4th Industrial Revolution and Cyber Insurance
November 5, 2018, Seoul, Korea

Insurance Business in Transition to the Cyber-Physical Market :

Harmonization, Communication and Coordination of Cyber Risk Matters

W. Jean Kwon, Ph.D., CPCU
Edwin A.G. Manton Chair Professor in Int'l Insurance & Risk Management
The School of Risk Management
St. John's University, New York

Web: Facpub.StJohns.edu/~KwonW/

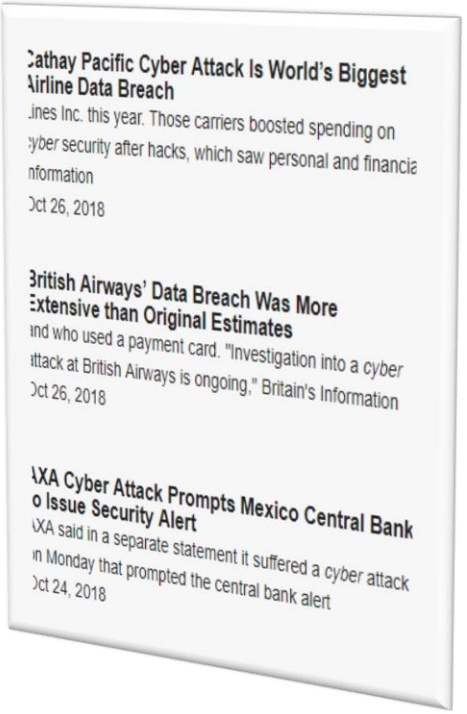
Email: KwonW@stjohns.edu

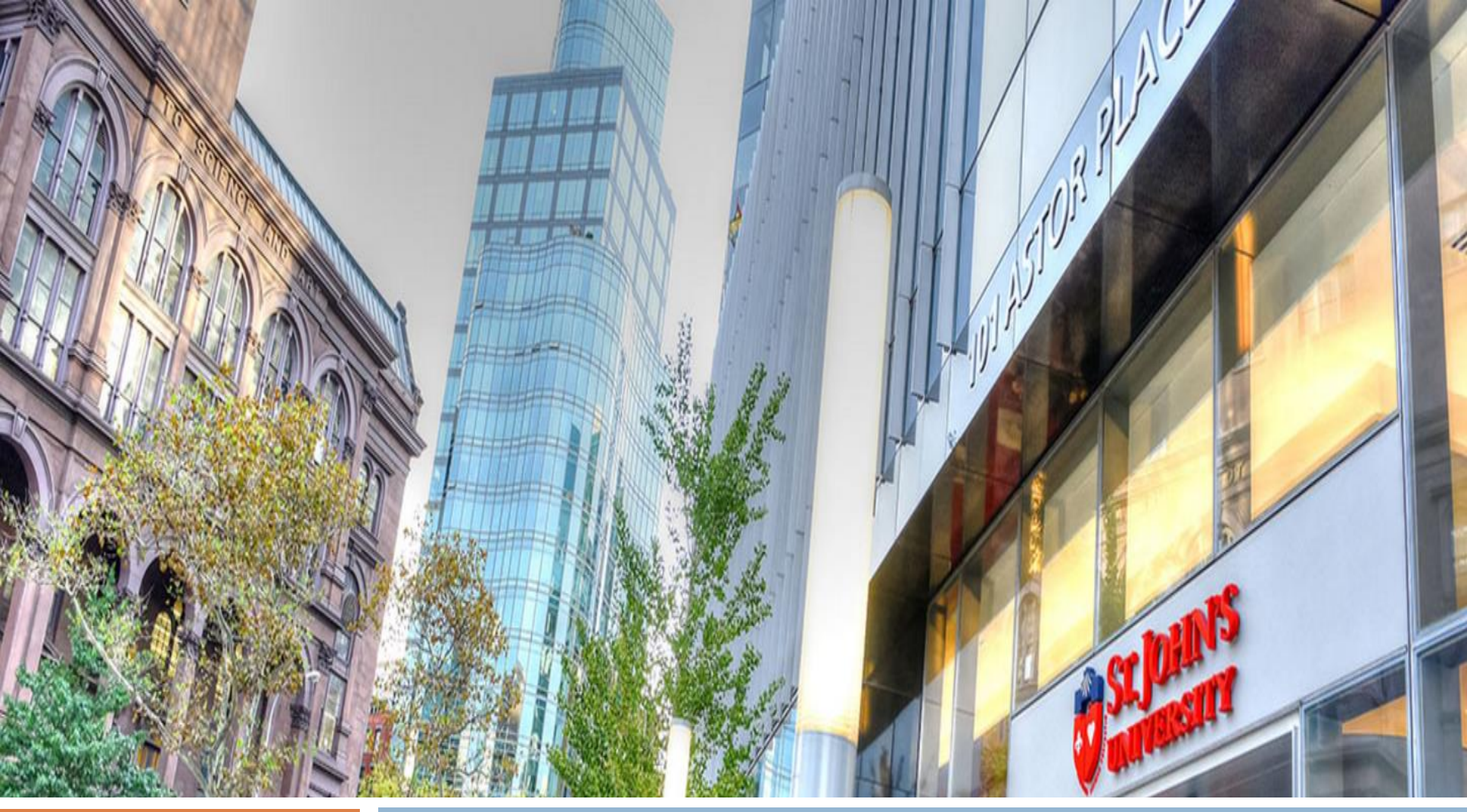
kiri 보험연구원
Korea Insurance Research Institute

Study Abstract

Full Report at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3201875

- Investigation of the business of insurance from a loss exposure and coverage development perspectives, data and privacy protection regulation, and the structure of cyber risk coverages
- The efforts of professionals inadequately coordinated, and each industry with its own cyber risk management language
- The multiplicity-in-cause, multiplicity-in-outcome nature of the risks in cyberspace warrants examination of the properness of cyber insurance market structures, let alone meaningful standardization of coverages

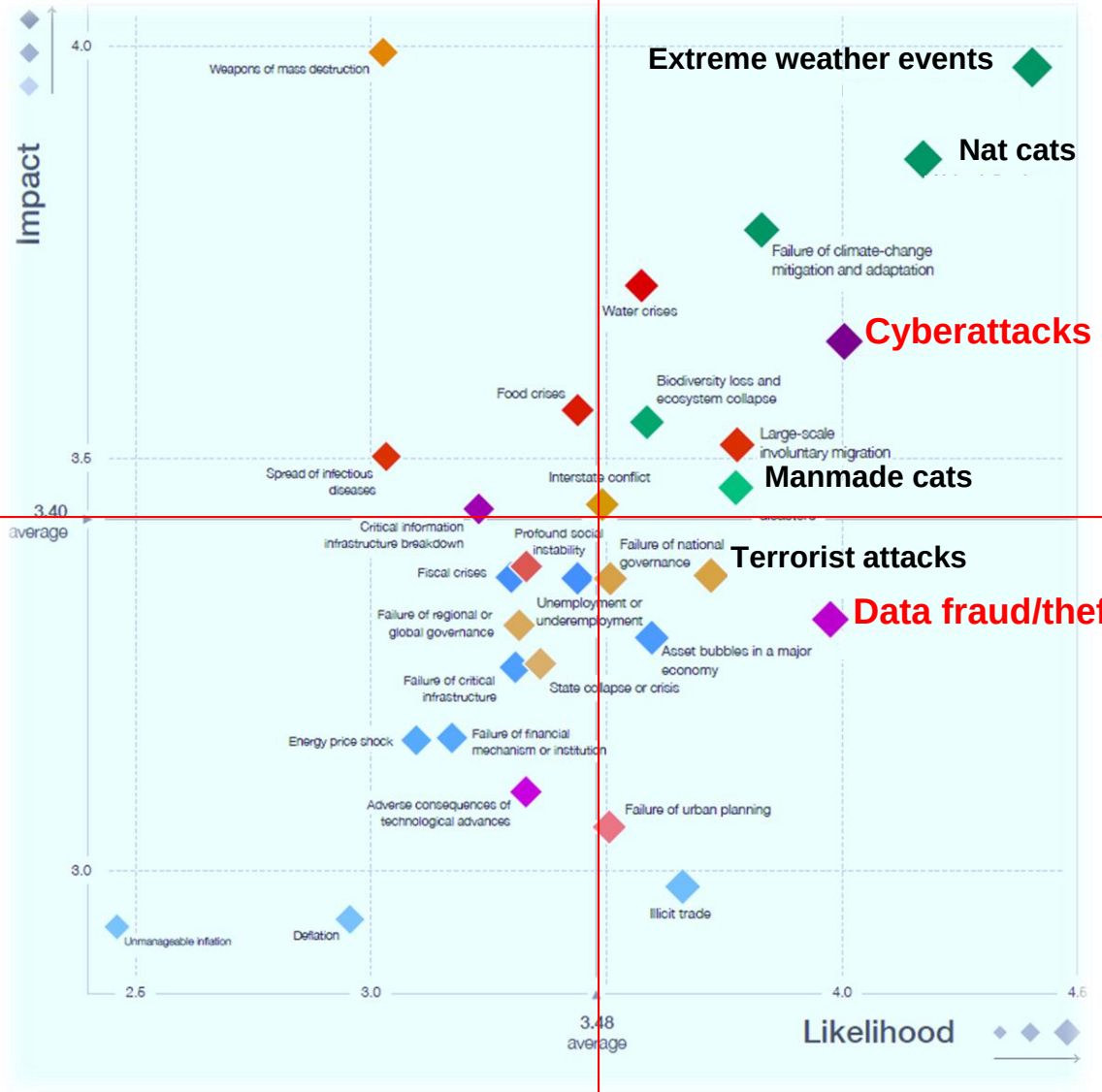




The World of Risk

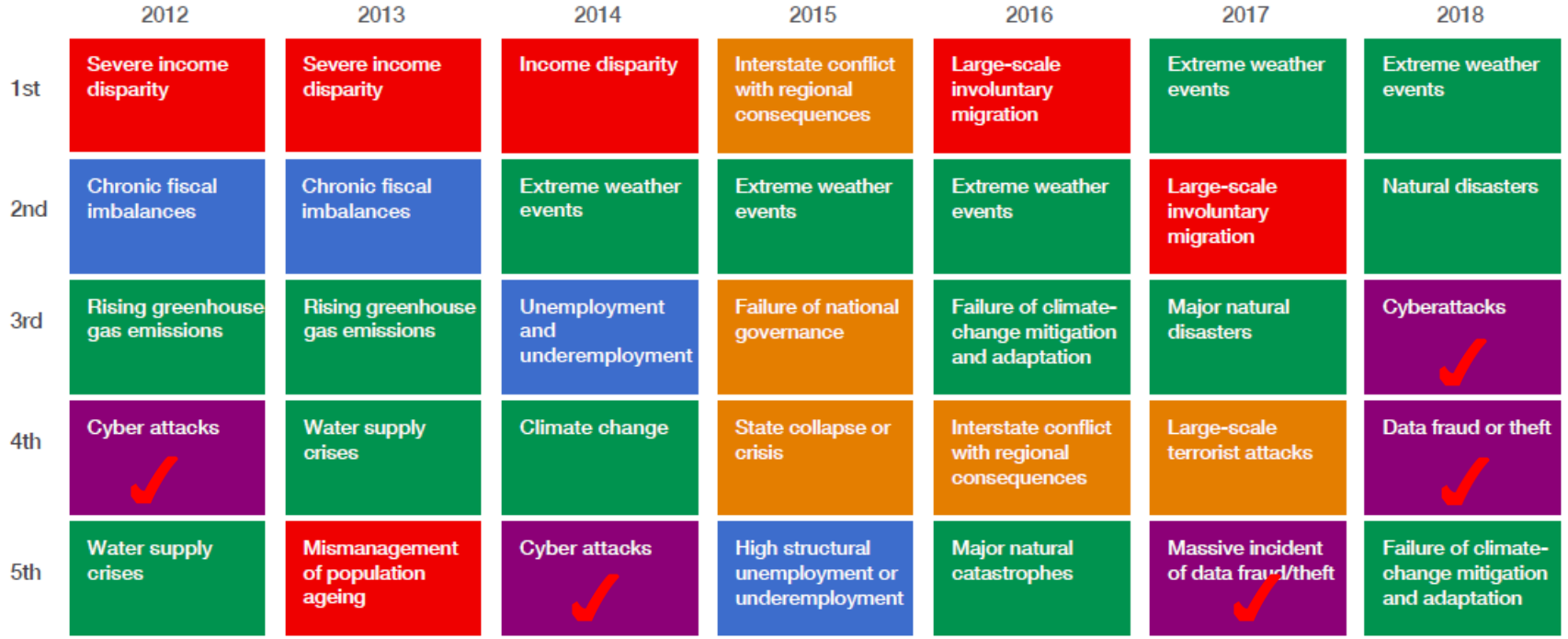
Global Risk Landscape 2018

World Economic Forum



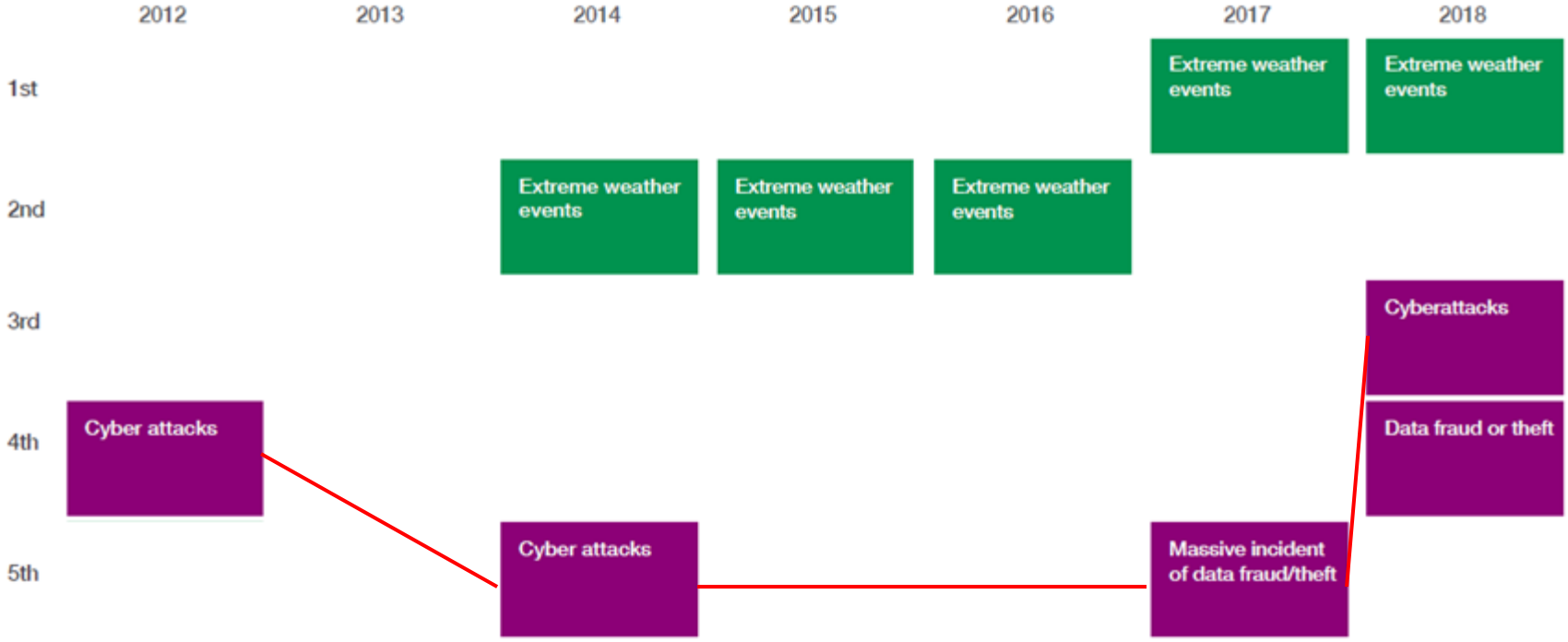
WEF Top 10 Global Risks

(2012-2018) (Likelihood Only)



World Economic Forum

WEF Top 10 Global Risks (2012-2018) (Likelihood Only)



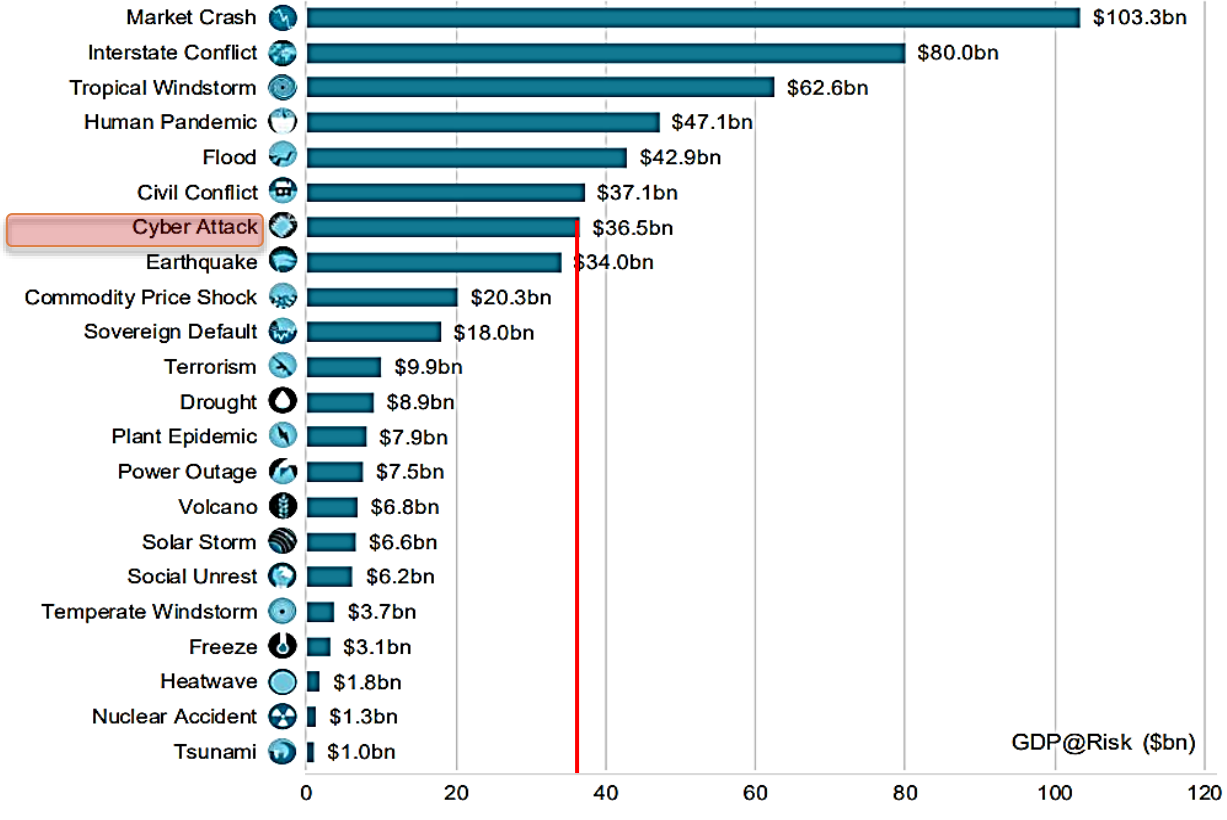
World Economic Forum

WEF Top 10 Global Risks
(2010 – 2018)

Year	Likelihood		Impact	
	Top-ranked	Cyber Risk	Top-ranked	Cyber Risk
2018	Extreme weather events	3	Weapons of mass destruction	6
2017	Extreme weather events	5	Weapons of mass destruction	--
2016	Large-scale involuntary migration	--	Failure of climate-change mitigation	--
2015	Interstate conflict	10	Water crisis	--
2014	Severe income disparity	5	Climate change	--*
2013	Severe income disparity	--*	Financial failure	--*
2012	Severe income disparity	--*	Financial failure	--*
2011	Climate change	4	Extreme energy price volatility	--*
2010	Asset price collapse	--*	Asset price collapse	--*

World Economic Forum
* Only top 5 ranked

Lloyd's Global Risk Outlook 2018



The aggregate impact of these 22 global risks likely yields 41% of global GDP.

Cyber risk contributes 7% (or $36.5 billion) of the aggregate impact.

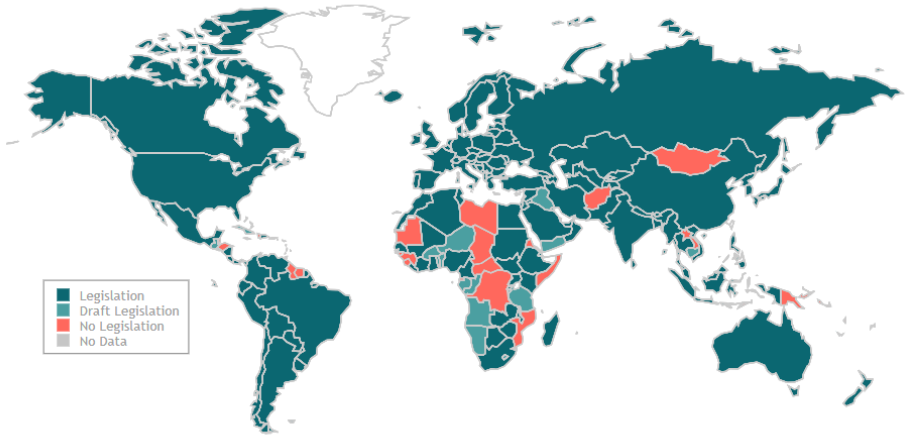
Critical protection gap issue exists, with a consumption rate of 3% or less (in the U.S.)*

* Estimate

Data Protection and Privacy Laws

Emphasis on Security in Business Transactions and Consumer Protection

72%	9%	18%	1%
COUNTRIES WITH **LEGISLATION**	COUNTRIES WITH **DRAFT LEGISLATION**	COUNTRIES WITH **NO LEGISLATION**	COUNTRIES WITH **NO DATA**



UNCTAD Global Cyberlaw Tracker (April 2018); Accessed (October 2018)

Regulation focuses on prevention and protection of data and privacy right

This survey does not examine the quality of laws and regulations.

Data Protection and Privacy Laws

Selected Countries

CHINA

Electronic Transactions:
Legislation

Consumer Protection:
Legislation

Privacy and Data Protection:
Legislation

Cybercrime:
Legislation

KOREA, REPUBLIC OF

Electronic Transactions:
Legislation

Consumer Protection:
Legislation

Privacy and Data Protection:
Legislation

Cybercrime:
Legislation

JAPAN

Electronic Transactions:
Legislation

Consumer Protection:
No Data ✓

Privacy and Data Protection:
Legislation

Cybercrime:
Legislation

USA

Electronic Transactions:
Legislation

Consumer Protection:
Legislation

Privacy and Data Protection:
Legislation

Cybercrime:
Legislation

RUSSIA

Electronic Transactions:
Legislation

Consumer Protection:
No Data ✓

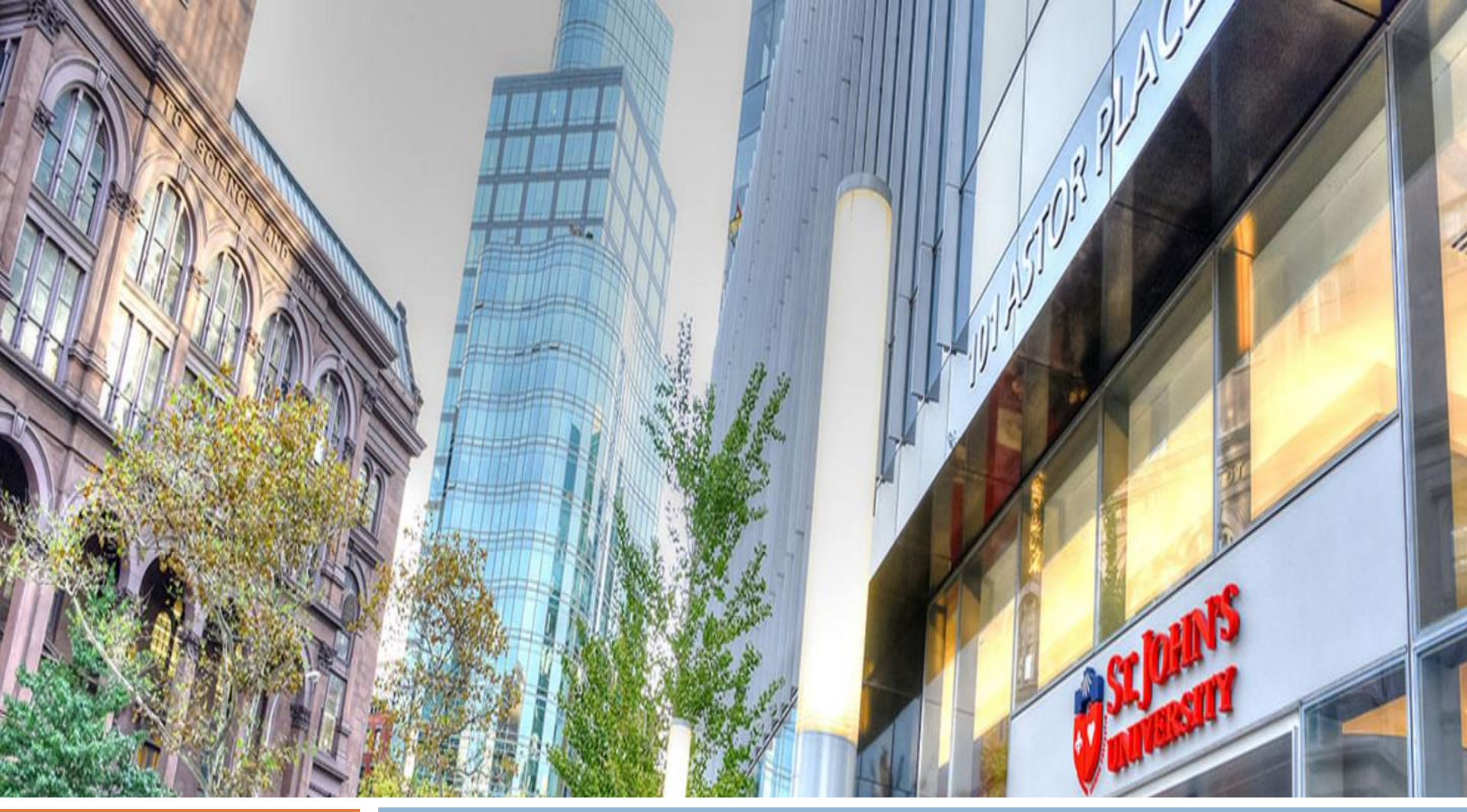
Privacy and Data Protection:
Legislation

Cybercrime:
Legislation

Data Protection Regulation: the EU and the US

- EU General Data Protection Regulation (GDPR, EU 2016/679)
  - In place from May 2018
  - Penalty for non-compliance
  - Fines up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year, whichever is greater.
- The EU has proposed the ePrivacy Regulation.

- US New York Department of Financial Services - Cybersecurity Rule (2/2017)
  - Risk-based minimum standards for technology systems and for addressing cyber breaches
  - Mandatory cyber incident reporting
  - Accountability
    - Including third party vendors



Cyber Risk(s)

Cyber Risk: Traits

- Commonly affect individual units in the economy – Targeted or random

- Potential catastrophic losses, affecting a group of units in the economy that are
  - Related as in a chain of service
  - Random

- Threat caused by
  - A third party (hackers)
  - An internal person and other persons with access authority

Cyber Terrorism Risk

Act of War

Economic Cost of Cyber Breaches

Romanosky (2016) Using Advisen Data

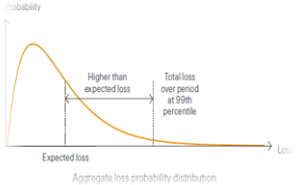
Event type	No. of events	Mean cost (USD mn)	Median cost (USD mn)	Maximum cost (USD mn)
Data breach(1)	602	5.87	0.17	572
Compromised systems(2)	36	9.17	0.33	100
Privacy violation(3)	234	10.14	1.34	750
Illicit access(4)	49	19.99	0.15	710
Total	**921**	**7.84**	**0.25**	**750**

(1) Unintentional disclosure of personally identifiable information (PII) stemming from loss or theft (eg, theft of computers containing personal information of employees or customers, by a hacker or malicious employee).
(2) Compromise or disruption of corporate IT systems or intellectual property (eg, a denial-of- service attack, theft, malicious infiltration and subsequent cyber extortion).
(3) Unauthorised collection, use and/or sharing of PII. Unlike (1) and (2), which refer to incidents "suffered by" a firm, this category relates to events "caused by" a firm (eg, a firm improperly collecting or selling PII).
(4) Computer or electronic crimes directly against other individuals or firms including phishing attacks, identity theft, or skimming attacks.

All data in a 10-year period from 2005 to 2014 for a sample of incidents where cost estimates are publicly available.

Romanosky (2016) and further refined by Swiss Re (2017).

Cyber Risk Modelling Issues



- Data issues
  - Limited and unstructured data about actual and potential losses
  - Ambiguity about the underlying risk drivers
  - Human/hacker behavior
- Inconsistency in survey findings
  - Across surveys
  - Over multiple periods by the same survey organization

Swiss Re (2017)

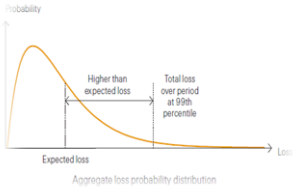
Findings from Selected Surveys of Risk Bearers

Surveyor and Year	Survey Title / Main Target Groups	Key Findings
General		
Castelli et al. (2018)	PwC Global State of Information Security Survey 2018 (9,500 executives in 122 countries)	• 44% of the respondents do not have an overall information security strategies • 48% have no employee security awareness program • 54% are without an incident response process • 39% are very confident in their attribution capabilities
Lloyd's (2017)	Lloyd's Survey 2016 (350 business leaders in Europe)	• CEO fraud result in significant financial losses in the target companies • Organized cybercrime targeted financial services companies; retail industry firms are increasingly targeted • Professional service firms are used as a gateway to attack their clients • Ransomware and DDoS attacks are increasingly used to against organizations in healthcare, media and entertainment services • Public sector entities and telecommunications industry firms are susceptible to espionage-focused cyber-attacks
Verizon (2008, 2012, 2017 and 2018)[a]	Data Breach Investigations Report (annual)	• Perpetration by outsiders contributed 73% of all cases (inclusive of 12% by nation-state (affiliated) actors) in 2017, 75% in 2016, 98% in 2011 and 73% in 2007
Deloitte-NASCIO (2016)	Cybersecurity Study 2016 (a survey of U.S. states)	• 45% of governors receive monthly cybersecurity reports, 16% quarterly and 6% annually • Cybersecurity is part of government operations. Top three cybersecurity initiatives in 2016 are: training & awareness: monitoring security operations centers; and strategy. • 54% have implemented at least some of the cybersecurity recommendations by the National Governors Association
The Economist (2014)	Cyber Incidence Report 2014	• 29% said most common incidents are not hacking but accidental major systems outrages • 27% experienced loss of sensitive data by employees.

Findings from Selected Surveys of Risk Bearers

Surveyor and Year	Survey Title / Main Target Groups	Key Findings
Insurance-related		
Marsh & McLennan and Microsoft (2018)	2017 Global Cyber Risk Perception Survey (1,312 respondents globally)	• Two-thirds of respondents ranked cybersecurity as a top five risk management priority, but only 19% are highly confident in managing the risk and 30% already have a plan • As firms become larger in terms of revenue, the more likely the IT department becoming the primary owner and decision-maker for cyber risk management • 75% identified business interruption as a critical potential financial impact, but less than 50% actually estimated financial losses • One fifth did not have or plan to purchase cyber insurance, and 25% did not know their cyber insurance status
Aon	2015 Global Risk Management Survey (125 Aon client companies)	• Business interruption, both during a breach and post-breach, rated as the top cyber risk concern • 59% of the companies used a formal risk assessment process • 68% of the companies bought cyber insurance for balance sheet protection • 95% of the companies stated clear policy wording as the most important issue in the cyber [insurance] market, and 75% of large companies concerned about the loss adjustment process
Marsh & McLennan (2016a)	UK Cyber Risk Survey Report 2016	• 30.3% of the respondents have board-level oversight of cyber risk. • 75% do not have a complete understanding of cyber risk. • 55.9% are engaged in the cyber insurance market
Marsh & McLennan (2016b)	2015/2016 Cyber & Data Security Risk Survey Report for SMEs	• 41% of the respondents have implemented data security insurance coverage. • 52% do not have a corporate recovery plan for the loss of confidential, personally identifiable information (PII). • 40% have no loss migration capability. • 46% of the respondents seldom discussing cybersecurity do not have loss migration techniques.
NetDiligence (2016)[a]	Cyber Claims Study 2016	• Of insurance claims submitted, 30% had insider involvement (comprising around 77% as the result of "unintentional" caused by employee errors and 22% malicious in nature)

Cyber Risk Modelling Issues



- Modeling issues
  - Generally, attempt to create a single model for causes and outcomes
  - Again, based on limited data and/or in simulated environment
- Similar observations in cyber insurance coverages

Cyber Insurance Pricing Issues

Insurer's Cost of Data Breach

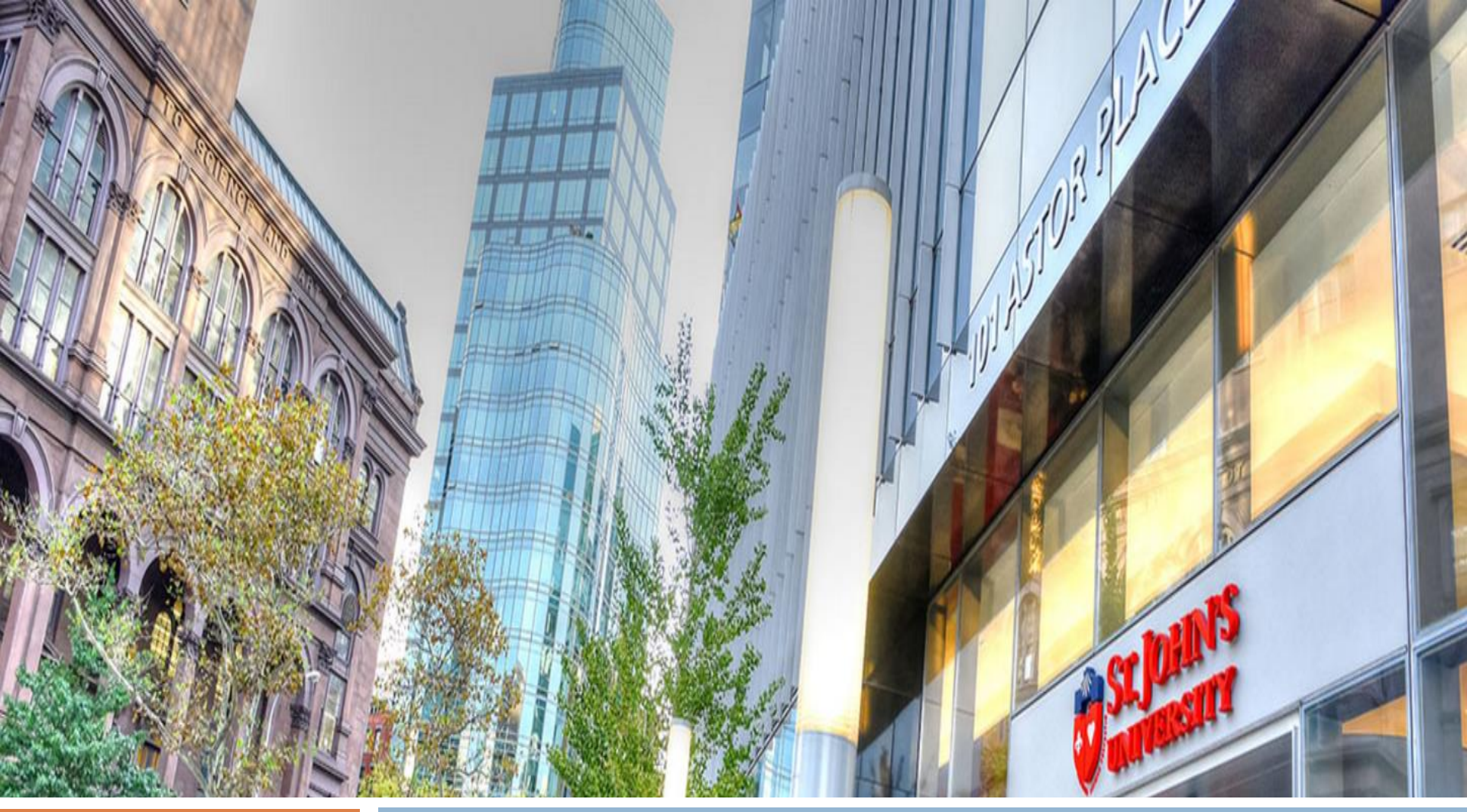
Above the Surface:
Well-known cyber incident costs

1. Customer breach notifications
2. Post-breach customer protection
3. Regulatory compliance (fines)
4. Public relations/crisis communications
5. Attorney fees and litigation
6. Cybersecurity improvements
7. Technical investigations

Beneath the Surface:
Hidden or less visible costs

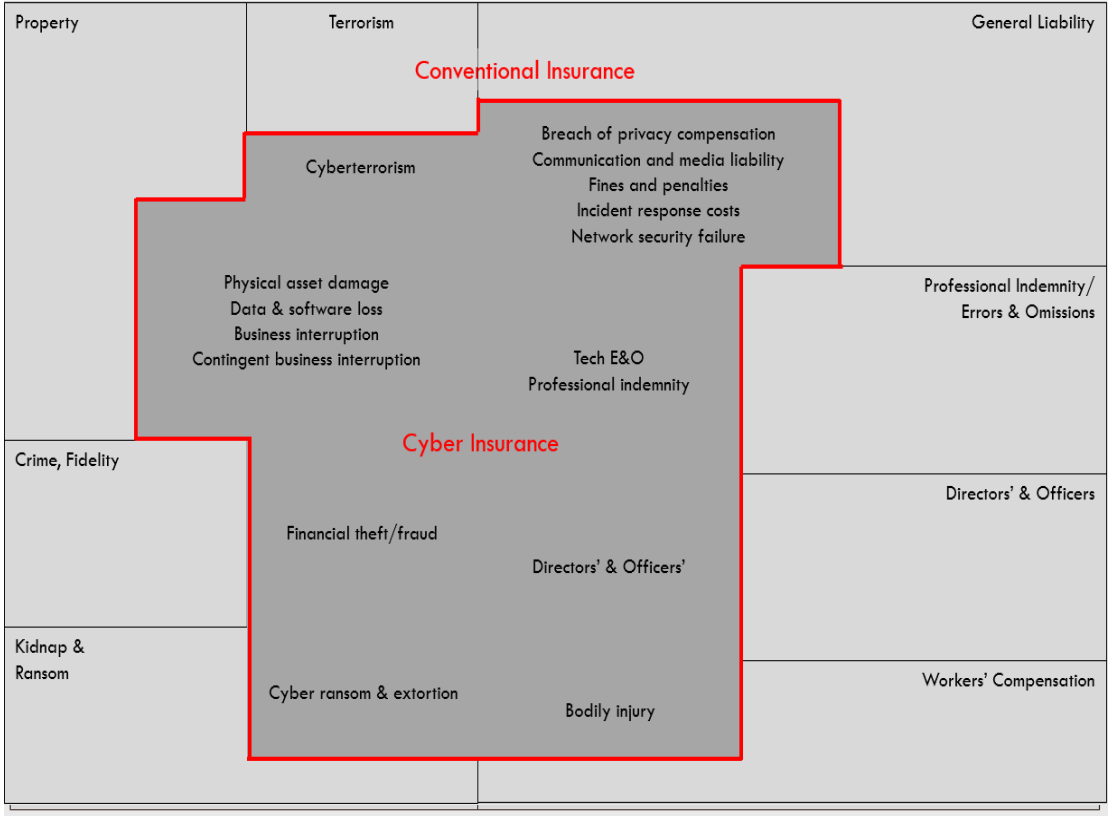
1. Insurance premium increases
2. Increased cost to raise debt
3. Operational disruption or destruction
4. Lost value of customer relationships
5. Value of lost contract revenue
6. Devaluation of trade name
7. Loss of intellectual property

Deloitte University (2016): Beneath the Surface of a Cyberattack



The Cyber-physical Insurance Market to Emerge

Conventional (Physical) Insurance Market



Not to scale of actual market size

Segmented (and being further segmented) by the cause(s) of loss

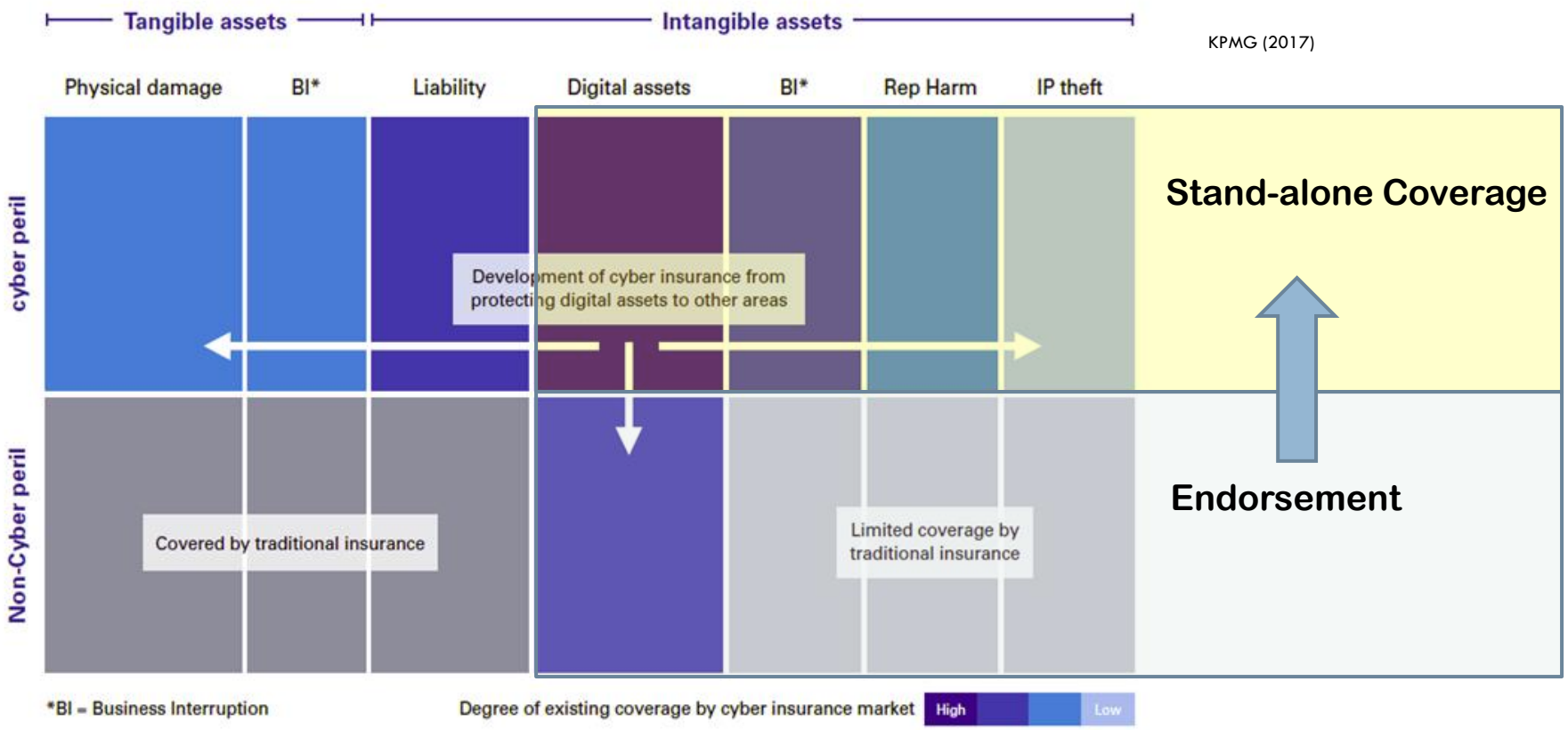
Stand-alone or

Endorsement

Better than ever but still with gaps in limits and scopes

The Insurance Market in Transition: Carving-out Cyber Risk

KPMG (2017)



Physical Insurance Market

Traditional Risks
(Natural and Man-made)

Physical Perils

Intangible Perils
(Human Errors)

Tangible Assets
Intangible (Intellectual) Assets

Direct

Property Damage

Bodily Injury

Personal Injury

Indirect

Business Interruption

Exposure-based, multiple Coverages
(Stand-alone; Endorsement)

Property Coverage

Liability Coverage

Package Coverage

Business Interruption

Cyber Insurance Market

Cyber Risks
(Man-made and Machine-made)

Intangible Perils
(Human Errors)

Security Breaches & Attacks

System Errors (Machine Learning & AI

Tangible Assets
Intangible (Intellectual) Assets

Direct

Property Damage

Bodily Injury

Personal Injury

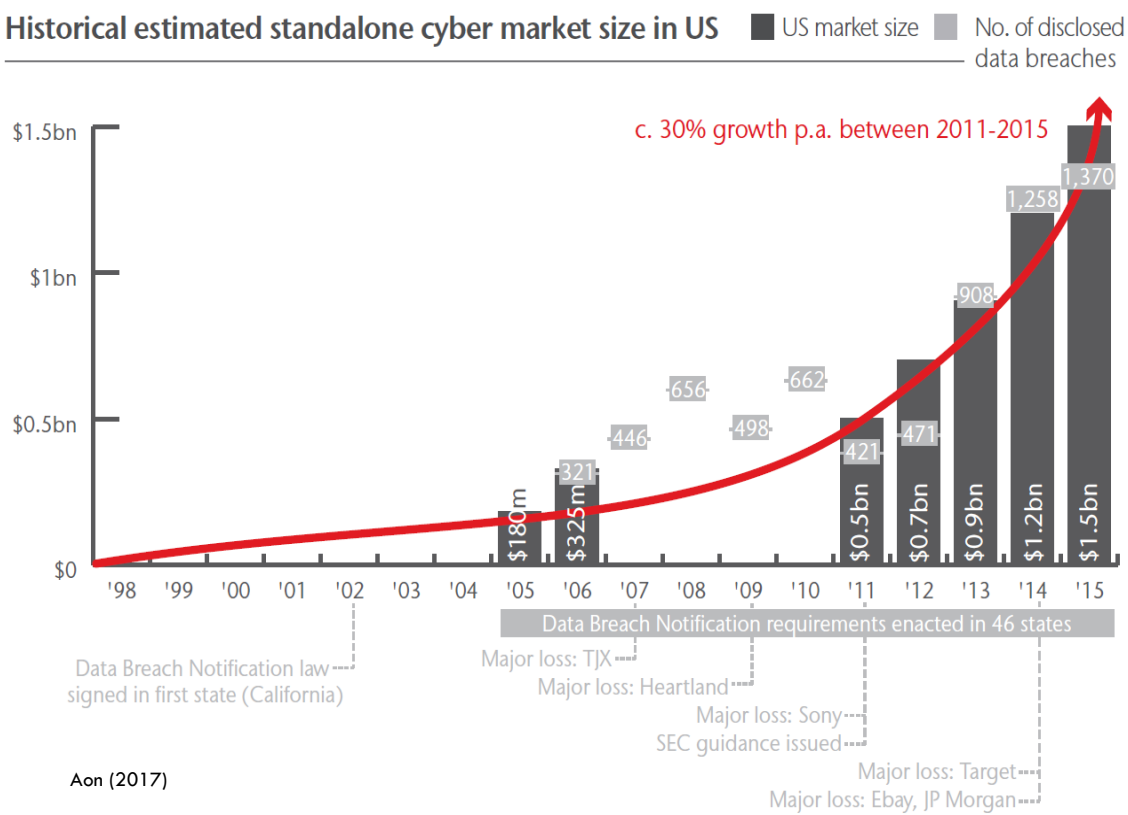
Indirect

Business Interruption

Single Coverage
(Trend to Stand-alone; Endorsement)

U.S. Cyber Insurance Markets

The U.S. Market (Stand-alone Cyber Insurance Policies) (1998 - 2015)



Aon (2017)

- Application of conventional market approaches
- Increase in the use of stand-alone policies

U.S. Cyber Insurance Markets

The U.S. Market (Estimated Breakdown of the Stand-alone Cyber Insurance Market (2015)

Company type	Industry and revenue	SME	Mid-market	Large corporate	% of total	
Companies storing personal data	Technology	$39.0m	$18.0m	$14.0m	5%	$242.0m (17%)
	Telecoms and media	$3.3m	$8.0m	$13.0m	2%	
	Education	$5.3m	$46.0m	$21.0m	5%	
	Professional services	$9.4m	$43.0m	$22.0m	5%	
Financial transactions driven companies	Retail and wholesale ✓	$76.0m	$141.0m	$93.0m	21%	$876.0m (59%)
	Financial institutions ✓	$31.0m	$180.0m	$227.0m	29%	
	Business services	$6.7m	$47.0m	$33.0m	6%	
	Hospitality	$5.5m	$22.0m	$13.0m	3%	
Companies exposed to operational risks	Manufacturing	$56.0m	$19.0m	$16.0m	6%	$126.0m (8%)
	Utilities	$1.3m	$4.1m	$15.0m	1%	
	Energy (Oil and Gas)	$1.2m	$3.6m	$9.0m	1%	
Companies storing personal data & exposed to operational risks	Healthcare ✓	$3.4m	$103.0m	$81.0m	15%	$256.0m (17%)
	Transportation	$13.0m	$14.0m	$10.0m	2%	
	Total	$282.0m	$649.0m	$567.0m	100%	$1.5bn

Large corporate ($39.0m, $18.0m) / $567m ($14.0m) / Mid-market ($31.0m, $6.7m, $5.5m, $56.0m, $1.3m, $1.2m) / $649m ($180.0m, $47.0m, $22.0m, $19.0m, $4.1m, $3.6m) / SME ($103.0m, $14.0m) / $282m ($3.4m, $13.0m)

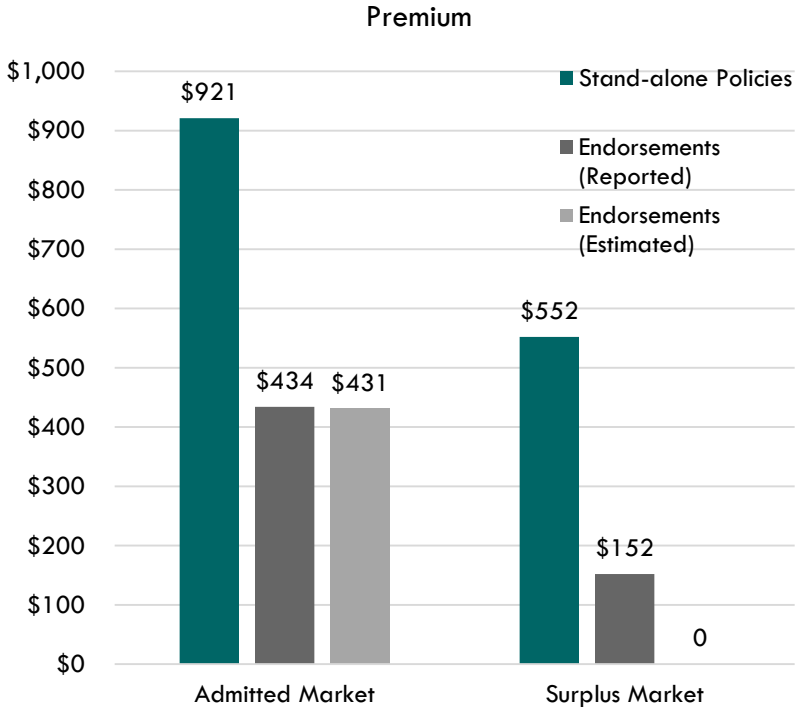
Aon (2017)

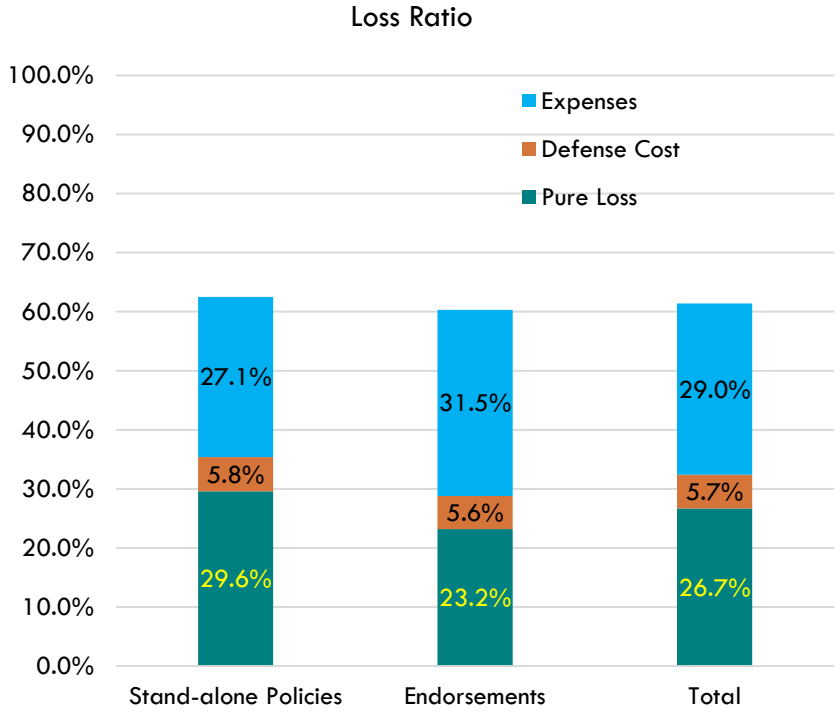
Notes: SME are defined as companies with sales/turnover below $100m; Mid-market: $100m to $1bn; Large corporate: >$1bn

Source: Advisen, Marsh, Bureau van Dijk, Aon placement data, Aon Inpoint analysis

U.S. Cyber Insurance Markets

The U.S. Market (Estimated Breakdown of the Stand-alone Cyber Insurance Market (2016)

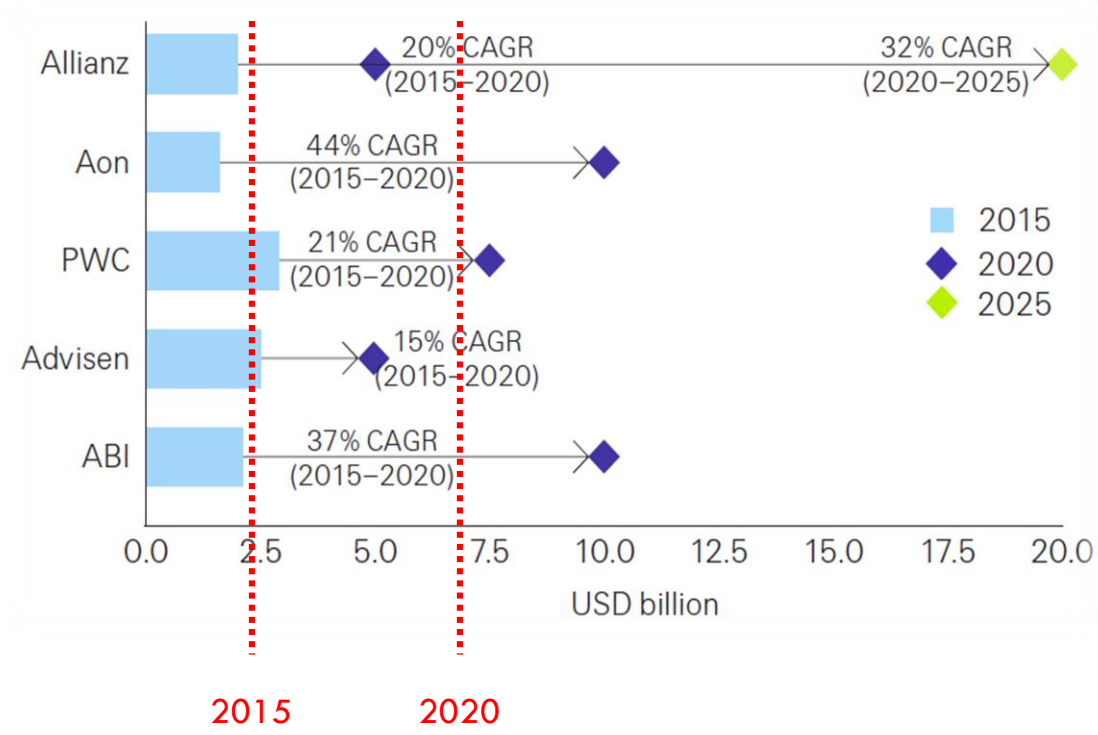




NAIC (2017), Aon (2017)

Global Cyber Insurance Markets

Estimates of Global Cyber Insurance Premiums (2015-2025)



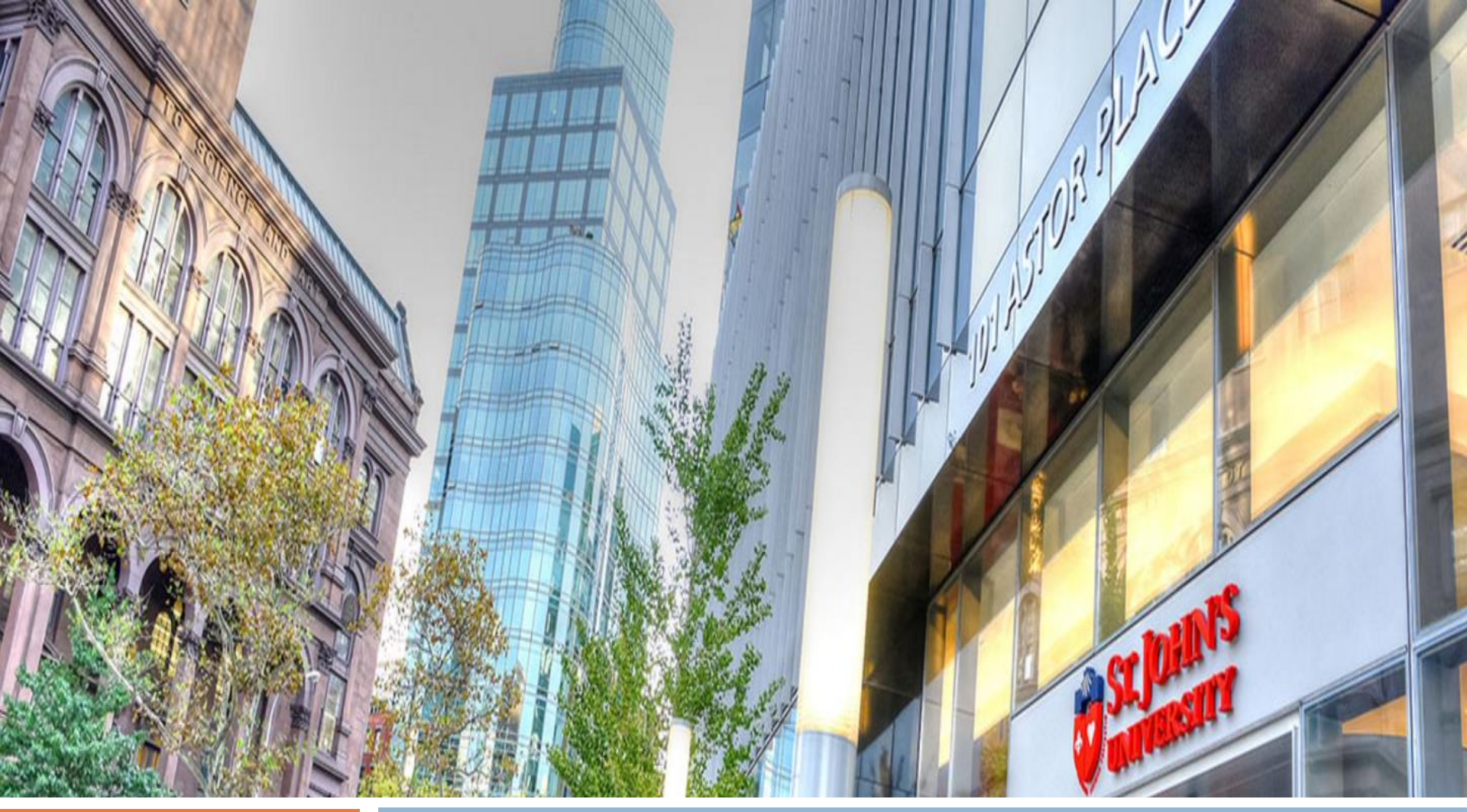
- Commercial account driven
- U.S. market driven

Swiss Re (2017)

Key Findings from Cyber Insurance Studies

Surveyor and Year	Method/Survey (Target Groups)	Key Findings
Willis Re (2017)	Silent Cyber Risk Outlook	• The mean of the risk factor of the "silent cyber loss" to property policies is 1.074 (that is, the likelihood of 1.074 cyber-related losses per 100 non-cyber-related losses)
Romanosky et al. (2017)	Survey of insurance companies	• Less than expected variations in the listing of "coverage topics" but the variations more significant in the listing of "coverage exclusions" • Significant variations in premium rating methodologies
Aon (2017)	Global Cyber Market Overview 2017	• 59% of the premium revenues in the U.S. cyber insurance market are from financial transaction-driven entities; 17% from entities that store personal data and are exposed to operational risks; 17% from entities that store personal data only; and the balance of 8% from entities exposed to operational risk only. • Lloyd's share of U.S. cyber insurance premiums at approximately 30%
OECD (2017b)	OECD Survey 2016	• The level of cyber risk is perceived "high" by insurers, reinsurers and intermediaries but "moderate" by insurance authorities.[36]
NetDiligence (2016)	Cyber Claims Study 2016	• During the 2013-2015 data year, 87% of insurance claims are from organizations with revenues of less than $2 billion • Average number of records lost was 2.04 million (median at 1,339) • Average insurance claims paid was $495,000 (median at $49,000) • Average cost of breach was $665,000 (median at $60,000)

Source: Author compilation



Coordination and Standardization Issues

Defining “Cyber Risk”: No Standard Yet

- "[Any] risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks" (CRO Forum, 2014) to “the risk of doing business in the cyber [environment]” (CRO Forum, 2016).

- “[Any] risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems” (Institute of Risk Management, the U.K.).

- “[Any] risk of financial or physical loss, disruption of services, privacy violation, or damage to the assets or reputation of an organization through either a failure of its information or technology systems, or a malicious act affecting their information or technology systems” (Advisen, 2017).

- “Cyber” short for the [world of cyberspace] which is an interactive domain composed of digital networks for storage, modification, information communication and other uses” (Biener, Eling, & Wirfs, 2015).

What is Cyber Risk and Loss Exposure

Exposure Groups for Insurance Coverage Scopes

- Business interruption (BI)
- Contingent business interruption (CBI) for non-physical damage
- Data and software loss
- Financial theft and/or fraud
- Cyber ransom and extortion
- Intellectual property theft
- Incident response costs
- Breach of privacy
- Network security/security failure
- Reputational damage (excluding legal protection)
- Regulatory & legal defense costs (excluding fines and penalties)
- Fine and penalties
- Communication and media
- Legal protection – lawyer fees
- Assistance coverage – psychological support
- Products
- Director's & Officer's (D&O)
- Tech E&O
- Professional services E&O, professional indemnity
- Environmental damage
- Physical asset damage
- Bodily injury and death

What is Cyber Risk and Loss Exposure?

RIMS (2017)

Santos (2017)

- First-party coverages
  - Network interruption/ business interruption
  - Cyber extortion/ransom
  - Data loss and restoration
  - Reputation/crisis management
  - Theft/fraud
  - Forensic investigation costs
  - Regulatory fines
  - Media liability
- Third-party coverages
  - Privacy liability
  - Breach notification costs
  - Credit monitoring
  - Transmission of viruses or malicious code

What is Cyber Risk and Loss Exposure

Swiss Re (2017), Regrouped by Kwon

- First-party coverages
  - Network, IT security failure (BI)
  - Contingent business interruption (CBI)
  - Cyber extortion

- Third-party coverages
  - Privacy breaches
  - Network liability
  - Errors and omissions (E&O)

Cross-Comparison

CRO Forum (2016)	Advisen and PartnerRe (2016, 2017)*	OECD (2017b)**	Swiss Re (2017)	RMS (2016)
Business Interruption (BI) of operations	Business interruption	Business interruption		Business Interruption
Contingent BI for non-physical damage	Dependent business interruption		Contingent business interruption	Contingent business interruption
Data and software loss	Data breach/restoration	Data and software loss		Data and software loss
Financial theft and/or fraud	Fund transfer fraud/social engineering	Financial theft and fraud		Financial theft and fraud
Cyber ransom and extortion	Cyber extortion	Cyber ransom and extortion	Cyber extortion	Cyber extortion
Intellectual property (IP) theft		IP theft		IP theft
Incident response costs		Incident response costs		Incident response costs
Breach of privacy		Breach of privacy compensation	Privacy breaches	Breach of privacy
Network security/security failure (liability)	System failure	Network security failure	Network, IT security failure/ network liability	Network service failure liabilities
Reputational damage (excluding legal protection)		Reputational damage		Reputational damage Multi-media liabilities (defamation and disparagement)
Regulatory & legal defense costs (excluding fines and penalties)	Regulatory fines & penalties	Regulatory & legal defense cost		Regulatory and defense coverage
Fine and penalties		Fine and penalties		
Communication and media	Internet media	Communication and media	Media	
Legal protection – lawyer fees		Regulatory & legal defense		
Assistance coverage – psychological support				
Products (liability)				Product and Operations
Directors & Officers (D&O) Liability				
Tech Errors & Omissions (E&O)				Technology E&O
Professional services E&O, Professional indemnity			E&O	Professional Services E&O
Environmental damage				Environmental damage
Physical asset damage	Property damage	Physical asset damage		Physical asset damage
Bodily injury and death	Bodily injury	Bodily injury		Death and bodily injury

Cyber Insurance Policy Comparison (Example)

Fuller table at the study report

Definition	Insurer A	Insurer B	Insurer C	Insurer D
Computer System	[Computer network] a connected network of computer hardware, software, and any associated components leased, owned, operated or controlled by the Company	[Computer] a device or group of devices that by manipulation of electronic, magnetic, optical or electromechanical impulses pursuant to a computer program can perform operations on Data.	[System] a Computer; and (A) any input, output, processing, storage and communication devices controlled, supervised or accessed by the operating systems that are proprietary to, or licensed to, the owner of the Computer; and (B) Media [Computer] computer hardware and software, and the electronic data stored thereon, as well as associated input and output devices, data storage devices, networking equipment, components, firmware and electronic backup facilities, including systems accessible through the internet, intranets, extranets or virtual private networks	[Computer system] any information technology or operational technology
Cyberattack	[Breach] the failure of the Insured or others on behalf of the Insured to prevent or protect against the following: 1. the disclosure of Confidential Information by an Insured or a third party for whom the Insured is legally responsible; 2. unauthorized access to the Computer Network; 3. unauthorized use of the Computer Network; 4. participation of the Computer Network in a denial of service (DoS) attack directed against a third party; 5. transmission of malicious code from the Computer Network causing harm to a third party; 6. denial of access to Computer Network; 7. physical theft of hardware on which data is stored; or 8. the failure to disclose the aforementioned in violation of Privacy Breach Notice Law	[Cyberattack] the transmission of fraudulent or unauthorized Data that is designed to modify, alter, damage, destroy, delete, record or transmit information within a System without authorization, including Data that is self-replicating or self-propagating and is designed to contaminate other computer programs or legitimate computer Data, consume computer resources or in some fashion usurp the normal operation of a System	[Denial-of-service attack] a malicious attack by a third party which is designed to slow or completely interrupt access to a targeted computer system or website by other third parties authorized to gain access to that computer system or website	[Denial-of-service attack] a malicious attack by a third party which is designed to slow or completely interrupt access to a targeted computer system or website by other third parties authorized to gain access to that computer system or website
Data	[Electronic data] any data stored electronically on a Computer Network, including Confidential Information	[Data] a representation of information, knowledge, facts, concepts, or instructions which are being processed or have been processed in a Computer	[Electronic data] information that exists in electronic form, including Personal Information; provided, however, [it] does not include Software.	[Data] Any electronic information or record of a form readily usable or readable by a Computer Program
Digital assets	[Electronic content] digital media including advertising and promotional material that is published, disseminated, released, gathered, distributed or transmitted in electronic or digital format on behalf of the Insured or by the Insured for themselves or for others, Electronic Content shall not include: 1. computer software except to the extent that it displays digital content; or 2. any actual products or services described, illustrated or displayed in such Electronic Content.		[Digital assets] electronic data, software, audio files, and image files stored on the company's computer system, and the capacity of such computer system. Digital assets do not include accounts, bills, evidences of debts, money, valuable papers, records, abstracts, deeds, manuscripts or other documents, except if they have been converted to electronic data, and then only in that form	[Media content] any information, including words, sounds, numbers, images or graphics and shall include advertising, video, streaming content, webcasting, online forums, bulletin board and chatroom contents, in any format, but does not include computer software or the actual goods, products, or services disabled,

Cyber Insurance Coverage Gaps and Need for Standardization

- Large data aggregators
  - Those with massive amounts of personally identifiable information present a unique and potentially costly risk and cyber limits have not caught up
- Cloud infrastructure services
- Integration with technology
  - IoT
  - Wearable (medical) devices

    …,
- First party and BI exposures
- Third party liability risks
  - Property damages
  - Bodily injuries
  - Personal injuries

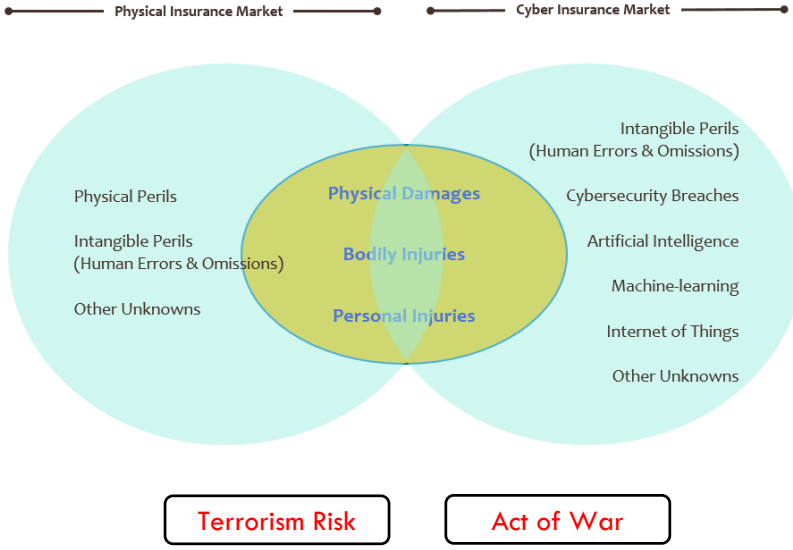
Cyber Risk Modelling or Cyberspace Risk Modelling?

Cyber Risk ≈

Business Email Compromise, Operational Technology, Vendor Risk,
People, Social Engineering,
Sophisticated Hackers, Organized (Nation-state) Cybercrime,
Robots, Machine Learning, IoT, Connected Devices,
Critical Infrastructure, Cloud, Misconfiguration,
Threat Environment,
Regulatory Compliance,
Aggregation

^ Interconnectedness

Cyber-physical Insurance Market



- Pooling all cyber risks into a single policy using a stand-alone policy or endorsement. Is it sustainable?
  - Structure-wise
  - Long-term perspective wise

Summing Up…,

- Human behavioral and IT factors affect the types and scopes of cyber losses
- A need arises to develop a cyber insurance market, rather than all-in-one cyber insurance policy
  - Coordination, harmonization and standardization among all parties of interest for the true service for and protection of clients – large and small
- Indeed, *the business of insurance is in transition to operations in the physical-cyber market*.

Thank You!

W. Jean Kwon
KwonW@stjohns.edu

Full report available at
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3201875
(Version October 15, 2018)

Advancing with you
MS&AD
INSURANCE GROUP

Cyber Insurance in Japan

November 5th, 2018

MS&AD InterRisk Research & Consulting

Takeshi Doi

Agenda

1. Self-introduction

2. Cyber Security in Japan

3. Cyber Insurance in Japan

Self-introduction

Advancing with you
MS&AD
INSURANCE GROUP

Takeshi Doi

- Senior Manager / New Market Development Sec.
  MS&AD InterRisk Research & Consulting, Inc.
- Deputy General Manager, Innovation Section
  MS&AD Insurance Group Holdings, Inc.
- Researcher of SFC Research institute Keio University
- Task force member, Trust mark committee,
  Sharing Economy Association Japan
- Assistant Coordinator, ILP,
  International Foundation for Information Technology

Carriers

1996	Join Sumitomo Marine & Fire Insurance Co., Ltd.
2004	Superintendent, Mitsui Sumitomo Seguros, ltda.
	(Went to Brazil)
2006	CIO and Director, Mitsui Sumitomo Seguros, ltda.
2009	MS Systems (Came back to Japan)
2013	Deputy director, Cabinet Secretariat Japan
	(Job Transfer for three years)
2016~	Current Position

MS&AD Insurnace Group

Advancing with you
MS&AD
INSURANCE GROUP

Holding Company

MS&AD

MS&AD Insurance Group Holdings

Domestic Non-life Insurance Business

Mitsui Sumitomo Insurance

Aioi Nissay Dowa Insurance
Mitsui Direct General Insurance

Domestic Life Insurance Business

Mitsui Sumitomo Aioi Life Insurance
Mitsui Sumitomo Primary Life Insurance

International Business

MS&AMLIN　MSIG　Box Innovation

Financial Services Business

Risk-related Services Business

MS&AD

MS&AD InterRisk Research & Consulting

Advancing with you
MS&AD
INSURANCE GROUP

Scale
Adequate capacity derived from scale

MS&AD's Strengths: Scale

Positioning in Each Business Domain

No. 8 in the world

Groupwide

No. 8 among non-life insurance groups in the world

▶Fortune Global 500: 2017 Income Ranking

(Ordinary income basis for Japanese insurance groups)
(US$ million)

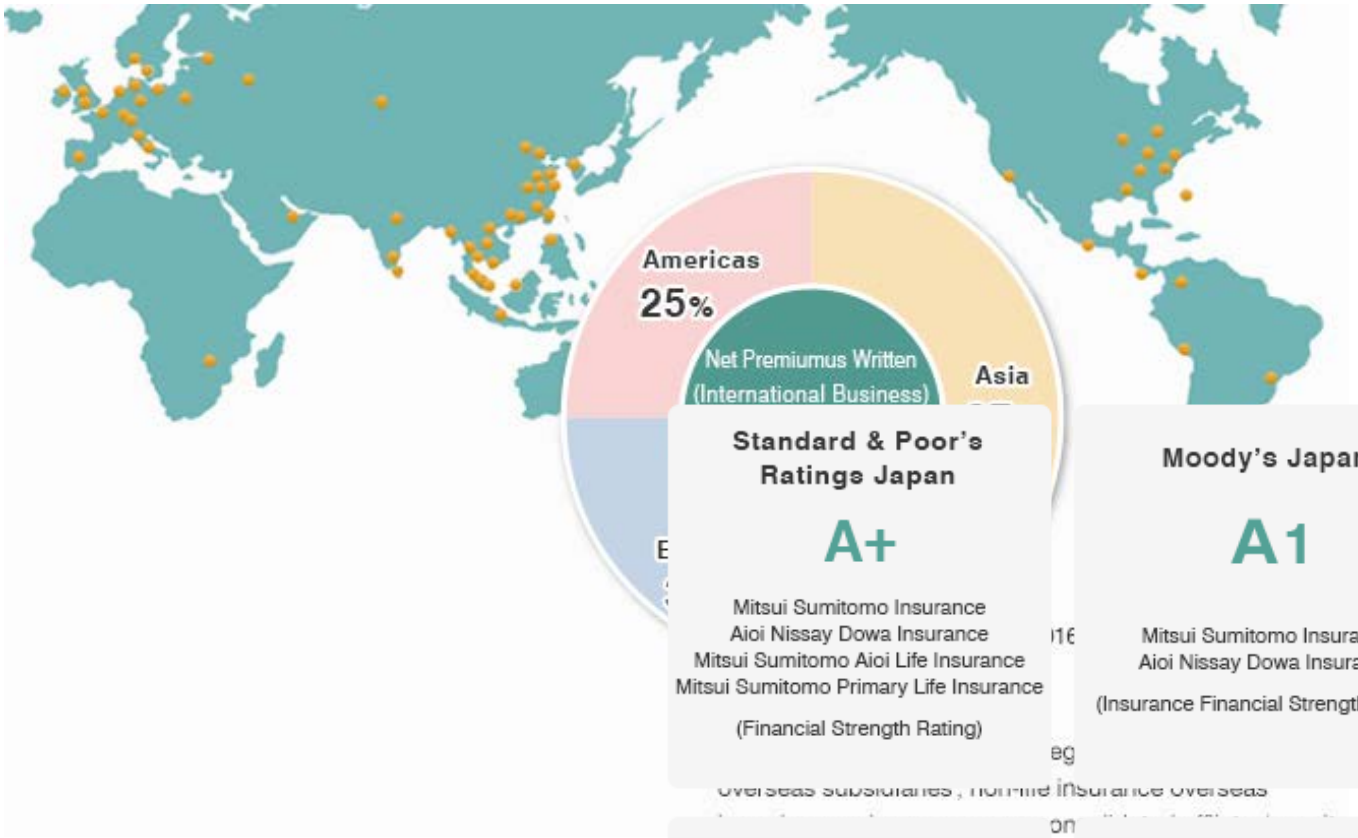
	Company/Group Name	Income
1	Berkshire Hathaway	$223,604
2	Allianz	$122,196
3	State Farm Insurance Cos.	$76,132
4	Munich Re Group	$68,700
5	Zurich Insurance Group	$67,245
6	People's Insurance Co. of China	$66,732
7	AIG	$52,367
8	**MS&AD Insurance Group Holdings**	**$49,239**
9	Tokio Marine Holdings	$48,292
10	Swiss Re	$43,786

Source: Fortune Global 500 2017 Insurance Property & Casualty (Stock + Mutual)

International Businesses

Advancing with you
MS&AD
INSURANCE GROUP

We do business across 46 countries and regions worldwide. In the ASEAN region, we are No.1*in total non-life insurance premiums.



Credit Ratings

As of September 27, 2017

Standard & Poor's Ratings Japan

A+

Mitsui Sumitomo Insurance
Aioi Nissay Dowa Insurance
Mitsui Sumitomo Aioi Life Insurance
Mitsui Sumitomo Primary Life Insurance

(Financial Strength Rating)

Moody's Japan

A1

Mitsui Sumitomo Insurance
Aioi Nissay Dowa Insurance

(Insurance Financial Strength Rating)

Rating and Investment Information(R&I)

AA

Mitsui Sumitomo Insurance
Aioi Nissay Dowa Insurance
(Issuer Rating)

Mitsui Sumitomo Aioi Life Insurance
Mitsui Sumitomo Primary Life Insurance

(Insurance Claims Paying Ability)

Japan Credit Rating Agency (JCR)

AA+

Mitsui Sumitomo Insurance
Aioi Nissay Dowa Insurance

(Long-Term Issuer Rating)

A.M.Best

A+

Mitsui Sumitomo Insurance
Aioi Nissay Dowa Insurance

(Financial Strength Rating)

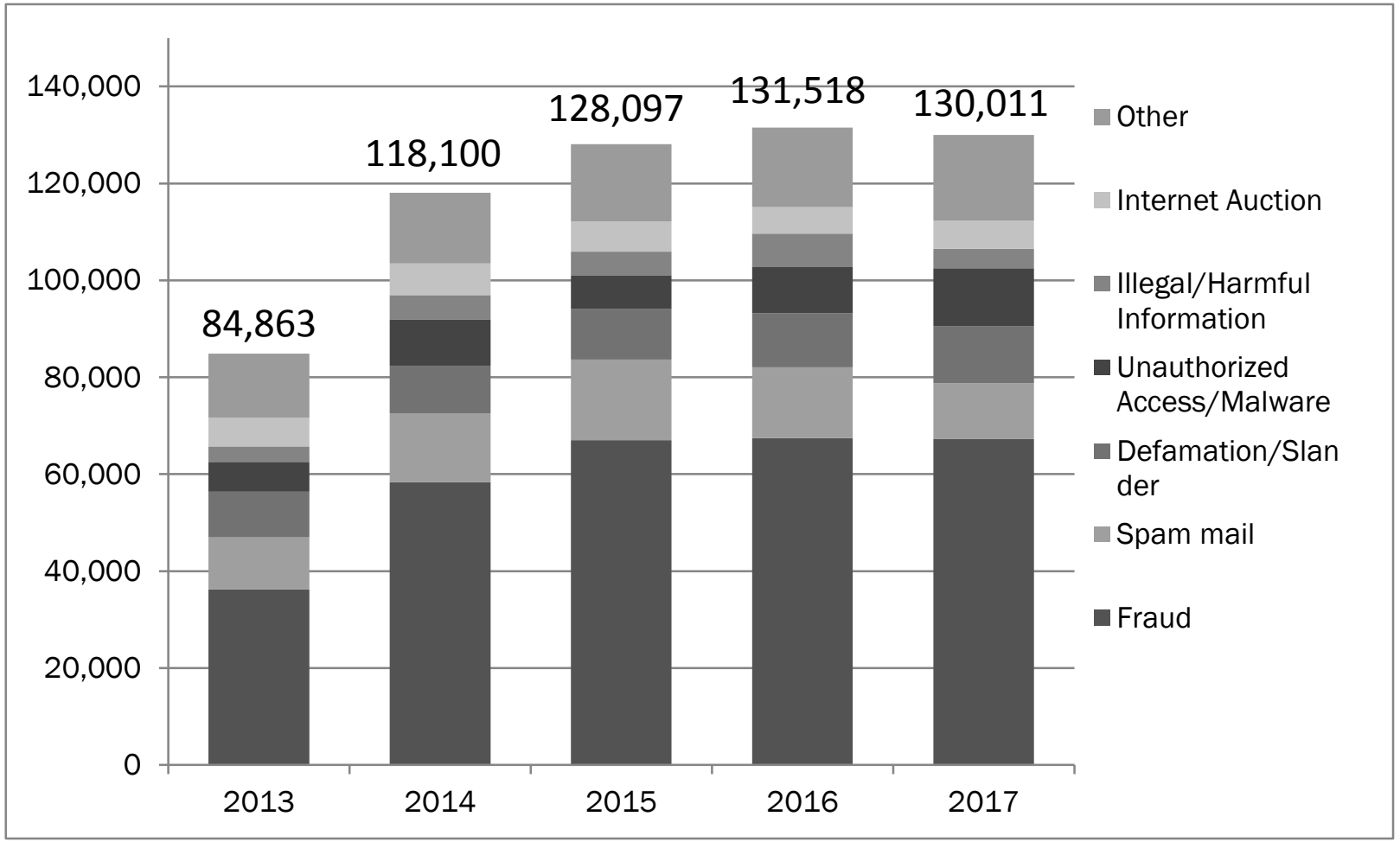
5 Domains & MS&AD InterRisk Research & Consulting, Inc.

Trend of Cyber Security in Japan

Cyber Crime reported to the Police in Japan

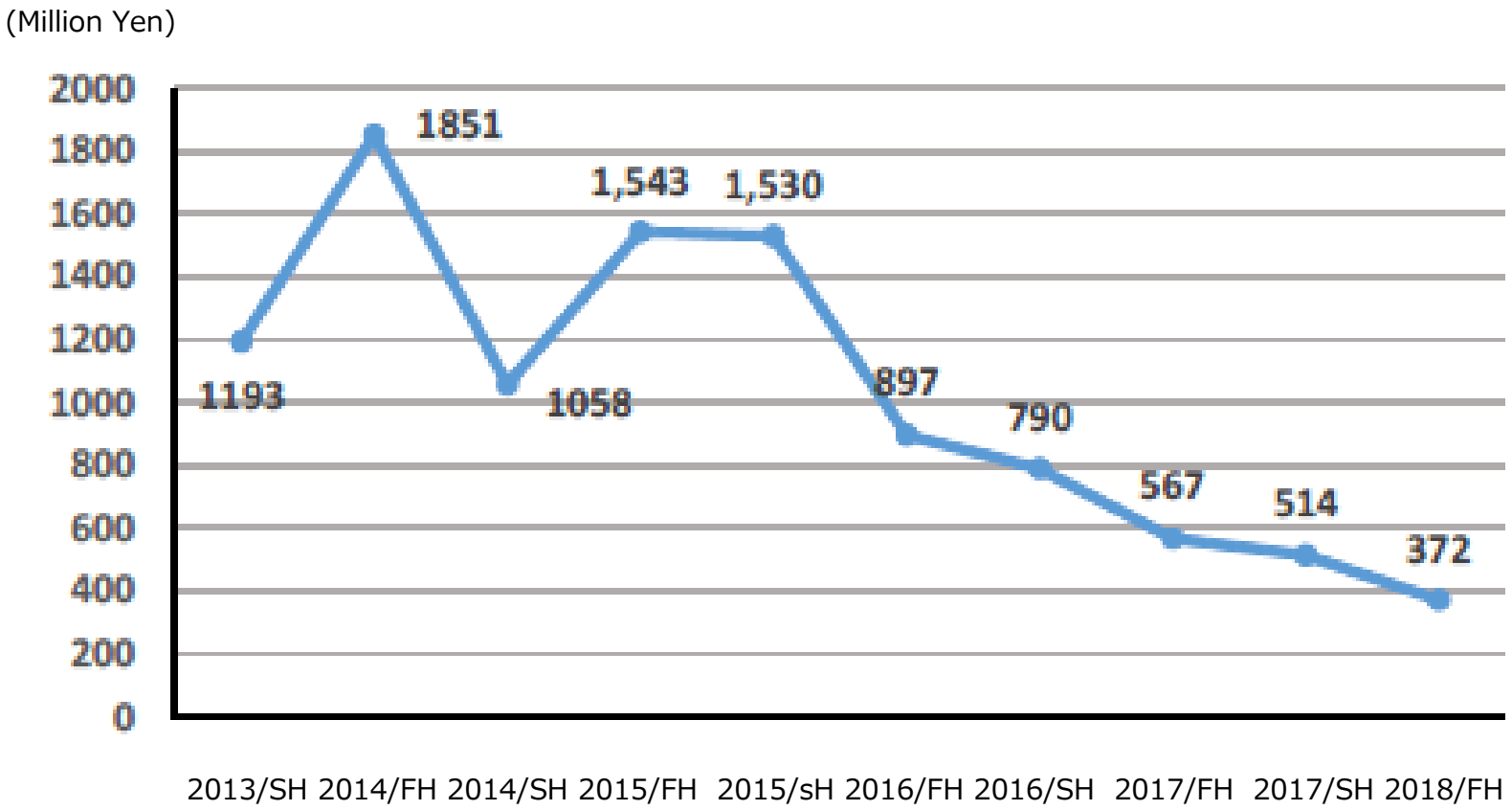
Advancing with you
MS&AD
INSURANCE GROUP

Number of Consultation to the Japanese Police



*National Police Agency of Japan: Cyber Crime Report

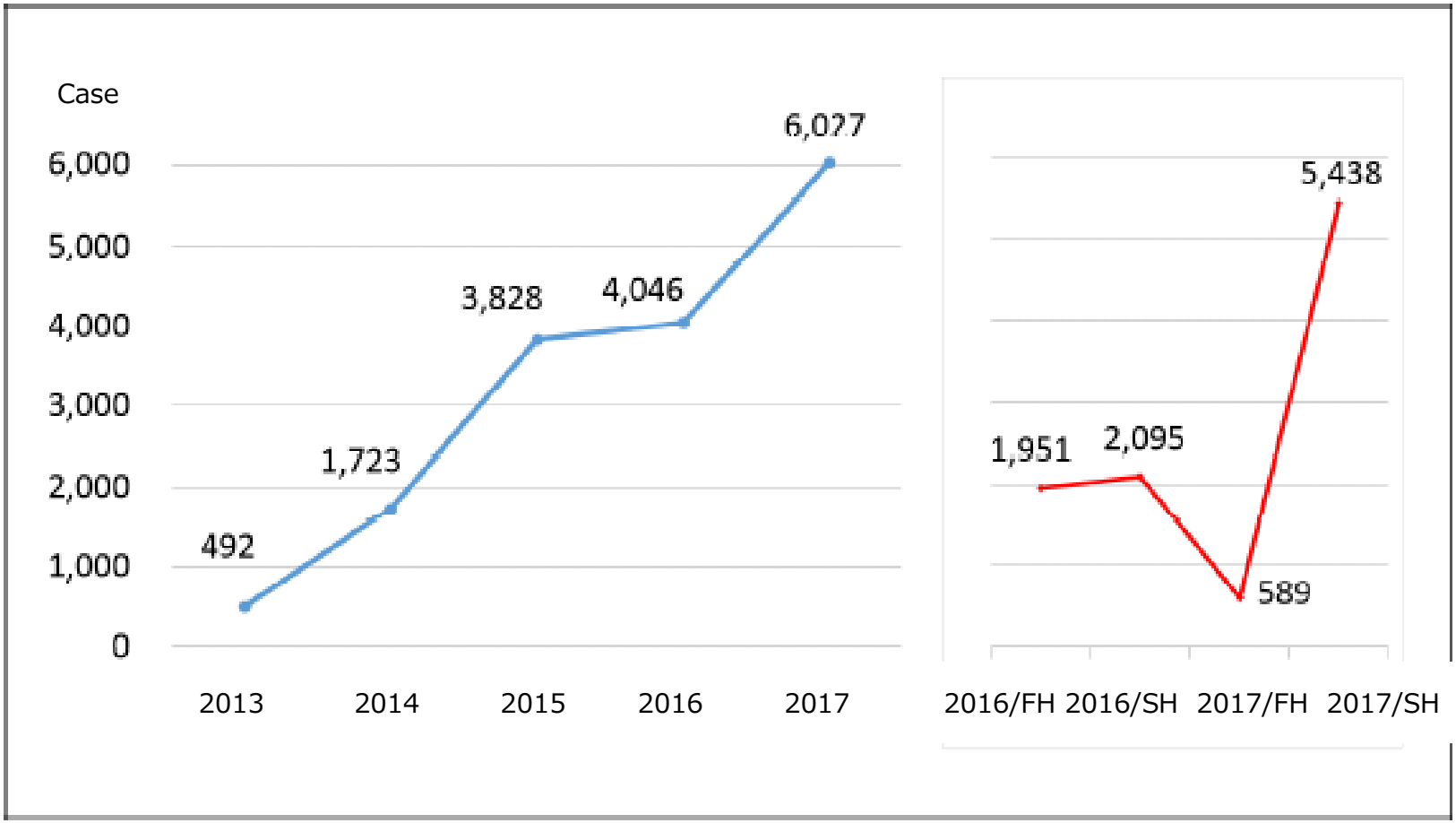
Internet Banking : Illegal remittance



Dramatic reduce in business (company) injury, total amount went down.

*National Police Agency of Japan: Cyber Crime Report

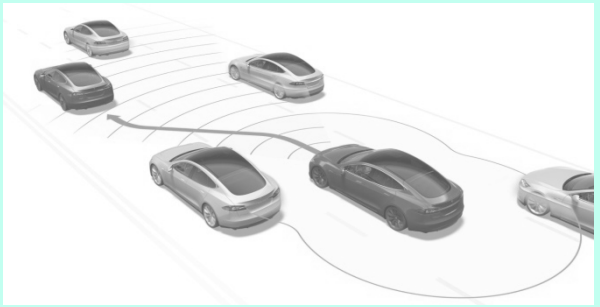
Targeted attacks



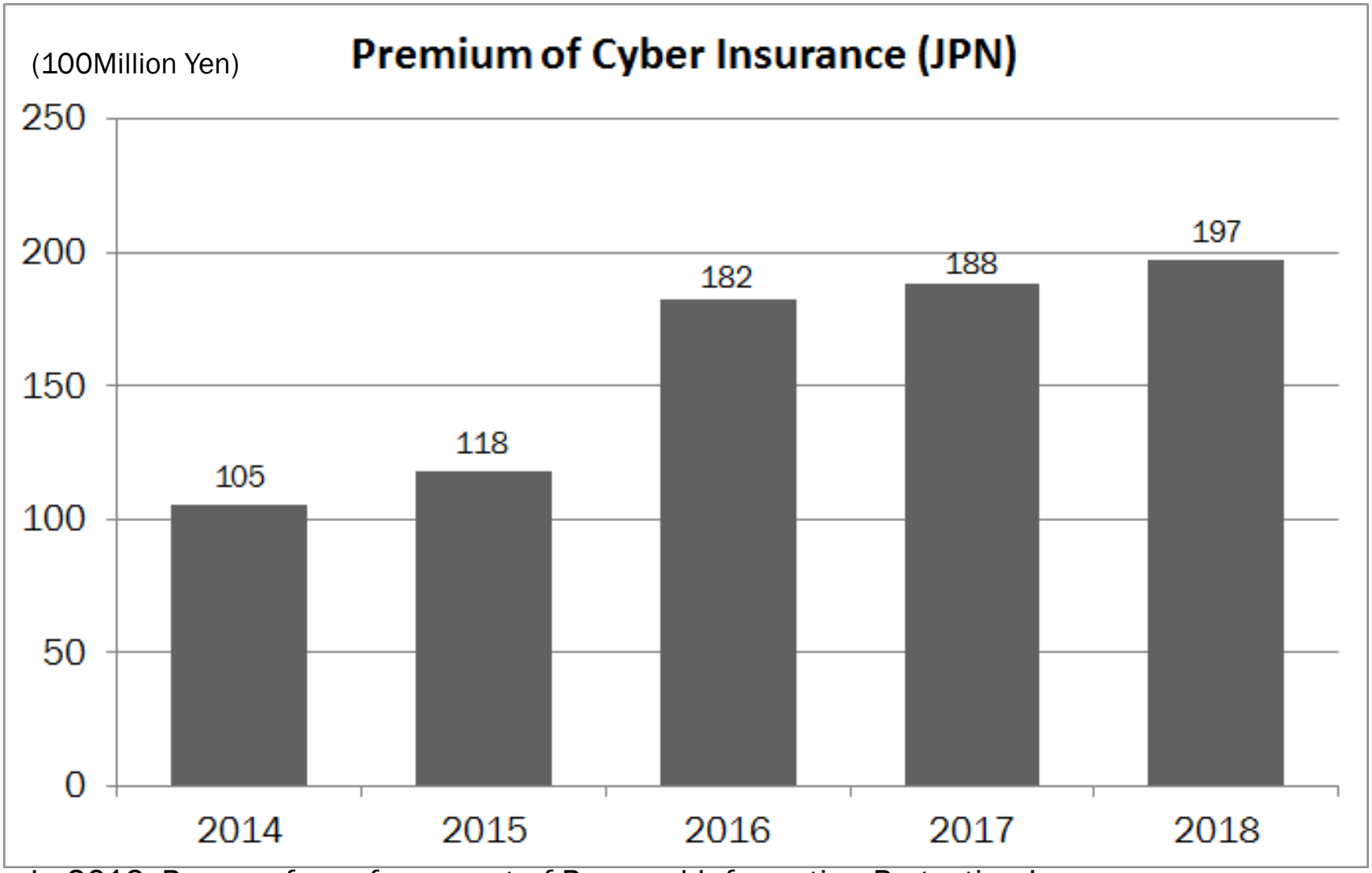
*National Police Agency of Japan: Cyber Crime Report

Cyber Insurance in Japan

Cyber Insurance (Affirmative and Silent)

Purpose	・Cyber space Ex. Data 	・Physical and Tangible ex. Automobile, House 
Incidents and losses	・Data leakage, Theft & etc.	・Car Accident ・Fire & etc.
Insurance Product	・Cyber Insurance	・Traditional Insurance
Classification	Affirmative Cyber	Silent Cyber

Market of Cyber Insurance in Japan



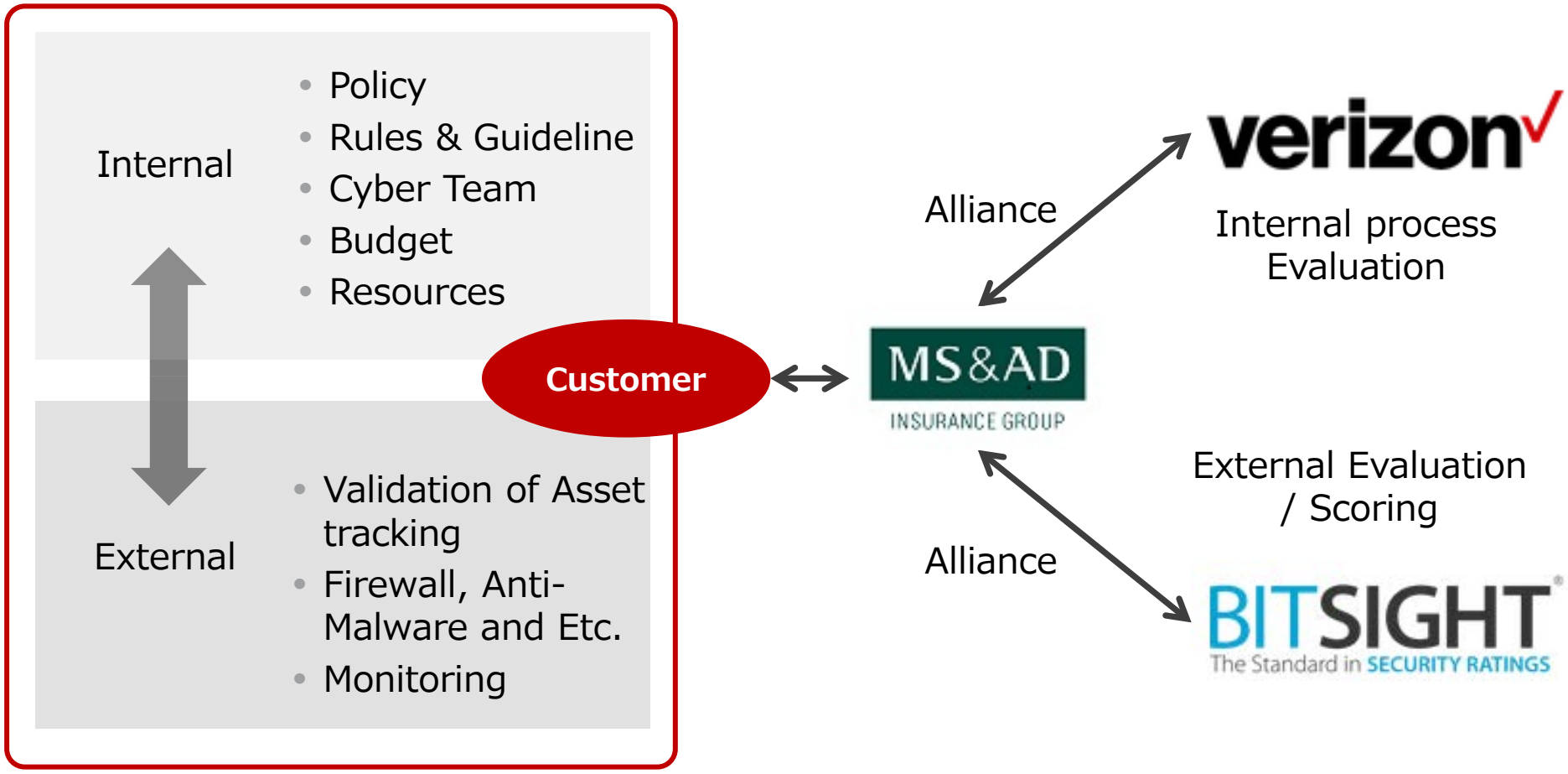
In 2016, Prepare for enforcement of Personal Information Protection Law

*JNSA: Cyber Industry Market Report

Advancing with you
MS&AD
INSURANCE GROUP

It’ll be shown in the screen.

MS&AD Cyber Risk Assessment Process



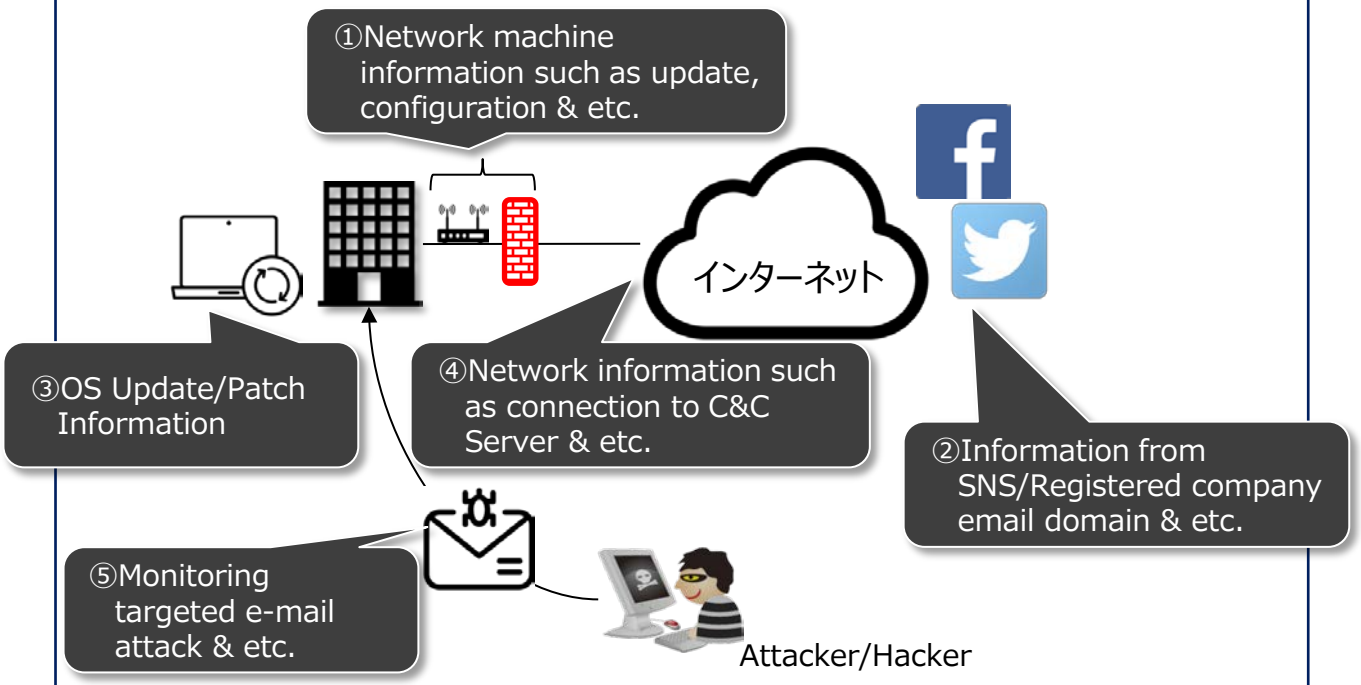
It’ll be shown in the screen.

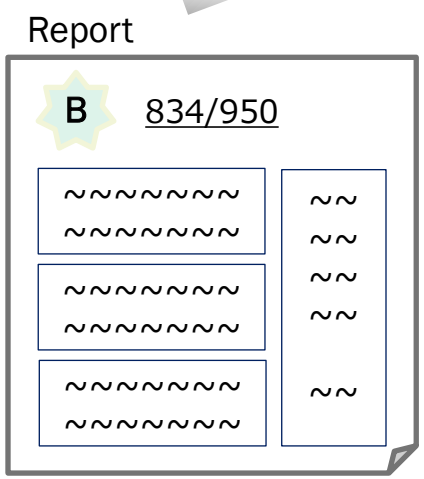
Cyber Risk Evaluation (External Scoring system)

Advancing with you
MS&AD
INSURANCE GROUP

BITSIGHT
The Standard in SECURITY RATINGS

Evaluate and Score the current situation from those information which are collected from Internet.





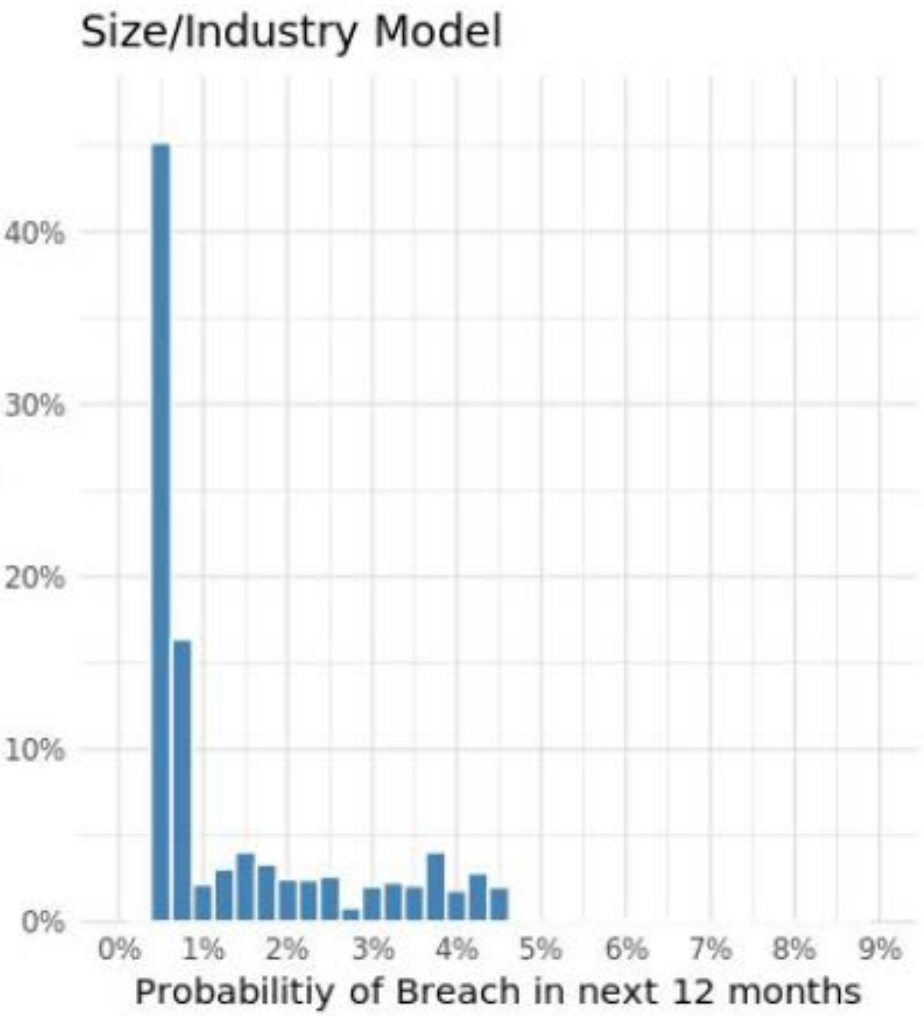
- Scoring by all information as ①～⑤ (weights of each category are defined by BitSight periodically).
- Do not make any penetration test. It is totally legal monitoring.

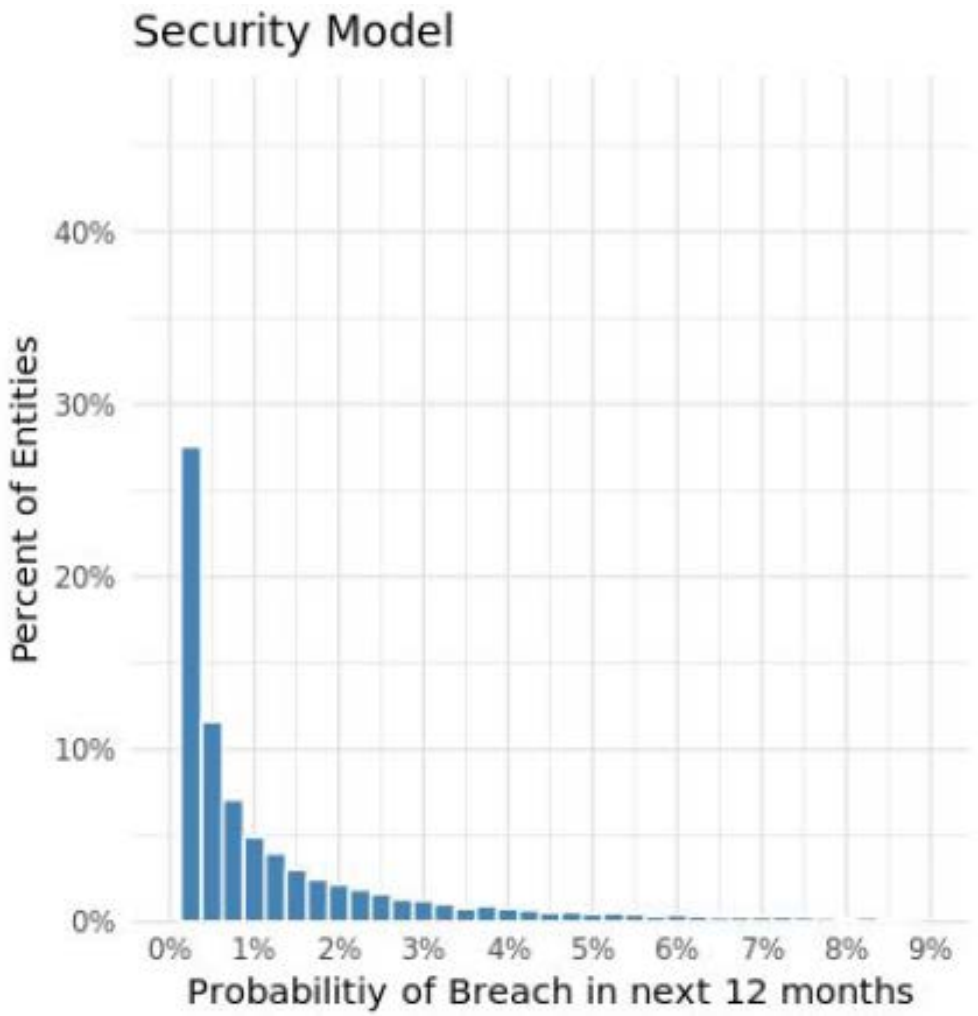
Cyber Risk Evaluation (External Scoring system)

Advancing with you
MS&AD
INSURANCE GROUP

It’ll be shown in the screen.

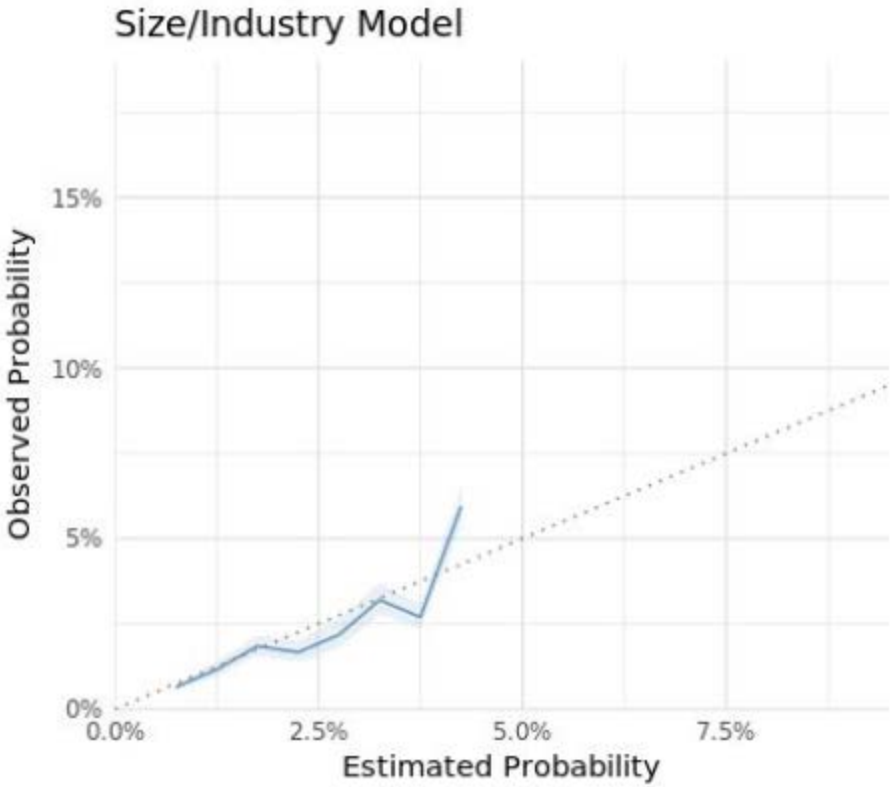
Model with (without) Security Score

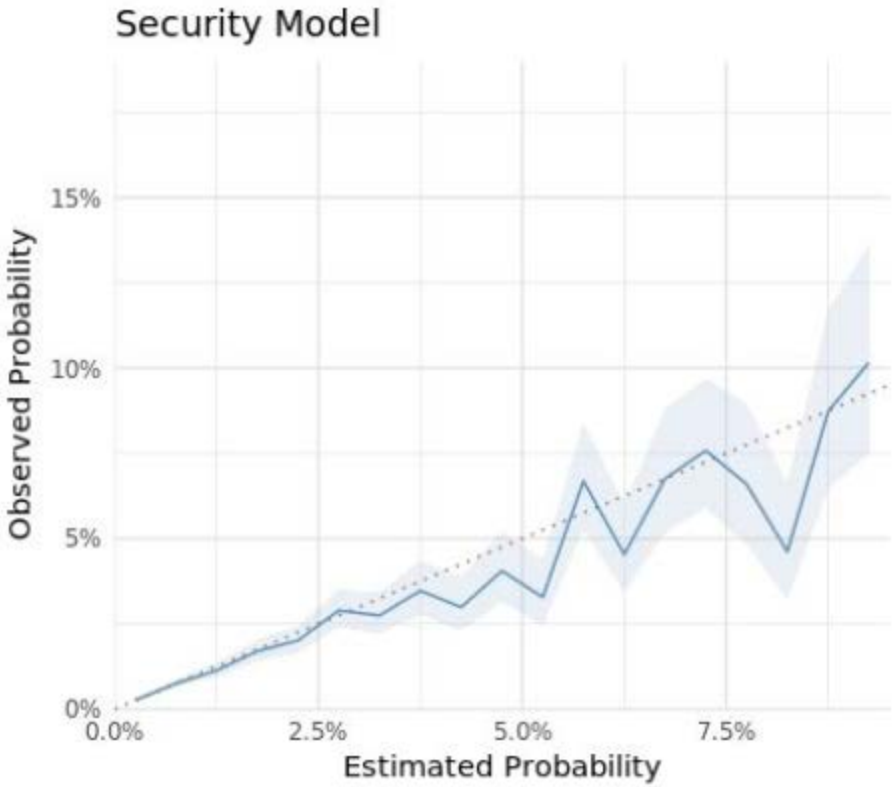




* BitSight study

Model with (without) Security Score





* BitSight study

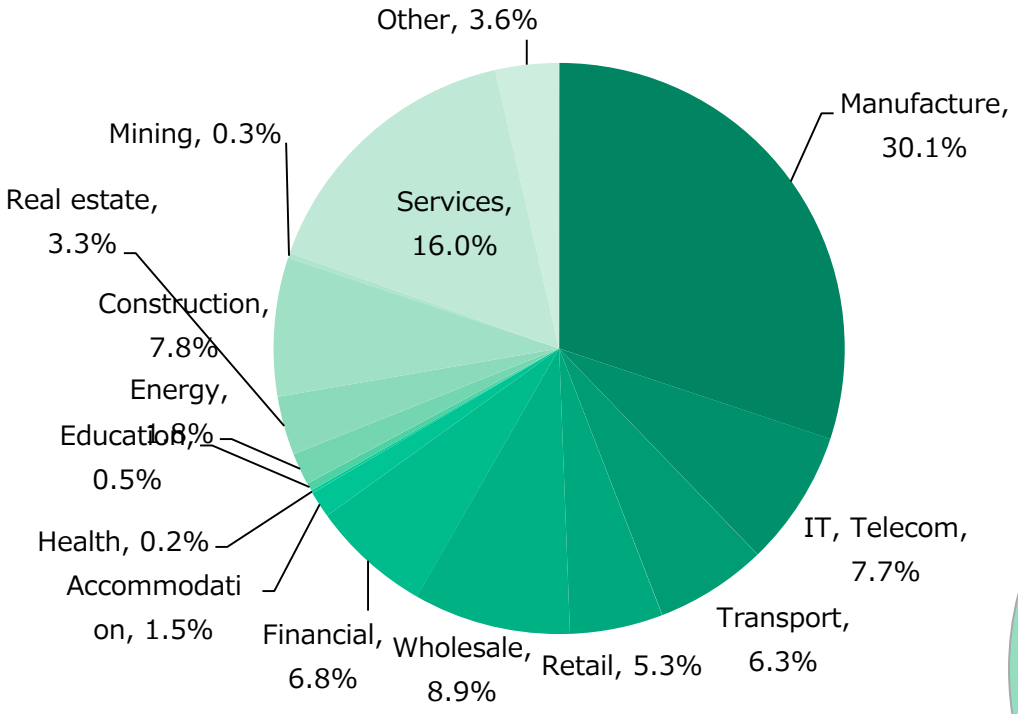
Advancing with you
MS&AD
INSURANCE GROUP

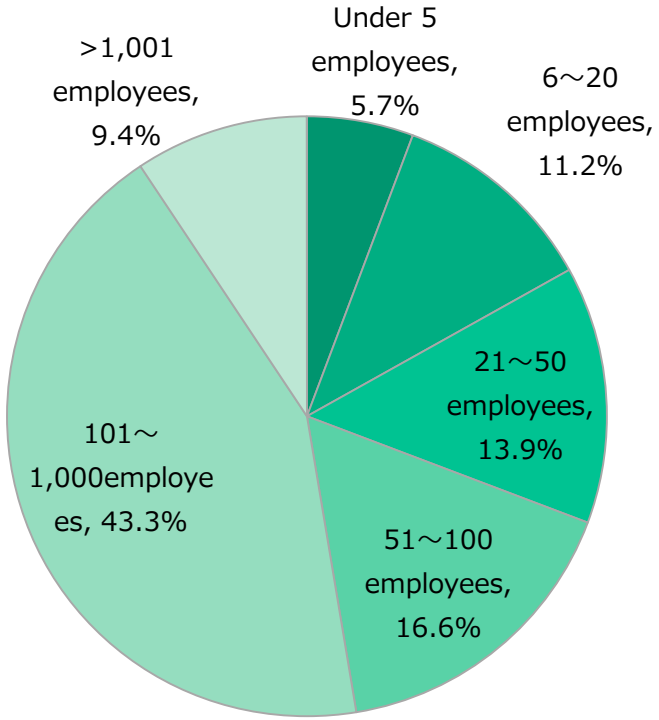
Outline of research

Survey method	Mailing questionnaire (combined with Web response)
Targeted companies	10,000 companies in Japan Extracted from Toyo Keizai Inc.'s "40,000 company data in Japan ((1) Basic data)" Companies that randomly extracted in industry by industry
Number of valid responses	664 (total collected number: 676) Recovery rate 6.6%
Survey period	September 26 - October 12, 2018

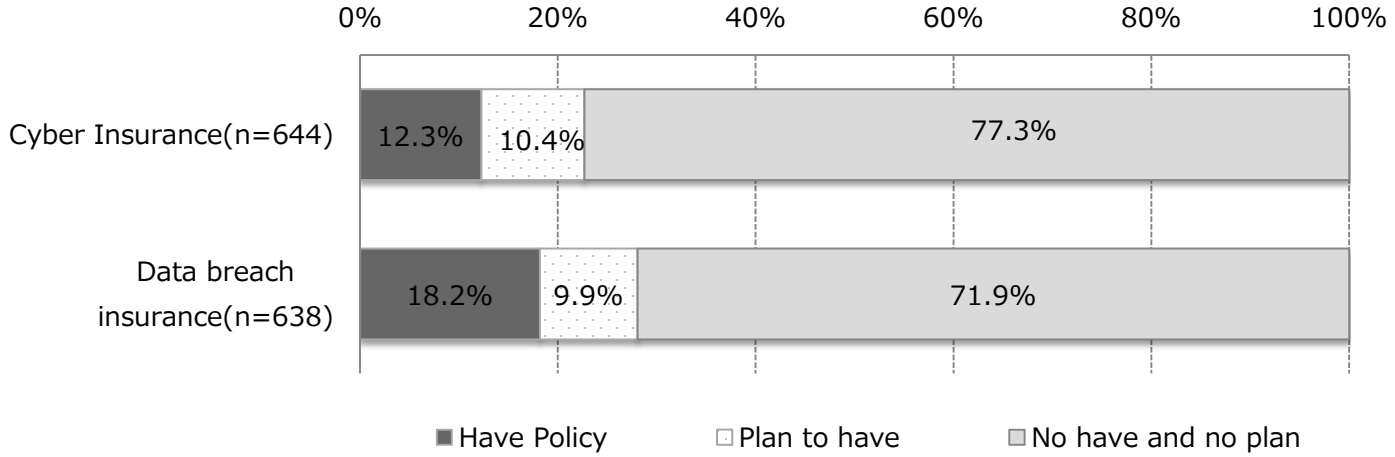
Research of SMB's Cyber Insurance

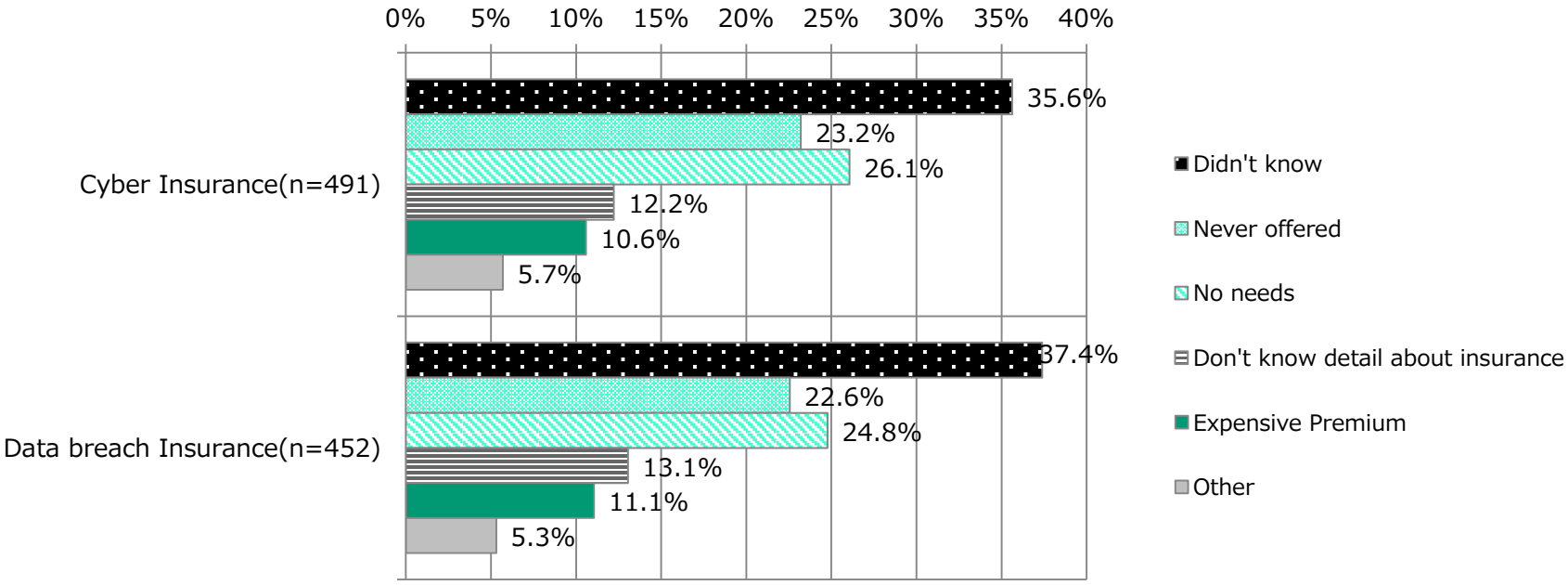
- Outline of researched companies





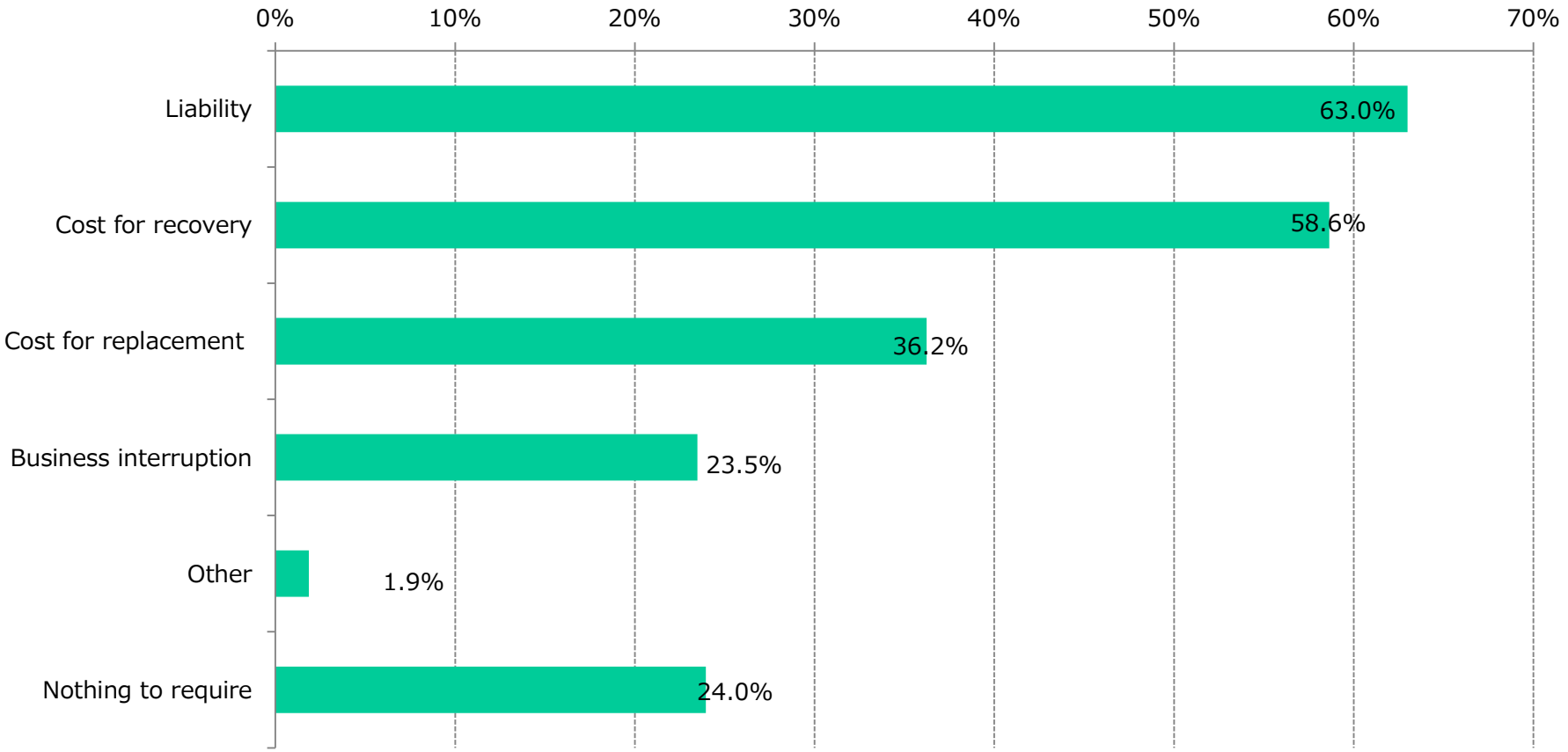
- About Cyber insurance





Research of SMB's Cyber Insurance

- Requirements for insurance cover




THANK YOU

China Cyber Insurance Market Status & Development Strategy

Frank Wang, LLM, CPCU, RPLU, ARe

Speaker Profile

- **Frank Wang, LL.M, CPCU, RPLU, ARe**
- **Casualty Treaty Practice Leader, Gen Re Asia**

- Frank Wang is an Attorney-at-Law and responsible for developing and underwriting casualty treaty portfolios and act as the key advisor on liability insurance/reinsurance and other liability related industry issues. He has more than 13 years liability experience and had worked for a few international leading general insurers before he joined Gen Re in 2013.

- Frank achieved his Bachelor degree in Risk Management and Insurance from Nankai University, Master degree in Insurance Law from East China University of Politics and Law, LL.M degree and Business Law Graduate Certificate from University of Southern California.

- Frank owns several leading professional qualifications including China Legal Professions Qualification, CPCU, RPLU, ARe, ANZIIF Fellow CIP. He is also the CPCU Society International Ambassador and Course Instructor.

- Frank is a regular speaker in Chinese and overseas insurance community and related industries.

Agenda

- China cyber risk profile
- China cyber legal environment
- Cyber insurance market
  - Products
  - Underwriting
  - Prospect and Strategy

Gen Re®

China Cyber Risk Profile

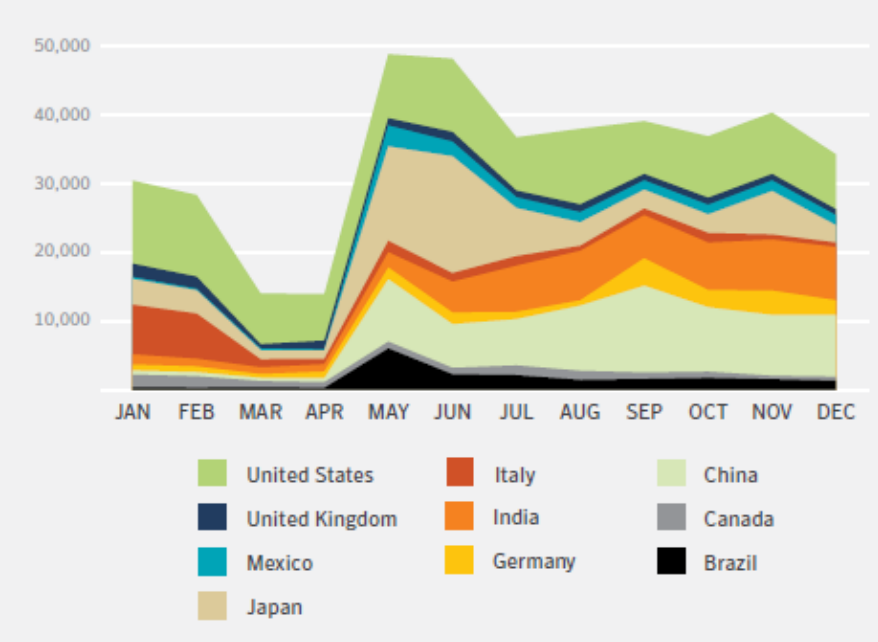
Ransomware activities in 2017

source: Symantec

Ransomware detections by country

Rank	Country	Percent
1	United States	18.2
2	China	12.2
3	Japan	10.7
4	India	8.9
5	Italy	4.1
6	Germany	3.4
7	Brazil	3.1
8	Mexico	2.5
9	United Kingdom	2.3
10	Canada	2.1

Ransomware detections by country by month



Spam activities in 2017

source: Symantec

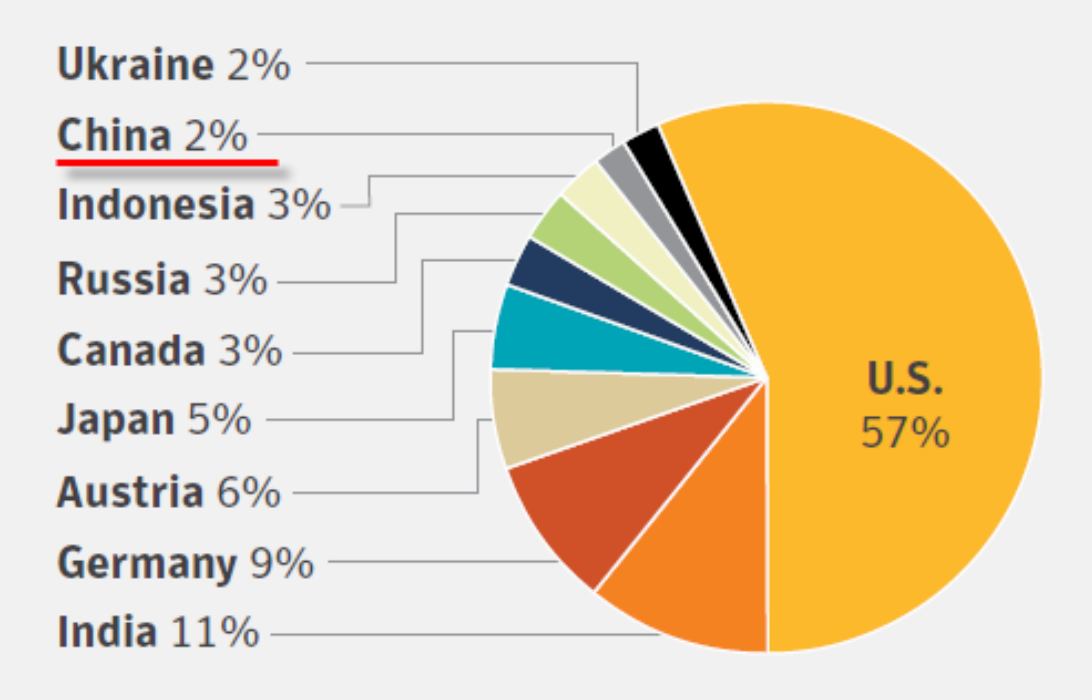
Spam rate by country

Rank	Country	Percent
1	Saudi Arabia	69.9
2	China	68.6
3	Brazil	64.7
4	Sri Lanka	64.6
5	Hungary	60.4
6	Kuwait	59.8
7	Oman	58.9
8	South Africa	57.1
9	Norway	56.9
10	United Arab Emirates	56.3

Mobile malware activities in 2017

source: Symantec

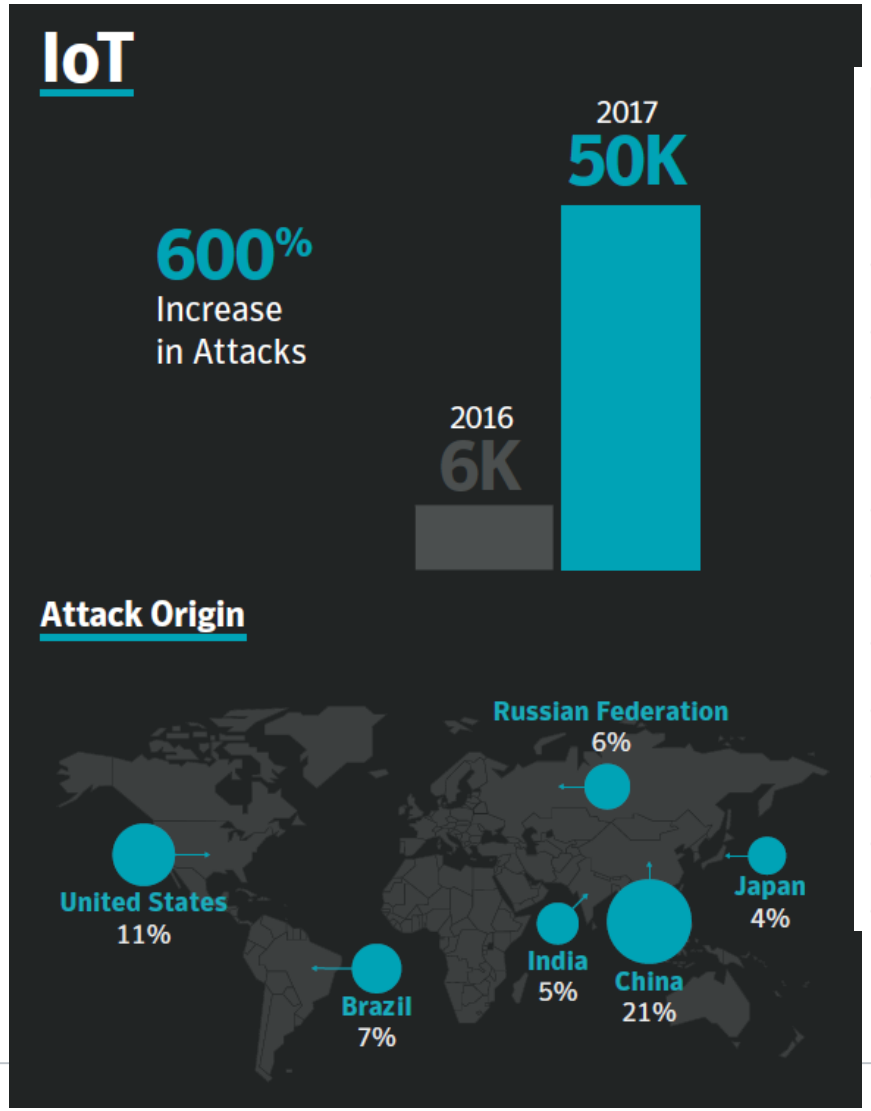
Top 10 list of countries where mobile malware was most frequently blocked in 2017



Internet of Things in 2017

source: Symantec

IoT attacks by source country



Rank	Country	2017 Percent	Country	2016 Percent
1	China	21	China	22.2
2	United States	10.6	United States	18.7
3	Brazil	6.9	Vietnam	6
4	Russian Federation	6.4	Russian Federation	5.5
5	India	5.4	Germany	4.2
6	Japan	4.1	Netherlands	3
7	Turkey	4.1	United Kingdom	2.7
8	Argentina	3.7	France	2.6
9	South Korea	3.6	Ukraine	2.6
10	Mexico	3.5	Argentina	2.5

China Cyber Legal Environment

The PRC Cybersecurity Law

- Took effect on 1 June 2017
- Significance: the first comprehensive privacy and security legislation on cyberspace

- Key Features:
  - Defines obligations of network operators
  - Imposes duties on network operators in relation to network security
  - Establishes rules for the protection of “personal” and “important” information
  - Establishes a framework of security for “Critical Information Infrastructure” (“CII”)
  - Localization. Data collected in the PRC must be stored in the PRC and may not be transferred out of and / or stored outside the jurisdiction.

Mandatory notification for data breach

Article 42 of the new Cybersecurity Law stipulates as follows:

- “Network operators shall adopt technical measures and the other necessary measures to ensure the security of the personal information that they have collected and prevent the information from being leaked, damaged, or lost;
- Under circumstances in which the leakage, damage, or loss of personal information has occurred or might occur, they shall immediately adopt remedial measures and notify users in a timely manner in accordance with the provisions and report to the relevant department in charge.”

First Cyber-Court established on August 16, 2017

China Establishes Its First Cyber-Court in Hangzhou: Thank You Alibaba

By Sara Xia on August 16, 2017

POSTED IN INTERNET, LITIGATION AND ARBITRATION

Cyber Insurance Market

Individual Bank Account Loss Insurance - CPIC

- **Coverage:** bank account loss caused by
  - fraud, embezzlement, copy
  - Forced to disclose the account number and password
  - Account replacement fee can be covered as an extension.

- **Exclusions:**
  - Failure to use the safety protection tools
  - Failure to change the password and notify the bank to block or suspend account after the insured finds the leakage of account information or loss of phones which receive the password.
  - Loss happened 72 hours earlier than the bank account is blocked or suspended.
  - Account manager's own system failure
  - Interests
  - Consequential loss

Individual Bank Account Safety Insurance - CPIC

- **Insured accounts:**
  - Normal bank accounts (debit & credit)
  - Mobile bank account
  - Online bank account
  - Telephone bank account
  - Wechat / Alipay bank account
  - Third party payment accounts

- **Limit of Liability:** RMB30,000 – 880,000
- **Basic rate / premium:** 0.16% / RMB48 – 1,408
- **Minimum charge:** RMB5

Cyber Virtual Property Insurance - PICC

- **Insured property:** account, equipment, tools, game coin of game players
- **Insured peril:** theft or hacking
- Co-developed by PICC and China Online Game Service Alliance
- Distributed purely at online platforms
- **One-key apply and one-key claims**

Mobile Payment Protection Insurance – Baidu & ZhongAn

- First product for mobile payment protection, launched in 2014
- **Insured peril:** financial loss due to malicious deduction or loss of password caused by mobile virus
- **Limit of Liability**: maximum RMB3,000 per loss & RMB100,000 annual aggregate
- Premium paid by Baidu only

Commercial Cyber Insurance in China

- Third Party Coverage:
  - Network security liability
  - Privacy liability
- First Party Coverage:
  - Business Interruption
  - Crisis Management / Remediation
  - Network Extortion
  - Regulatory Defense
  - Digital Asset loss

- Major players: AIG, Allianz, Zurich, Ping An
- Very few buyers such as online platforms, financial institutions, international manufacturers
- Not aware of any big cyber insurance payment

Key concerns for insurers

- Quantifying the risk
- Lack of historical loss data
- Keeping up with technology change & best practices
- Increased dependence on Cloud providers
- Aggregation & Correlation

Key concerns for Reinsurers

- **Reinsurers are concerned with the same issues that worry primary insurers**
- **Aggregation**
  - Potential clash exposure / contagion
  - Cloud exposure
  - Difficult to diversify within a primary portfolio & book of business
    - Reinsurers usually supporting standalone Cyber QS treaties in China
- **Soft market conditions**
  - Pricing adequacy especially for non-proportional reinsurance
  - Extreme competition in excess layers
  - Abundance of capacity
  - Broadening of terms and conditions
- **Underwriting**
  - Keeping up with ever-changing technology
  - 1st Party Coverage
    - 3rd party underwriter underwrites 1st party exposure

Market Prospect and Strategy in China

- Growing awareness of cyber risk contributes to insurance solutions.
- Improving cyber security laws and regulations
- Personal information protection needs to be improved.
- Judicial support shall be strengthened based on the civil liability.
- Cyber risk management resources need to be integrated with insurance solutions.
- Tailor-made cyber insurance products

Reference reading

Frank (Min) Wang, LLM, CPCU, RPLU, ARe

InsurTech | Cyber | Casualty | Financial | Reinsurance | Speaker

Pudongxin District, Shanghai, China

Add profile section | More...

Gen Re

USC Gould School of Law

See contact info

See connections (500+)

Gen Re

NOVEMBER 2017

CASUALTY MATTERS®

Cyber Insurance Ready for Take-Off in China

by Frank Wang, Gen Re, Shanghai

The WannaCry ransomware worm that hit organisations in 150 countries around the world took awareness of cyber risk to a new level in 2017. In China, where computers at nearly 30,000 institutions were infected by the deadly virus, the attack served as a loud wake-up call.

Content

China and the Global Cyber Insurance Market 2

Challenges and Countermeasures 3

Underwriting Cyber Risk 4

Thank You!

Q&A

frank.wang@genre.com

Visit genre.com for more info.

KiRi 보험연구원

한국의 사이버보험 현황 및 정책과제

『4차 산업혁명과 사이버보험』 KIRI 국제심포지엄
2018.11.5(월) 14:00~17:40
중소기업중앙회 제2대회의실

KiRi 보험연구원

목차

I. 기업시장: 보험가입률 제고 방안을 중심으로

II. 가계시장: 보험소비자 설문 조사를 중심으로

III. 공공부문: 위험재무 전략을 중심으로

IV. 종합정리

I. 기업시장: 보험가입률 제고 방안을 중심으로

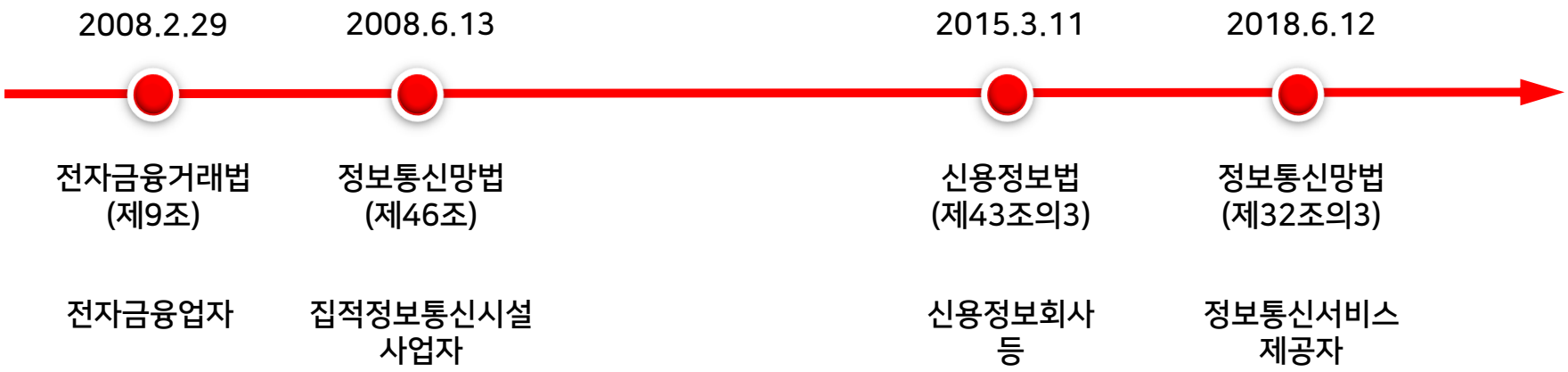
1. 이슈제기
2. 정책현황
3. 주요국의 사이버보험 활성화 전략
4. 홍수보험 사례분석
5. 소결

1. 이슈제기

환경변화	• **초연결사회(Hyper-connected Society)로의 진화**: 사물인터넷(Internet of Things)의 확산과 함께 사이버(Cyber) 세계와 물리적(Physical) 세계가 결합 ⋯› 다양한 산업에서 사물인터넷 도입: 정보기술(Information Technology)과 운영기술(Operational Technology)의 수렴
위험변화	• 개인정보유출에 의한 프라이버시 침해 ⋯› **물리적 피해(physical damage) 수반**(예: 2014년 해커의 우크라이나 발전소 공격 ⋯› 전력중단)
위험재무	• 사이버 사고가 물리적 피해를 수반할 경우 정상적인 영업활동이 어려워 빠른 피해복구가 중요해짐 ⋯› 피해복구 재원조달을 위한 **위험재무(보험 등) 전략의 중요성 증대**
시장현황	• 위험재무 전략 가운데 보험이 효과적인 수단으로 알려져 있기는 하나 사이버보험의 경우 여러 제약요인에 의해 **가입률 저조** ⋯› 보험회사의 경우 재앙적 수준의 손실 가능성에 대한 우려 때문에 보험료를 높게 책정, 보험 가입을 제고하기 위해 정책적으로 보험료를 낮추는 것도 보험제도의 건전성 측면에서 볼 때 부적절
이슈제기	• **보험제도의 건전성도 유지하면서 보험 가입률을 제고할 수 있는 방안**은 무엇인가?: 국내 정책현황을 살펴보고, 사례분석을 통해 시사점 도출

2. 정책현황

- 국내 사이버보험 정책은 제3자(third party) 피해 관련 의무화 도입을 중심으로 이루어져 왔음
- 2008년 전자금융거래법, 2015년 신용정보법, 그리고 2018년 정보통신망법에 의무화 조항 도입



정책이슈	• 향후 의무화만으로는 한계에 부딪힐 경우 어떤 대안들을 생각해볼 수 있는가? ⋯› 동시대 주요국의 사이버보험 정책 사례와 보다 긴 역사를 가진 자연재해보험 관련 정책 사례 분석을 통해 시사점을 도출하고자 함

3. 주요국의 사이버보험 활성화 전략

- 공급측면은 사이버 사고 데이터 집적 및 표준화, 그리고 수요측면 정책은 사이버위험 인식 제고 중심
  - 아직까지는 의무보험이나 보험가입률 제고를 위한 직간접적인 보험료 지원 제도 시행 사례 부재
- 적극적인 정부 개입 관련 시도: 미국의 Data Breach Insurance Act 발의 & 영국의 Insurance Pool 논의

	공급측면	수요측면
미국	‣ 영리사업자인 NetDiligence, Advisen, Insurance Services Office 등에서 사이버 사고 관련 데이터 집적	‣ 2016년 Data Breach Insurance Act 발의: 사이버보험에 가입하고 NIST의 보안 가이드라인 준수 시 보험료의 15% 세액공제
유럽	‣ 유럽 보험협회 Insurance Europe: Template for Data Breach Notifications 마련	‣ 개별 국가의 보험협회를 중심으로 중소기업의 사이버위험 인식 제고를 위해 중소기업협회 등과 함께 홍보활동 전개
일본	‣ 상공회의소를 통해 손해보험회사에 맞춤형 사이버보험 상품개발 의뢰 & 공동 구매	‣ 정부 및 공공사업의 발주 시 업체 선정에 있어서 사이버보험 가입 기업에 가점을 부여하는 방안 검토
중국	‣ 클라우드 서비스 기업, 데이터 복구 서비스 기업과 제휴를 통해 기업성 사이버보험 상품 개발	‣ 온라인 간편결제 서비스 기업과 제휴하여 온라인을 통해 가계성 사이버보험 상품 판매

3.1. EU 사례

네덜란드	‣ 2015년, 네덜란드 보험협회는 중소기업협회와 함께 중소기업의 사이버위험 인식 제고를 위한 로드쇼 추진 ‣ 개인과 기업에 사이버위험 관련 정보를 제공하는 인터넷 포털 구축 ‣ 네덜란드 보험협회 내에 보험회사를 위한 사이버 사고 대응 팀 조직
독일	‣ 2017년 3월, 독일 보험협회는 중소기업 관련 권고 약관(Non-binding Wording for Cyber Insurance) 마련 ‣ 독일 보험협회 부속 표준화 기관은 중소기업을 위한 사이버 보안 가이드라인을 만들어 배포
영국	‣ 2016년 5월, 영국 보험협회는 중소기업을 위한 사이버보험 안내책자 발간 ‣ 로이즈를 중심으로 사이버 사고 시나리오 모델 개발
오스트리아	‣ 오스트리아 보험협회는 사이버보험 관련 권고 약관(Non-binding Model Conditions for Cyber Insurance) 마련 ‣ 2017년, 기업연합회는 중소기업의 사이버위험 및 사이버보험 인식 제고를 위해 로드쇼 기획 ‣ 또한, 중소기업의 사이버 보안 상태를 자가 점검할 수 있는 온라인 테스트 서비스 제공
프랑스	‣ 2016년 10월, 프랑스 보험협회는 사이버위험 및 사이버보험 관련 Think Tank인 “Le Club des Jurites” 설립 ‣ 2017년 5월, 프랑스 보험협회는 중소기업에게 사이버위험에 대한 정보를 제공하기 위해 안내책자 배포 ‣ 2017년 6월, 프랑스 보험협회 부속 표준화 기관인 CNPP는 보안표준인 APSAD D32 발표

3.2. 일본 사례

민간차원	공동가입	• 중소기업 및 자영업자 등은 중앙상공회의소, 지방상공회의소, 각 산업협회, 공제단체, 지역 공동체 등 자사가 소속된 단체를 통해 단체할인 혜택 하에 맞춤형 상품에 가입
	가전회사와의 협력	• 동경해상일동화재보험과 일본 마이크로소프트는 자택 근무 과정 중 발생한 정보 유출 피해를 보장하는 보험상품 개발 ⇢ PC 판매 시에 부가상품으로 사이버보험 판매
	보안업체와의 협력	• MS & AD는 미국의 Verizon Communications와 업무제휴 • 동경해상일동화재보험도 사이버리스크 모델링 전문회사인 미국의 Cyence와 업무제휴
	보안사업 진출	• 손보재팬은 고객에게 사이버보안 관련 종합 서비스를 제공하기 위하여 플랫폼을 구축하고 2017년 1월부터 사이버 보안 사업에 진출
정부차원	기업공시제도	• 일본 총무성은 상장기업을 대상으로 기업통합보고서 또는 유가증권 보고서에 별첨으로 정보보안 보고서를 공시하도록 관련규정의 개정 권고
	보안인증제도	• 정보처리추진기구(IPA)는 중소기업 정보보안 대책 가이드라인 제정: 상세 정보공개로 인증 받은 기업에게 사이버보험 할인 혜택 부여

3.3. 중국 사례

- 중안보험회사는 다음과 같은 이유에서 클라우드 서비스 기업과 협력
- **상품개발**: 협력기업이 사이버보험 상품개발 및 요율 산출에 필요한 데이터 제공
- **고객관리**: 사이버보험 가입자에게 사이버 사고 발생 전후에 부가서비스 제공
- **판매채널**: 협력기업의 고객이 사이버보험의 잠재적인 가입자가 될 수 있어 고객 확보에 유리

클라우드 사이버보험	알리윈과 협력	• 알리윈의 설비 장애로 인한 클라우드 서비스 이용 기업의 영업중단 손실 보장
데이터 사이버보험	알리윈과 협력	• 기본약관: 클라우드 서비스 이용 기업의 데이터 복구 및 고객정보 유출에 따른 배상책임 보장 • 특별약관: 보안 취약점에 따른 손실 및 디도스 공격에 따른 손실 보장
사이버 종합보험	귀신쟈닝과 협력	• 데이터 사이버보험: 데이터 복구 비용 보장 • 클라우드 사이버보험: 데이터 복구 및 고객정보 유출에 따른 배상책임 보장 • 분쟁검증 사이버보험: 인터넷 거래 분쟁에 대한 검증 비용 보장

4. 홍수보험 사례분석

- 사이버보험 활성화와 관련하여 미국에서는 Data Breach Insurance Act가 발의되고, 영국에서는 Insurance Pool 논의가 있었는데, 그러한 논의들은 그 나라들의 홍수보험 정책 역사에서도 찾아볼 수 있음 ⋯› 미국은 재보험풀 도입과 함께 Incentive제도 도입 논의가 있었고, 영국은 재보험풀 도입

미국 홍수보험 정책사례

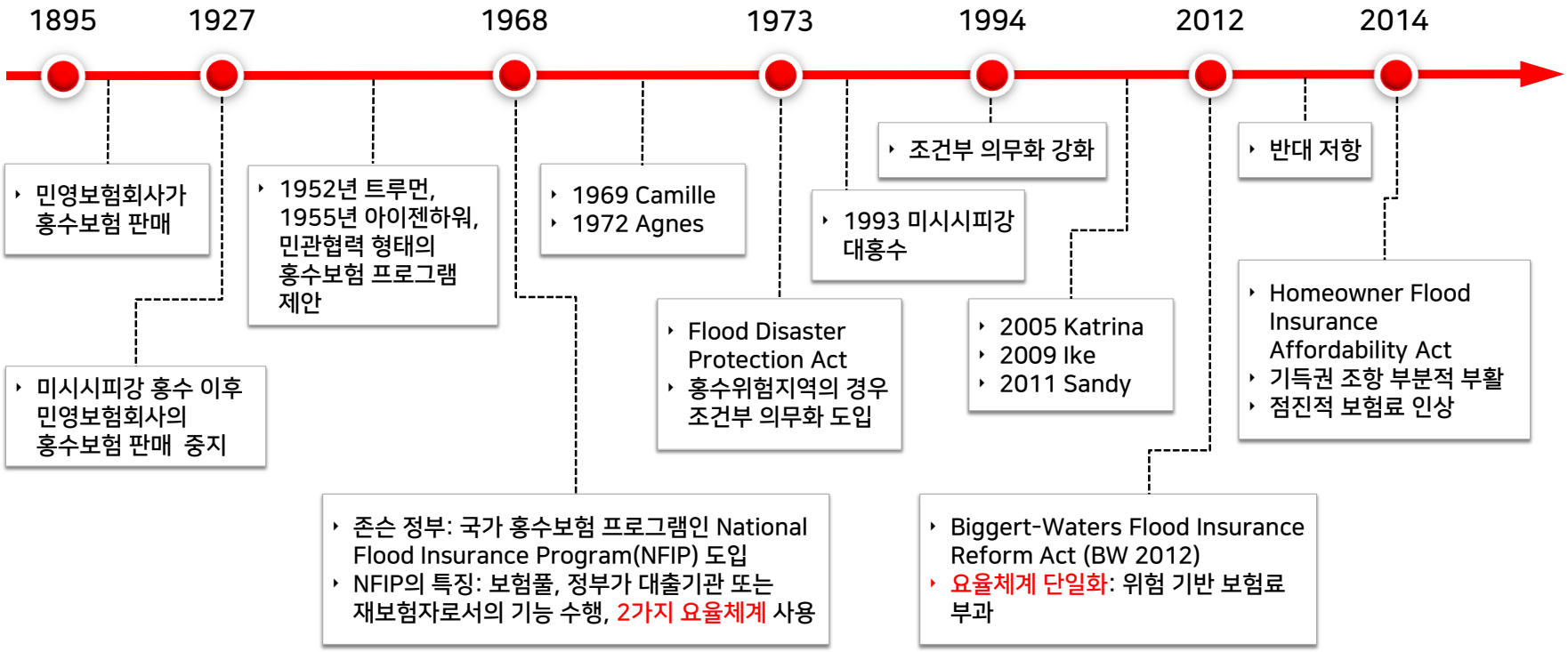
- 홍수보험시장에서 민영보험회사가 철수한 이후 국가 홍수보험 프로그램 도입
- 보험가입률 제고를 위해 고위험 지역에 대해서는 위험수준에 상응하는 보험료 수준보다 낮은 수준의 보험료 부과
- 국가 홍수보험 프로그램이 재정적으로 위기를 맞으면서 Risk-based Premium 도입 논의
- 위험 기반 보험료 부과 시 예상되는 보험가입률 감소 문제에 대한 대책도 함께 연구(13번 슬라이드 참조)

영국 홍수보험 정책사례

- 공적 홍수보험 프로그램을 도입한 미국과 달리 정부와 보험산업간 협상을 통해 민영보험회사가 보험공급
- 협상내용: 정부가 적극적으로 홍수위험 방지 인프라를 구축한다는 조건 하에 보험산업이 적극적으로 홍수보험 판매
- 최근(2016년) 근본적인 문제 해결 방안으로 재보험풀인 Flood Re 탄생: 고위험 가구에 위험에 상응하는 수준보다 낮은 보험료로 홍수보험 공급

4.1. 미국의 홍수보험 정책사례

- 미국 홍수보험 관련 정책의 역사는 **보험가입률 제고**와 **보험제도의 건전성**이라고 하는 두 개의 정책목표간 상충의 역사
  - Dilemma: 보험 가입률 제고를 위해서는 보험료 인하, but 보험제도의 건전성을 위해서는 보험료 인상 필요



4.1. 미국의 홍수보험 정책사례

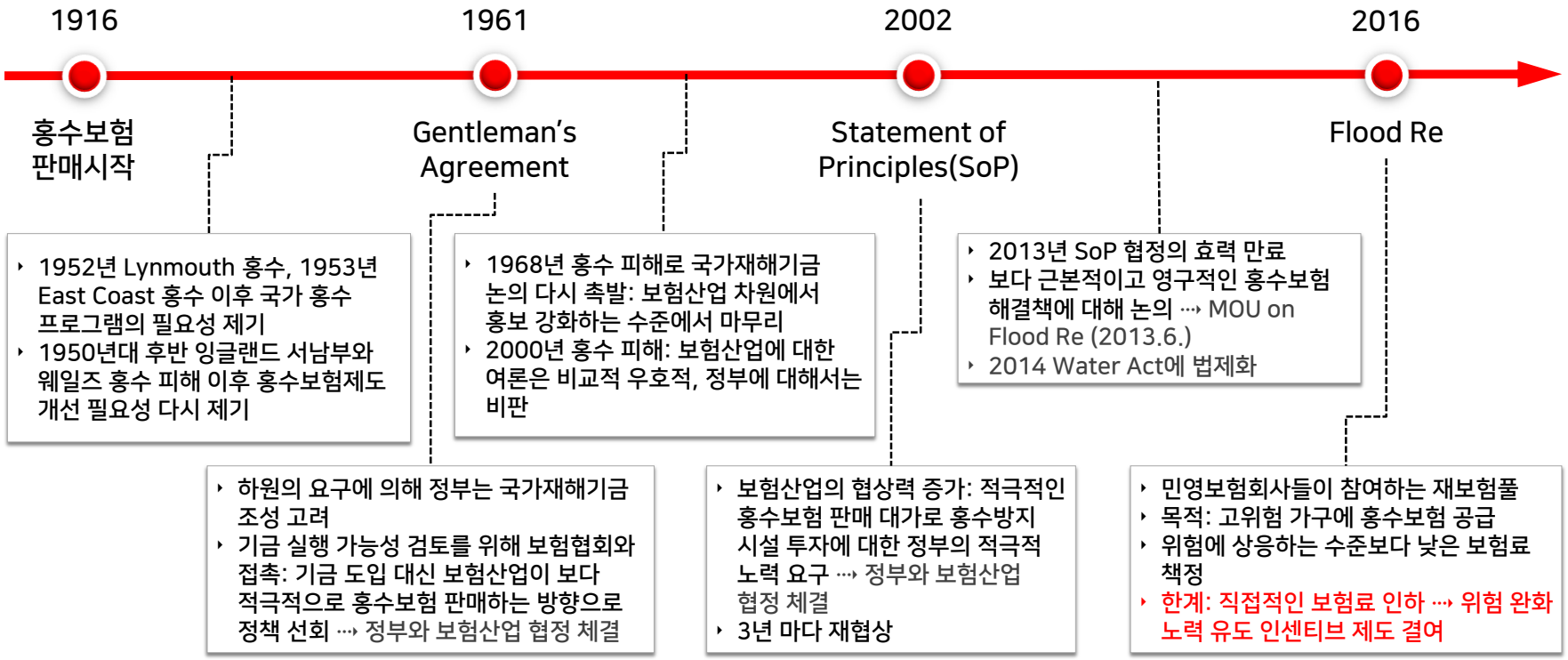
- 위험기반 요율 도입 시 예상되는 문제점: 보험 가입률 감소 ⋯› 이러한 문제점의 해결을 위해 의회와 Federal Emergency Management Agency는 National Research Council에 연구 의뢰

1	Mitigation Loan	• 홍수 대비 시설에 투자하는 경우 정책금융을 통해 장기 저리 대출 ⋯› 홍수 대비 시설 투자 시 위험 감소로 보험료 인하 효과 발생
2	Voucher	• 위험 기반 요율 적용 시 보험료가 급격히 상승하게 되는 가구를 대상으로 바우처 발급 ⋯› 바우처는 보험료 납부나 홍수 대비 시설 투자의 대출금 상환에 사용
3	Tax Incentives	• 개인 또는 근로자수가 50인 이하인 소기업이 일정조건 (홍수보험 가입, 홍수 대비 시설 투자를 위한 지출 등)을 충족하는 경우 세액공제 혜택 부여
4	Disaster Savings Account	• 소득공제 혜택을 받을 수 있는 재해저축계좌 도입 ⋯› 재해저축계좌의 자금을 홍수보험의 자기부담금 이하의 비용 지출에 사용, 자기부담금 수준 인상을 통해 보험료 인하 효과 발생

핵심특징	• 직접적인 보험료 감면이 아닌 간접적인 보험료 감면: 인센티브 제도를 통해 위험방지 시설에 대한 투자 유도 ⋯› 사이버위험 감소 ⋯› 보험료 인하 ⋯› 사이버보험 수요 증가

4.2. 영국의 홍수보험 정책사례

- 영국의 경우에도 미국과 마찬가지로 **보험가입률 제고**와 **보험제도의 건전성**간 상충의 역사
- 그러나 미국과 다른 점은 홍수보험은 정부의 영역이라기 보다는 민간이 담당해야 할 영역으로 생각 ⋯› 민영보험회사 중심으로 보험 공급



5. 소결

Revisited Issue	• 사이버보험의 경우 공급측면과 수요측면 요인에 의해 **가입률 저조 ⋯› 보험제도의 건전성도 유지하면서 보험 가입률을 제고할 수 있는 방안**은 무엇인가?
정책현황	• 현재는 의무화 대상을 확대하는 방향으로 보험가입률 제고 도모 ⋯› 제3자 피해보상 재원 마련에 초점
향후정책	• 향후 시장상황의 변화 등으로 인해 의무화만으로는 한계에 부딪힐 경우 재보험풀이나 인센티브 제도 도입과 같은 대안들을 생각해볼 수 있음

Ⅱ. 가계시장: 보험소비자 설문 조사를 중심으로

1. 이슈제기
2. 사이버위험에 대한 주관적 인식
3. 사이버보험 상품판매 인지도
4. 사이버보험 수용도
5. 소결

1. 이슈제기

- 향후 가계성 사이버보험 시장의 성장이 예상되고 있으나 아직은 관련 국내연구가 활발하지 않은 상황: 기초적인 연구결과 조차도 부재
- 본 자료에서는 개인의 사이버위험 인식 및 사이버보험 상품에 대한 수용도 조사 결과 소개: 사이버위험 가운데 사이버 금융범죄와 사이버 명예훼손에 대해 조사

사고 동향

(단위: 건)

		사이버 금융범죄	사이버 명예훼손
2015년	발생	14,686	15,043
	검거	7,886	10,202
2016년	발생	6,721	14,908
	검거	4,034	10,539
2017년	발생	6,066	13,348
	검거	2,632	9,756

자료: 경찰청 사이버안전국

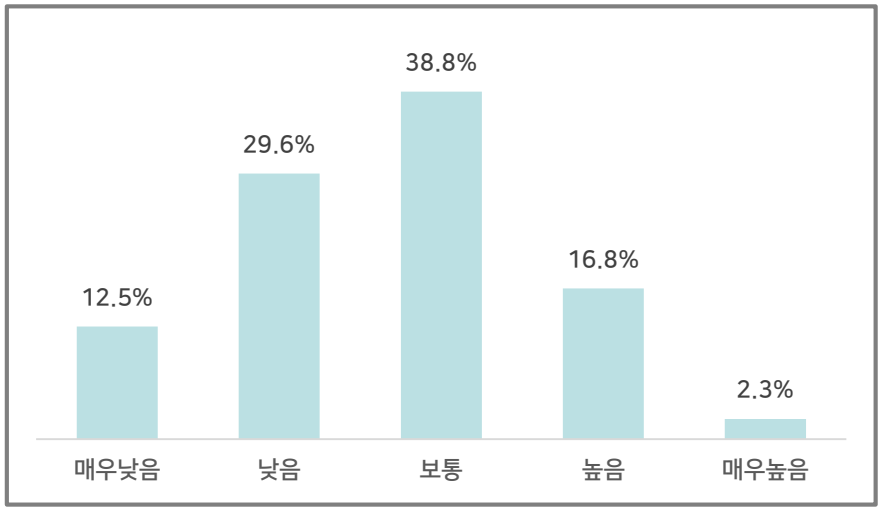
상품 현황

사이버 금융범죄	• 담보: 법률상담비용, 소송비용, 금전손실, 일실소득 및 기타 비용 등
사이버 명예훼손	• 피보험자가 보험기간 중에 발생한 사이버 명예훼손 사건의 피해자가 되어 수사기관에 신고, 고소, 고발 등이 접수되고 피의자에 대해 검찰의 기소처분결정이 내려진 경우 보험금 지급
판매형태	• 대부분 특약 형태로 판매되고 있음 ⋯› 단독형의 경우 수수료 문제로 인해 설계사 채널을 통해 판매하기는 어려움

2. 사이버위험에 대한 주관적 인식

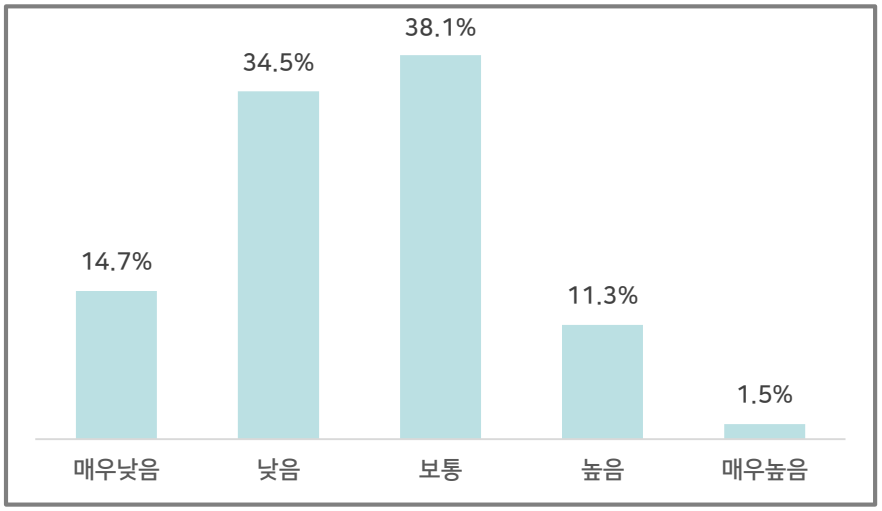
- 사이버 사고를 당할 가능성이 낮다고 생각하는 응답자가 사고를 당할 가능성이 높다고 생각하는 응답자보다 많음
  - 사이버 금융범죄: 매우 낮음 또는 낮음의 응답자 비중은 약 42.1%, 높음 또는 매우 높음의 응답자 비중은 약 19.1%
  - 사이버 명예훼손: 매우 낮음 또는 낮음의 응답자 비중은 약 49.2%, 높음 또는 매우 높음의 응답자 비중은 약 12.8%

사이버 금융범죄 피해 가능성



주: 조사대상자 수는 2,440명
자료: 보험소비자 설문조사(2018)

사이버 명예훼손 피해 가능성

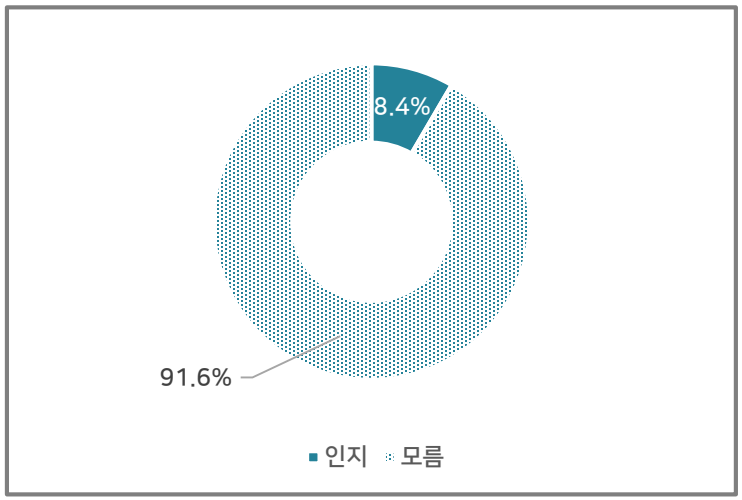


주: 조사대상자 수는 2,440명
자료: 보험소비자 설문조사(2018)

3. 사이버보험 상품판매 인지도

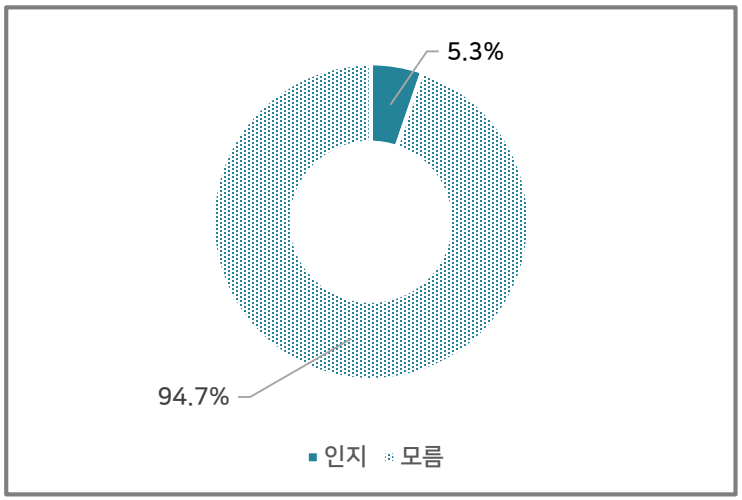
- 조사 대상자 가운데 현재 사이버보험에 가입해 있지 않은 사람들의 경우, 90% 이상이 관련 보험상품의 판매사실을 인지하지 못하고 있었음
  - 사이버 금융범죄 관련 보험상품: 응답자의 약 8.4%만이 판매사실에 대해 인지하고 있었음
  - 사이버 명예훼손 관련 보험상품: 응답자의 약 5.3%만이 판매사실에 대해 인지하고 있었음

사이버 금융범죄



주: 현재 사이버 금융범죄 관련 보험상품에 가입하지 않은 2,429명을 대상으로 조사
자료: 보험소비자 설문조사(2018)

사이버 명예훼손

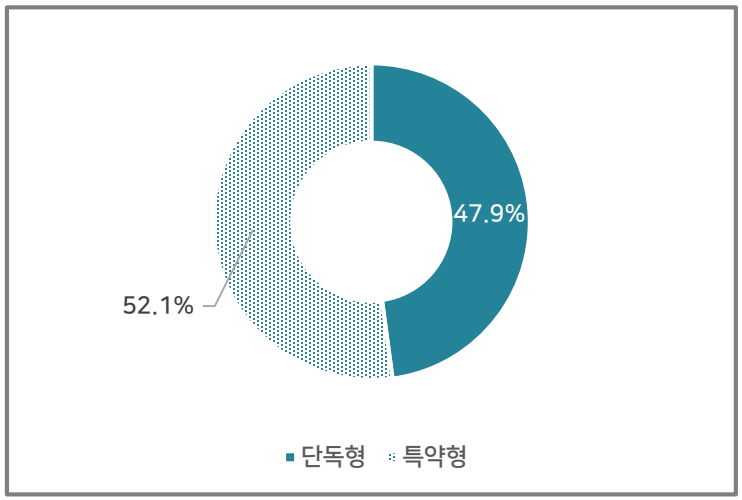


주: 현재 사이버 명예훼손 관련 보험상품에 가입하지 않은 2,435명을 대상으로 조사
자료: 보험소비자 설문조사(2018)

4. 사이버보험 수용도

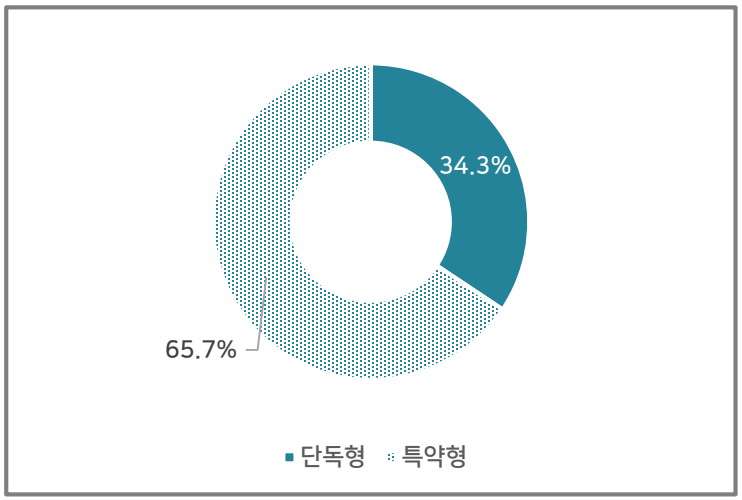
- 가계성 사이버보험 가입 의향이 있는 사람들을 대상으로 구입 형태에 대해 조사한 결과, 단독형 상품에 대한 수요가 적지 않게 존재
  - 사이버 금융범죄 관련 보험상품에 대한 수용도: 응답자의 약 47.9%가 단독형 선호
  - 사이버 명예훼손 관련 보험상품에 대한 수용도: 응답자의 약 34.3%가 단독형 선호

사이버 금융범죄



주: 사이버 금융범죄 관련 보험상품 구입의향이 있는 211명을 대상으로 조사
자료: 보험소비자 설문조사(2018)

사이버 명예훼손



주: 사이버 명예훼손 관련 보험상품 구입의향이 있는 99명을 대상으로 조사
자료: 보험소비자 설문조사(2018)

5. 소결

판매전략

- 단독형 가계성 사이버보험의 경우 주상품(primary products)의 부가상품(add on)으로 판매하는 것이 하나의 판매전략이 될 수 있음
- 예를 들어, 웨어러블 디바이스(wearable device) 판매 시 사이버보험도 함께 판매

정책이슈

- 부가상품 형태로 사이버보험을 판매할 경우 소비자가 인식하지 못한 상태에서 보험에 가입되는 등의 소비자보호 이슈 발생 가능
- 부가상품에 대한 투명한 정보제공 등의 소비자보호 장치 마련 필요

향후 연구과제

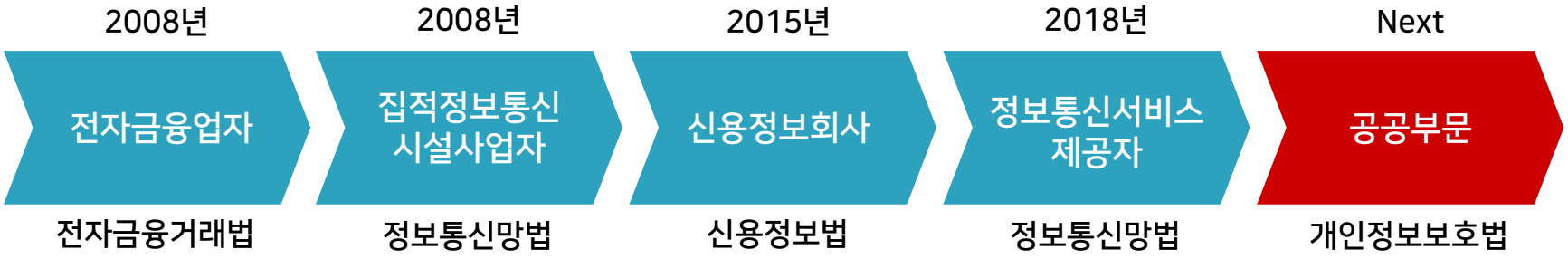
- IoT의 발전과 함께 예상되는 사이버 사고: 웨어러블 디바이스(wearable device) 사용 과정에서의 개인 건강정보 유출, 스마트 홈(Smart Home) 관련된 사이버 사고
- 가계성 사이버보험 or 기업성 사이버보험?

III. 공공부문: 위험재무 전략을 중심으로

1. 이슈제기
2. 빅데이터 시대 정보보호 규제체계
3. 공공데이터 개방정책
4. 위험재무 전략
5. 소결

1. 이슈제기

- 기업 이외의 대량의 데이터 보유주체: 공공부문 ⋯› 공공부문에 있어서는 정보유출 등 사이버위험의 중요성이 다른 위험에 비해 특별한 의미를 가짐 ⋯› 공공부문을 별도 연구분야의 하나로 다룸
- 기존 선행연구 등에서는 공공부문의 위험재무 전략과 관련하여 의무보험 도입 주장 ⋯› 우리나라의 경우 의무화 대상을 확대하는 방향의 정책을 추진, 공공부문의 경우에도 다른 경제주체와 동일한 차원에서 접근



이슈제기	• 공공부문의 경우 의무화 도입 이외에 다른 대안은 없을까? ⋯› 기존 선행연구와는 다른 관점에서 접근함으로써 차별적인 시사점을 도출하고자 함

2. 빅데이터 시대 정보보호 규제체계

현행 규제체계

- 핵심원칙: 개인의 자기결정권 ⋯› 자신의 개인정보를 제공할 것인지, 제공한다면 누구에 의해 어떻게 사용하도록 할 것인지에 대한 결정권을 개인에게 부여
- 개인의 자기결정권 원칙이 실제적인 제도로 구현된 형태 ⋯› 통지와 동의(notice and consent)
- 암묵적인 규제 목적: 위험 zero ⋯› 정보활용에 소극적

- 현행 규제체계 하에서는 빅데이터의 혁신적인 활용을 통한 부가가치 창출에 있어서 근본적인 한계 존재

빅데이터 시대 규제체계

- CIPL은 빅데이터 시대 정보보호 원칙으로 다음 3가지 제시
- 첫째, 정보사용자의 책임 강화
- 둘째, 일정 수준의 위험은 수용하면서 위험 관리 ⋯› 사고 발생 시 피해복구를 위한 위험재무(risk financing, 보험 등) 전략 중요
- 셋째, 개인정보의 정의 등 기존 원칙의 재해석

- Center for Information Policy Leadership's White Paper: Three Solutions for Protecting Privacy In a World of Big Data
- Paper1: The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Information Society (2015)
- Paper2: The Role of Risk Management (2016)
- Paper3: Reinvigorating Privacy Principles (forthcoming)

3. 공공데이터 개방정책

- 공공부문의 경우 대량의 데이터를 보유하고 있으나 혁신적인 활용에 있어서는 미흡했다는 비판이 제기되면서 민간에 개방하자는 Open Government Data 운동이 2009년 미국에서 시작되어 전세계로 확대
- 국내에서도 2013년 '정부3.0'이라는 타이틀 아래 공공데이터 개방 운동 추진

정책평가	• 그 동안 개방에만 초점이 맞추어져 있었으며, 사고가 발생 시 피해구제 재원을 조달을 어떤 방식으로 할 것인지에 대한 위험재무(Risk Financing) 전략은 미흡

4. 위험재무 전략

- 빅데이터 시대 데이터 기반 혁신(Data-driven Innovation)을 촉진하기 위해서는 공공부문의 보다 적극적인 개방정책이 필요 ⋯› 공공부문의 위험재무 전략을 어떻게 가져가야 하나?
- 민영보험회사로의 위험전가가 어려울 경우 공공부문이 적극적인 위험재무 전략을 통해 보유: 자가보험(Captive Insurance)과 정부지원 재보험풀(Government-backed Reinsurance Pool) 모델

자가보험

- 자가보험은 위험보유(Risk Retention)의 한 형태로 시장에서 적절한 보험회사를 찾기 어려울 경우 위험을 인수할 보험회사를 자회사 형태로 직접 설립하는 위험재무 전략
- 1980년대 중반 미국에서 배상책임보험 위기 발생 ⋯› 지자체, 항공, 의료 분야의 경우 보험가입이 어려워졌음 ⋯› 항공 자가보험, 의료 자가보험 등 산업별 그룹 자가보험을 만들어 대처하였음
- 적용: 국가중점 데이터의 소관부처들이 그룹 자가보험을 만들어 운영하는 방안을 생각해볼 수 있음

정부지원 재보험풀: 영국 Pool Re 사례

- Pool Re는 1993년 영국의 손해보험회사와 로이즈가 출자해서 만든 테러위험 관련 Mutual Reinsurer
- 탄생배경: 1990년대 초 원수보험회사와 재보험회사들은 엄청난 규모의 잠재적 피해 가능성과 미래 손실에 대한 신뢰할만한 추정 방법의 부재로 인해 테러위험 보장 중단 고려 ⋯› 대안으로 민관협력 모델인 Pool Re 도입
- 구조: 피해규모가 1.5억 파운드까지는 Pool Re 참여 보험회사들이 부담, 1.5억을 초과해서 80억 파운드까지는 Pool Re와 민간 재보험사 부담, 그 이상은 정부가 부담

5. 소결

Revisited Issue	• 기존 선행연구의 경우 공공부문의 위험재무 전략 대안 가운데 하나로 **의무화** 거론 ⋯› 다른 대안으로는 어떤 것들을 생각해볼 수 있을까?
다른 관점	• 데이터 기반 혁신을 촉진하기 위해서는 공공데이터의 적극적 개방 필요 ⋯› 예를 들어, 의료 관련 공공데이터를 보다 적극적으로 공개하기 위해서는 어떤 위험재무 전략이 필요한가?
대안	• 민영보험회사로의 위험전가가 어려울 경우 공공부문이 적극적으로 위험 보유 ⋯› 자가보험과 정부지원 재보험풀 등을 대안으로 생각해볼 수 있음

Ⅳ. 종합정리

종합정리

		현황 및 문제점	정책과제
1	기업시장	• 수요측면 및 공급측면 등의 여러 제약요인에 의해 사이버보험 가입률이 저조한 상황 • 낮은 보험가입률 문제에 대한 대책으로 의무화 도입 및 대상 확대: 제3자(Third-party) 피해구제에 초점	• 향후 시장상황 변화 등으로 인해 의무화가 한계에 부딪힐 경우, 재보험풀이나 인센티브 제도 도입 등을 대안으로 검토 필요
2	가계시장	• 보험소비자 설문조사(2018) 결과에 의하면, 첫째, 가계성 사이버보험의 판매사실을 인지하고 있는 응답자가 소수 • 둘째, 판매사실을 모르고 있던 응답자 가운데 일부는 보험가입 의사를 밝혀 잠재수요 확인 • 셋째, 현재는 주로 특약형으로 판매하는데, 단독형 수요 존재	• 판매전략: 단독형 상품의 경우 IoT 업체 등과의 제휴에 의해 부가(add on) 상품으로 판매 • 부가상품으로 판매할 경우 소비자보호 장치 보완 필요
3	공공부문	• 공공부문은 4차 산업혁명 시대 핵심자원의 하나로 부상하고 있는 데이터의 보고 가운데 하나 • 그 동안 정부는 공공데이터 개방 확대 및 고도화, 데이터 활용 관련 규제 혁신 등의 정책 발표 • 그러나 피해 발생 시 보상과 관련된 위험재무 전략 미흡	• 빅데이터 시대 데이터 기반 혁신을 촉진하기 위해서는 적극적인 공공데이터 개방 필요 ⋯› 위험을 민영보험회사에 전가하기 어려운 경우 공공부문 보유 방안 검토

감사합니다