based corporations since 2014 (62.5% of the total breached records)
   - Moore's law?



Plot to display the Moore's law

→ The y-axis indicates the number of transistors per microprocessor, which shows a clear distinction at the time point of 2014 for the data period since 2005.

Empirical Estimation (3 / 4)

Time series analysis on data breach loss maxima

Testing stationarity

Composite				
		Week	Biweek	Month
Entire	ADF	-8.76***	-4.86***	-4.89***
	PP	-749.85***	-377.90***	-184.09***
	KPSS	0.109	0.105	0.114
Pre-2014	ADF	-7.37***	-5.80***	-4.90***
	PP	-522.13***	-163.37***	-105.20***
	KPSS	0.071	0.067	0.068
Post-2014	ADF	-6.07***	-2.98	-2.74
	PP	-264.88***	-137.82***	-62.39***
	KPSS	0.113	0.111	0.109

H_0: Series contains a unit root
vs.
H_1: Series is stationary

H_0: Series is stationary
vs.
H_1: Series contains a unit root

Testing temporal dependency

Entire period					
Data	Block	Model	AIC	BIC	AICc
Composite	Week	AR(12)	9086.33	9150.65	9086.84
	Biweek	AR(6)	4797.92	4829.14	4798.23
	Month	AR(3)	2328.69	2344.31	2328.94
Malicious	Week	AR(4)	9094.00	9121.57	9094.08
	Biweek	AR(2)	4806.25	4821.86	4806.32
	Month	AR(0)	2336.41	2342.66	2336.44
Negligent	Week	AR(0)	7887.98	7897.17	7887.99
	Biweek	AR(0)	4202.95	4210.76	4202.96
	Month	AR(0)	2060.41	2066.66	2060.44

Testing heteroscedasticity

Entire period					
	Composite			Malicious	
# Lags	Week	Biweek	Month	Week	Biweek
Lag=4	0.712	0.307	0.172	0.685	0.283
Lag=8	0.726	0.656	0.266	0.695	0.488
Lag=12	1.554	1.432	0.329	1.176	0.511
Lag=16	1.578	1.554	0.394	1.186	0.559
Lag=20	1.594	1.574	0.445	1.199	0.580
Lag=24	3.031	1.609	0.483	1.209	0.605

Empirical Estimation (4 / 4)

Fitting GEV distribution

$$G_\gamma(x) = \begin{cases} \exp\left[-(1+\gamma x)^{-\frac{1}{\gamma}}\right], & \gamma \neq 0 \\ \exp[-\exp(-x)], & \gamma = 0 \end{cases}$$

$\Rightarrow$

Type I (Gumbel, $\gamma = 0$): $\exp[-\exp(-x)] \quad -\infty < x < \infty$

Type II (Fréchet, $\gamma > 0$): $\begin{cases} 0 & x \leq 0 \\ \exp\left[-x^{-1/\gamma}\right] & x > 0, \gamma > 0 \end{cases}$

Type III (Weibull, $\gamma < 0$): $\begin{cases} \exp\left[-(-x)^{1/\gamma}\right] & x < 0, \gamma < 0 \\ 1 & x \geq 0 \end{cases}$

where γ is the shape parameter of the extreme distribution.

Panel A: GEV fitting results

		Statistics			Parameter
Data	Block	AIC	K-S	A-D	Shape
Comp	Weekly	19,435.2	0.030	0.802	**2.272**
	Bi-weekly	10,762.7	0.035	0.567	**2.115**
	Monthly	5,464.7	0.058	0.667	**1.661**
Mal	Weekly	16,894.2	0.457***	296.64***	**4.025**
	Bi-weekly	10,182.0	0.103***	7.785***	**3.670**
	Monthly	5,310.7	0.043	0.459	**2.636**

Panel B: Comparison with other distributions (AIC)

Data	Block	GEV	L-norm	Gamma	GPD
Comp	Weekly	**19,435.2**	19,458.9	20,353.8	19,456.8
	Bi-weekly	**10,762.7**	10,814.0	11,229.7	10,784.4
	Monthly	**5,464.7**	5,503.7	5,665.2	5,480.1
Mal	Weekly	16,894.2	16,819.3	17,453.1	**15,665.4**
	Bi-weekly	10,182.0	10,063.5	10,343.0	**9,780.3**
	Monthly	**5,310.7**	5,398.2	5,415.3	5,359.8

Panel C: GPD fitting results for weekly and bi-weekly malicious series

Block (malicious risk)	Loglik	AIC	K-S	Shape
Weekly	-7,830.6	15,665.4	0.000	3.033
Bi-weekly	-4,888.1	9,780.3	0.016	2.971

Panel A: Test for extreme dependency

	Entire period		
	Week	Biweek	**Month**
Pickands test	0.338***	0.027*	**0.025**

Panel B: Bivariate extreme value copulas

Family	Copula	Week	Biweek	Month
Extreme Value	Gumbel-Hougaard	-	-	1.702 (0.192)
	Galam	-	-	1.646 (0.189)
	Tawn	-	-	**1.593 (0.189)**
	Husler-Reiss	-	-	1.617 (0.186)
Elliptical	Gauss	1.733 (0.043**)	1.995 (0.026)	-
	T	3.790 (0.415***)	4.014 (0.040)	-
Archi-mean	Clayton	**-2.410 (0.054**)**	**1.968 (0.027)**	-

Applications (1 / 5)

Probable maximum loss for data breach risk

$$\mathrm{P}\left[\widetilde{M}_n \leq \xi_p\right] = 1 - p,$$

$$\xi_p = G_{\widetilde{M}_n}^{\theta}{}^{-1}(1 - p)$$

for some small $p \in [0,1]$, where $\widetilde{M}_n$ is a series of the cyber loss maxima and ξ_p is the probable maximum loss and $G_{\widetilde{M}_n}^{\theta}$ is the probability function of the cyber loss maxima series with the parameter of θ.

- Quantile-based estimation (Value-at-Risk)
- The loss vector consists of the maximum values at the quantile p

  → a probable worst loss likely to occur p times out of 100 corresponding time units

Applications (2 / 5)

Probable maximum loss for data breach risk

Panel A: PML estimates (million breach)

		Composite	Malicious	Negligent	Dependence
Next 1 yr	Entire Period	61.79	85.22	6.33	142.83
	Pre-2014	8.53	17.18	2.99	26.73
	Post-2014	1,333.90	785.04	18.26	1,347.07
Next 3 yr	Entire period	692.21	1,539.94	52.46	2,241.70
	Pre-2014	50.72	227.04	15.19	284.48
	Post-2014	62,693.28	20,533.20	313.14	33,004.61
Next 5 yr	Entire period	2,053.21	5,987.12	140.76	8,723.67
	Pre-2014	117.62	784.80	32.63	876.31
	Post-2014	371,964.44	98,198.51	1,179.38	132,992.70

Panel B: Estimates of the recent literature (million breach)

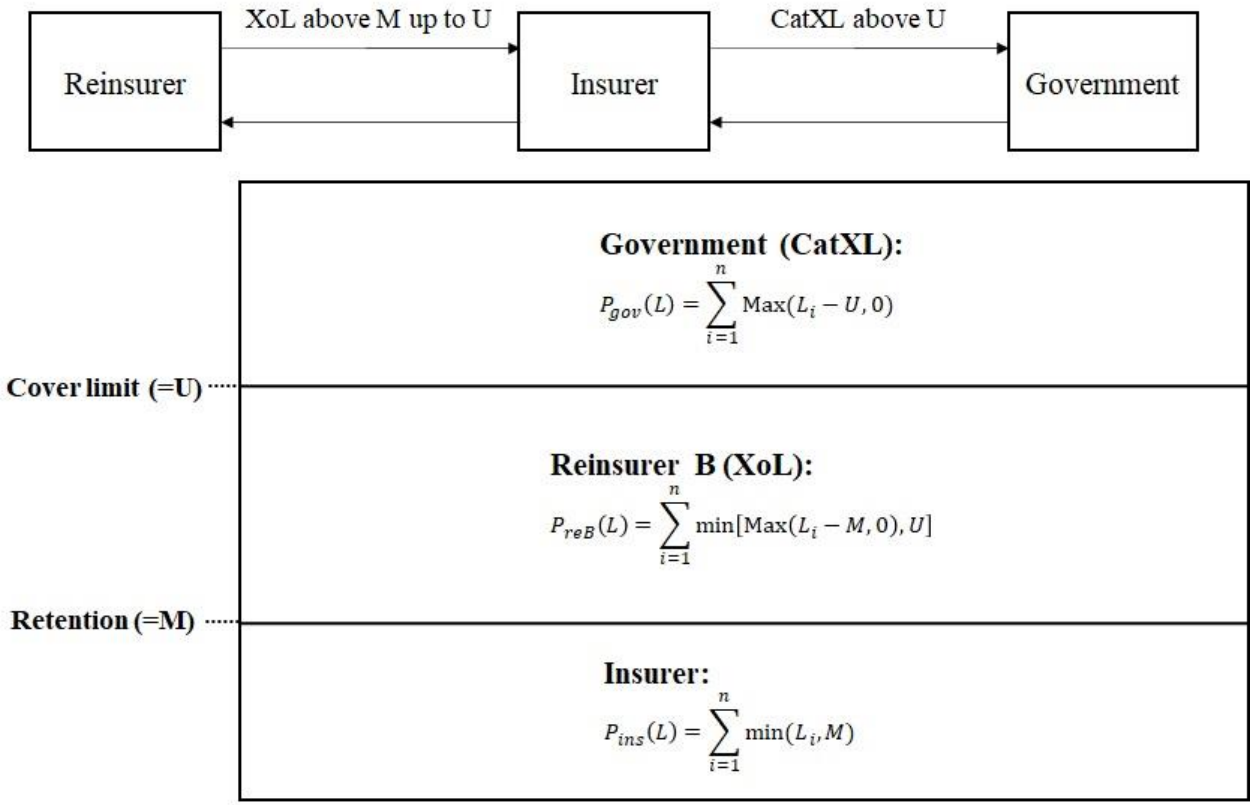
	Edwards et al. (2016) (Lognormal)	Wheatley et al. (2016) (Truncated Pareto)	Eling and Jung (2018) (Correlated risk)
Data period	Jan, 2005 – Feb, 2015	Jan, 2007 – Apr, 2015	Jan, 2005 – Dec, 2016
Data source	PRC	Open Security Foundation & PRC	PRC
Loss estimate	130.00	300.00	1,053.11
Time prediction	Next 3 yr	Next 5 yr	1 out of 200 cases (99.5%)

Panel C: Threshold-based estimation (Pareto density in the tail) (million breach)

		99%	99.5%	99.9%
Entire	Comp	10.81	263.64	1,001.86
	Mal	8.18	382.35	1,407.30
	Neg	0.50	110.21	478.38
Pre-2014	Comp	0.94	29.91	111.47
	Mal	4.24	46.58	149.14
	Neg	1.22	13.87	56.66
Post-2014	Comp	2.43	315.90	1,240.32
	Mal	34.19	524.63	1,761.11
	Neg	0.63	202.33	734.77

Applications (3 / 5)

Reinsurance design with public-private partnership (three-layer program)



Applications (4 / 5)

Reinsurance design with public-private partnership (three-layer program)

- Translation from breach records to monetary loss

Panel A: Descriptive statistics of variables

	N	Mean	Std. Dev.	Q1	Median	Q3
Ln(total loss amount)	295	13.774	2.477	12.172	14.039	15.450
Ln(records)	295	9.011	4.195	5.635	8.491	11.747
Ln(revenue)	295	20.733	3.462	17.791	20.614	23.769
Ln(num of employees)	295	8.338	3.114	5.669	8.868	10.905
Risktype	295	0.942	0.233	1.000	1.000	1.000
Litigation	295	0.708	0.455	0.000	1.000	1.000

Panel B: Results of modeling the relation

	Dependent variable: Ln(total loss amount)				
	Complete set	Size effect		Time break effect	
Variable	Model 1	Model 2-1	Model 2-2	Model 3-1	Model 3-2
Ln(records)	0.2491***	0.3367**	0.2737***	0.2453***	0.2727***
	(0.0333)	(0.1377)	(0.0646)	(0.0438)	(0.0594)
Ln(revenue)	-0.0888	0.1769	0.0255	-0.0771	-0.1083
	(0.1353)	(0.2320)	(0.1815)	(0.1673)	(0.2599)
Ln(num of employees)	0.1986	0.0855	-0.0003	0.1817	0.2055
	(0.1497)	(0.2499)	(0.2044)	(0.1850)	(0.2884)
Risktype	0.3555	0.7923	0.1295	0.3997	-0.2654
	(0.5907)	(0.9255)	(0.7704)	(0.6993)	(1.3022)
Litigation	0.4945	1.2228**	-0.0171	0.7361*	-0.1080
	(0.3308)	(0.5659)	(0.4236)	(0.4094)	(0.6151)
Intercept	11.169***	3.907	9.819***	11.415***	13.392***
	(2.2207)	(3.7827)	(3.2975)	(2.8624)	(3.6852)
Year FE	YES	YES	YES	YES	YES
Industry FE	YES	YES	YES	YES	YES
Obs	295	148	147	203	92
R^2	0.3521	0.4014	0.4060	0.3378	0.4710

Applications (5 / 5)

Reinsurance design with public-private partnership (three-layer program)

$$H(X) = (1 + \delta) \cdot E(X)$$

Panel A: Aggregate annual premium size for the reinsurer and the insurer

	Insurer			Reinsurer		
($ million)	Entire	Pre-2014	Post-2014	Entire	Pre-2014	Post-2014
Malicious event	557.811	359.155	617.910	501.155	108.444	1,836.967
Negligent event	526.667	333.518	614.827	366.959	26.890	1,408.630

Panel B: Loss estimates per cyber event for the government in the next year (above the cover limit)

($ million)	Average loss	Std	90%	95%	99%	99.5%
Malicious event	4.145	11.928	12.769	21.809	49.900	65.502
Negligent event	1.016	4.177	3.077	6.516	15.702	20.175

- If a malicious loss event at the 99.5% confidence level occurs, the government would pay nearly $65.5 million for this event, which is above the cover limit based on the probable maximum loss estimate.
- Lowering vs. raising the cover limit and the effect of the public back-stop on the adjustment of the cover limit.

Sum-up & Implications

Findings and Conclusion

Research questions	Findings
1) Can we estimate the size of cyber dragon king?	✓ Significant **structural break** in severity between pre-2014 and post-2014 ✓ **Short-range temporal dependency** is identified (weekly, bi-weekly) ✓ **Seven times larger** than the one with a widely used Pareto-based model
2) If we can estimate the size of cyber dragon king, how can we apply this to the insurance market and what could be a solution to manage catastrophe cyber loss?	✓ Reinsurance design with the public intervention → **higher cover limit set-up**

Further implications

- **A social discussion** between (re)insurers and responsible government entities is encouraged to agree on the limit level to determine the size of financial backstop by the government.
- **A comprehensive offer** for cyber risk management by insurers with a government's regulation to require a certain level of cyber security (public good) can be another way of the partnership.

Sum-up & Implications

Implications in the Korean market (토의 쟁점)

데이터 3법과 사이버 리스크

- 가명정보의 활용 가능성과 함께 데이터의 활용범위 확대, 활성화로 인해 위험으로의 노출은 커질 것.
- 단, 가명정보의 가치는 매우 낮고, 실제 개인정보로의 결합을 위한 추가정보 유출도 난해.
- DB결합을 위한 전문 기관으로의 해킹, 개인정보 유출 사건들이 증가할 가능성.

Dragon King 손실가능성

- Dragon King 손실이 발생할 가능성:
  1. 상호연결성이 높은 금융사들로의 해킹 발생
  2. 주요 공공/산업 인프라로의 해킹 발생
  3. 시스템 리스크로 인한 손실과 기존 손해보험 보장으로의 영향
  4. 징벌적 손해배상

Thank you for your attention!