APRIA
Asia-Pacific Risk and Insurance Association

POZNAŃ UNIVERSITY OF ECONOMICS AND BUSINESS

ST. JOHN'S UNIVERSITY
School of Risk Management, Insurance and Actuarial Science
The Center for the Study of Insurance Regulation

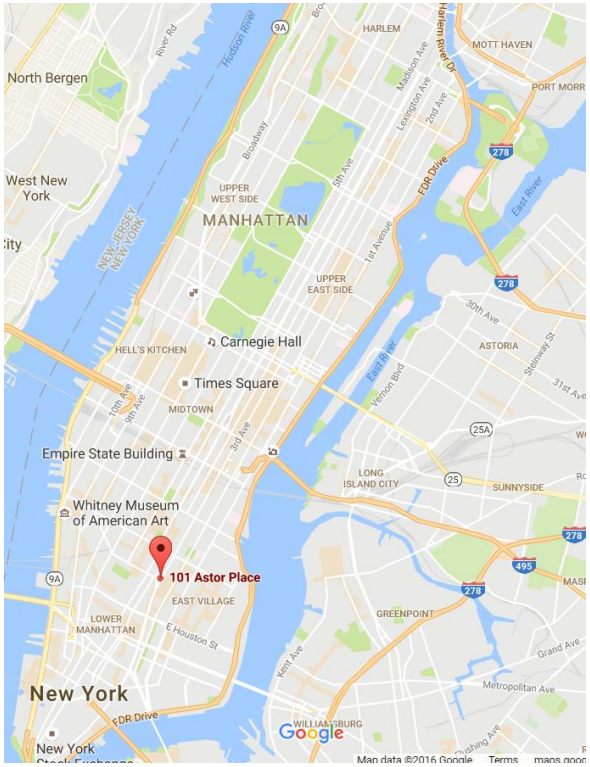
Cyber Security, Risk and Insurance: Insurers' and Consumers' Perspectives

W. Jean Kwon, Ph.D., CPCU

Edwin A.G. Manton Chair Professor in International Insurance and Risk Management
School of Risk Management,
St. John's University, New York

KwonW@stjohns.edu

The College of Insurance
(1902 – 2001)



Świętojański Uniwersytet

The School of Risk Management
St. John's University
(2001 ~)

School of Risk Management
St. John's University

- Undergraduate/master degrees
  - Actuarial Science
  - Risk Management and Insurance
- World's largest insurance library
- Center for the Study of Insurance Regulation

  October 19, 2017 at the Havard Club, Manhattan
- International Insurance Society
  - The Insurance Hall of Fame

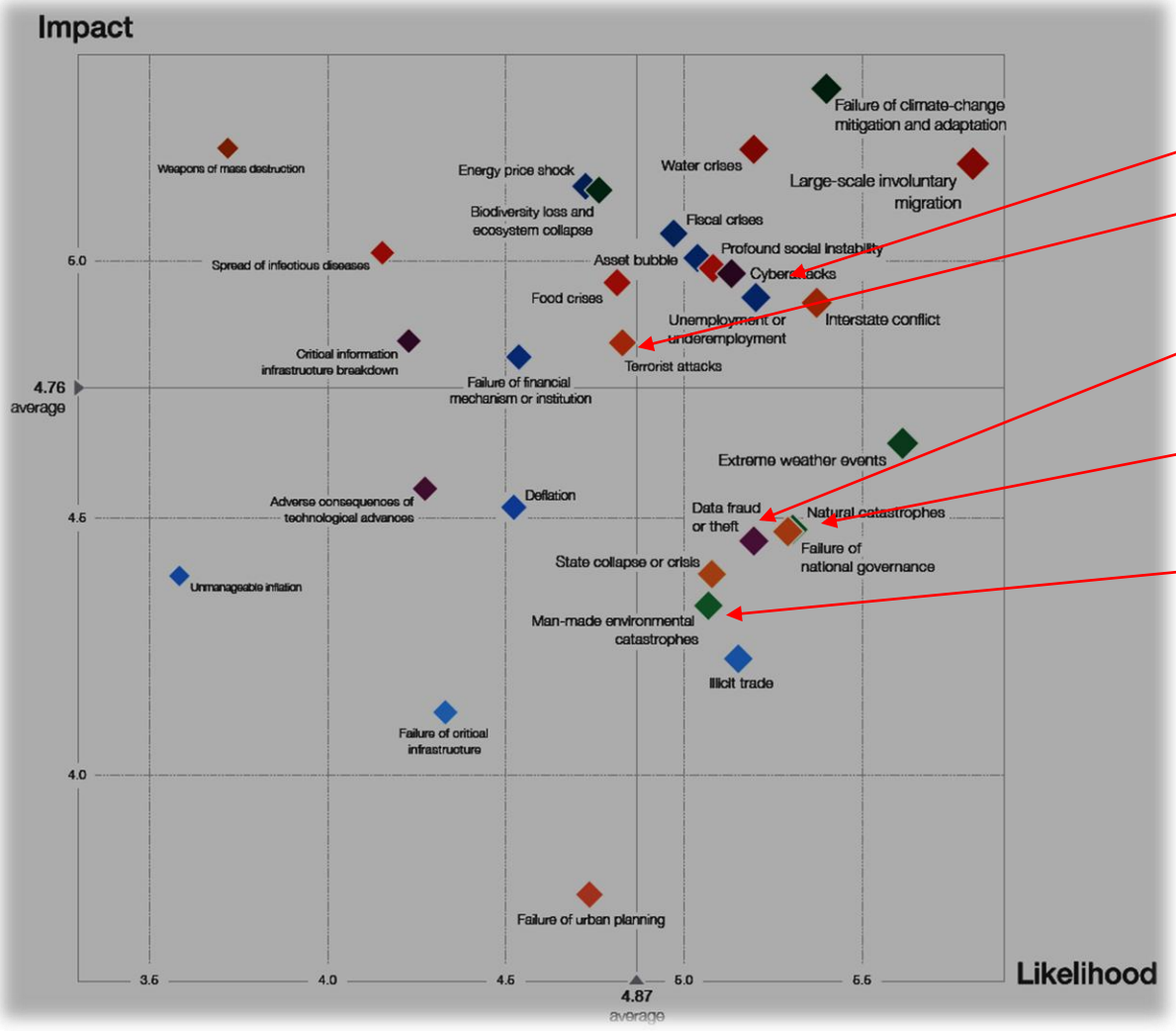
  The Research Network (20+ Research Centers Globally

Cyber Risk

- Usually affects an individual unit in society
- Potential to become a catastrophic loss, affecting a group of the units that are
  - Related as in a chain of production/service or as clients of a financial services institution
  - Unrelated but as users of a cyber-attacked communication hub
- Threat caused by
  - A third party
  - An internal person (for example, employee)

Global Risk Landscape 2016

World Risk Forum



Cyber attacks

Terrorist attacks

Data fraud/theft

Natural catastrophes

Man-made environmental catastrophes

Most Likely Global Risks 2016: A Regional Perspective

Cyber attacks (North America)

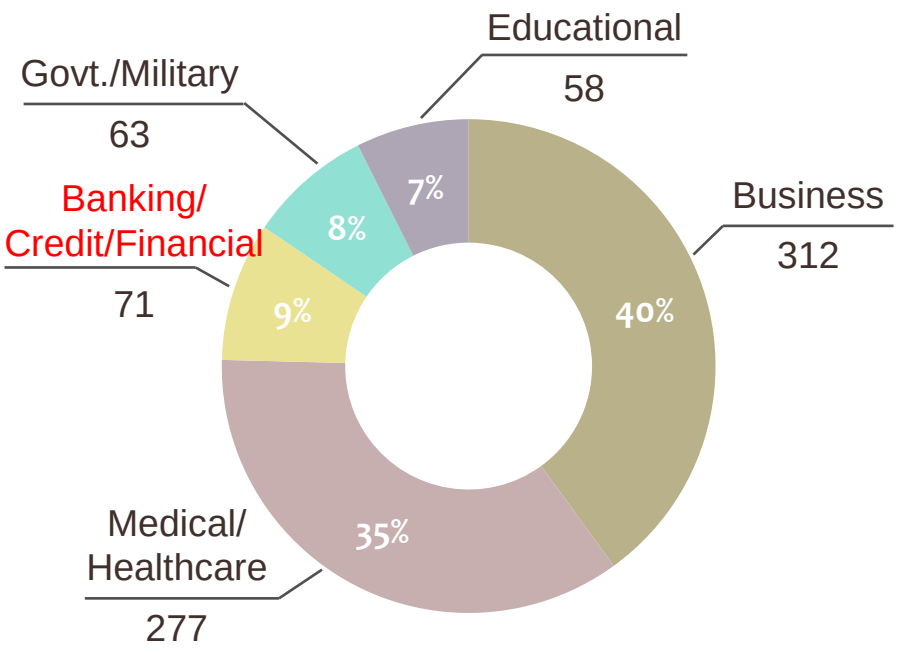
Natural catastrophes (Japan)

Global Risks Perception Survey (2015); quoted in World Economic Forum (2016)

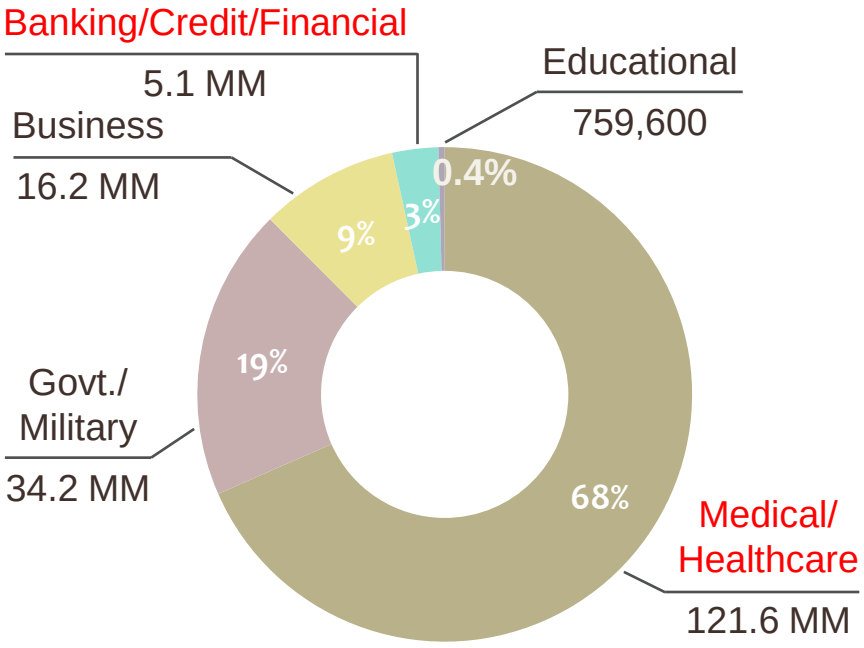
Who Gets Attacked the Most?

Identity Theft Resource Center (2016)

2015 Data Breaches by Business Category, by Number of Breaches



Medical and Healthcare Records Were More Than Half of All Records Stolen

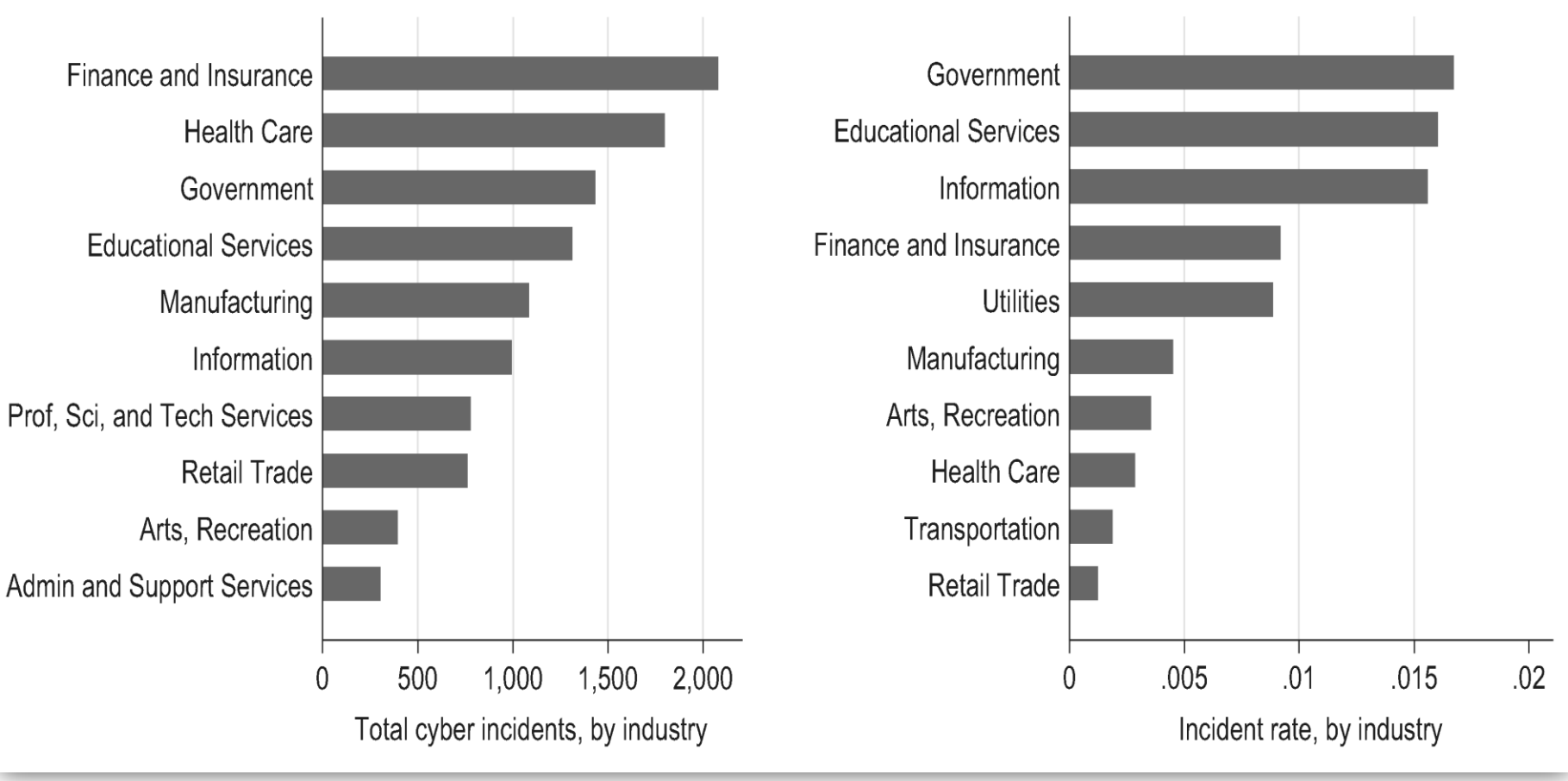


Total may not equal 100% due to rounding.

III (2016) and Identity Theft Resource Center

Who Gets Attacked the Most?

Romanosky (2016) Using Advisen Data



Romanosky (2016), "Examining the costs and causes of cyber incidents", Journal of Cybersecurity, 2 (2): 121-135.

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).

Data Protection and Privacy Laws

UNCTAD Global Cyberlaw Tracker (December 2016)

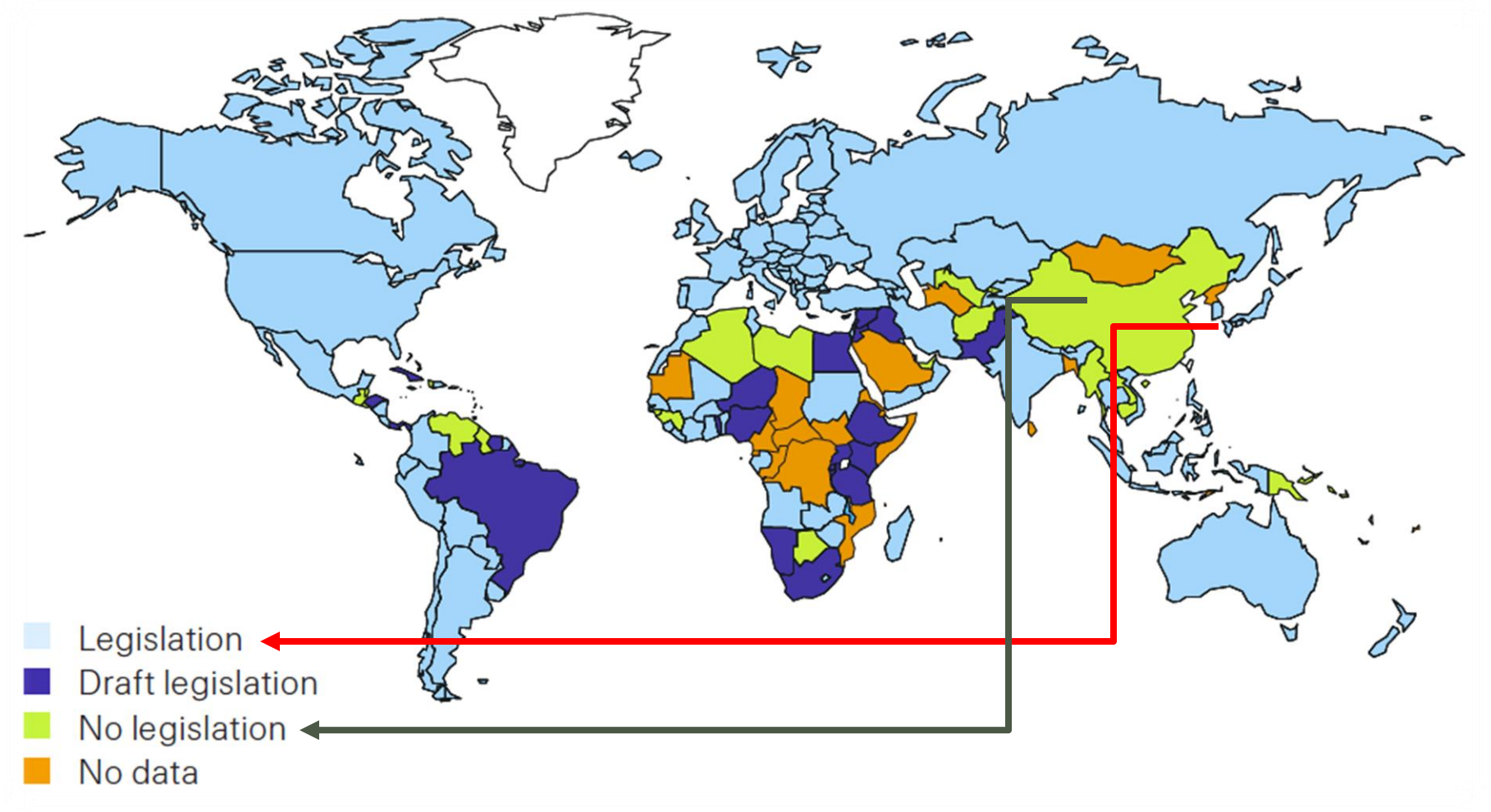


Figure by Swiss Re (2017).

Data Protection Laws

The European Union

- General Data Protection Regulation (GDPR, EU 2016/679)
  - Currently in the transition period for regulated firms
  - Expected to be in place in May 2018 by replacing the Data Protection Directive (Directive 95/46/EC)
  - Fines up to €10 million or up to 2% (or up to €20 million or up to 4% depending of the specific violation) of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater
  - Does not cover the handling of personal data in the insurance industry

The United States

New York Department of Financial Services - Cybersecurity Rule (2/2017)

- Robust cybersecurity program
  - Adequately funded and staffed, overseen by qualified management, and reported on periodically to the most senior governing body of the organization
- Risk-based minimum standards for technology systems
  - Access controls, data protection including encryption and penetration testing
- Required minimum standards to help address any cyber breaches
  - Incident response plan, preservation of data to respond to such breaches and notice to NYDFS of material events, including the events experienced by third party vendors
- Accountability
  - Identification and documentation of material deficiencies, remediation plans and annual certifications of regulatory compliance to NY Department of Financial Services

$25Billion

$50Billion

Lloyd's says cyber-attack could cost $120bn, same as Hurricane Katrina

Monday 17 July 2017 0

Lloyd's of London has warned that a serious cyber-attack could cost the global economy more than $120bn (£92bn) - as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy.

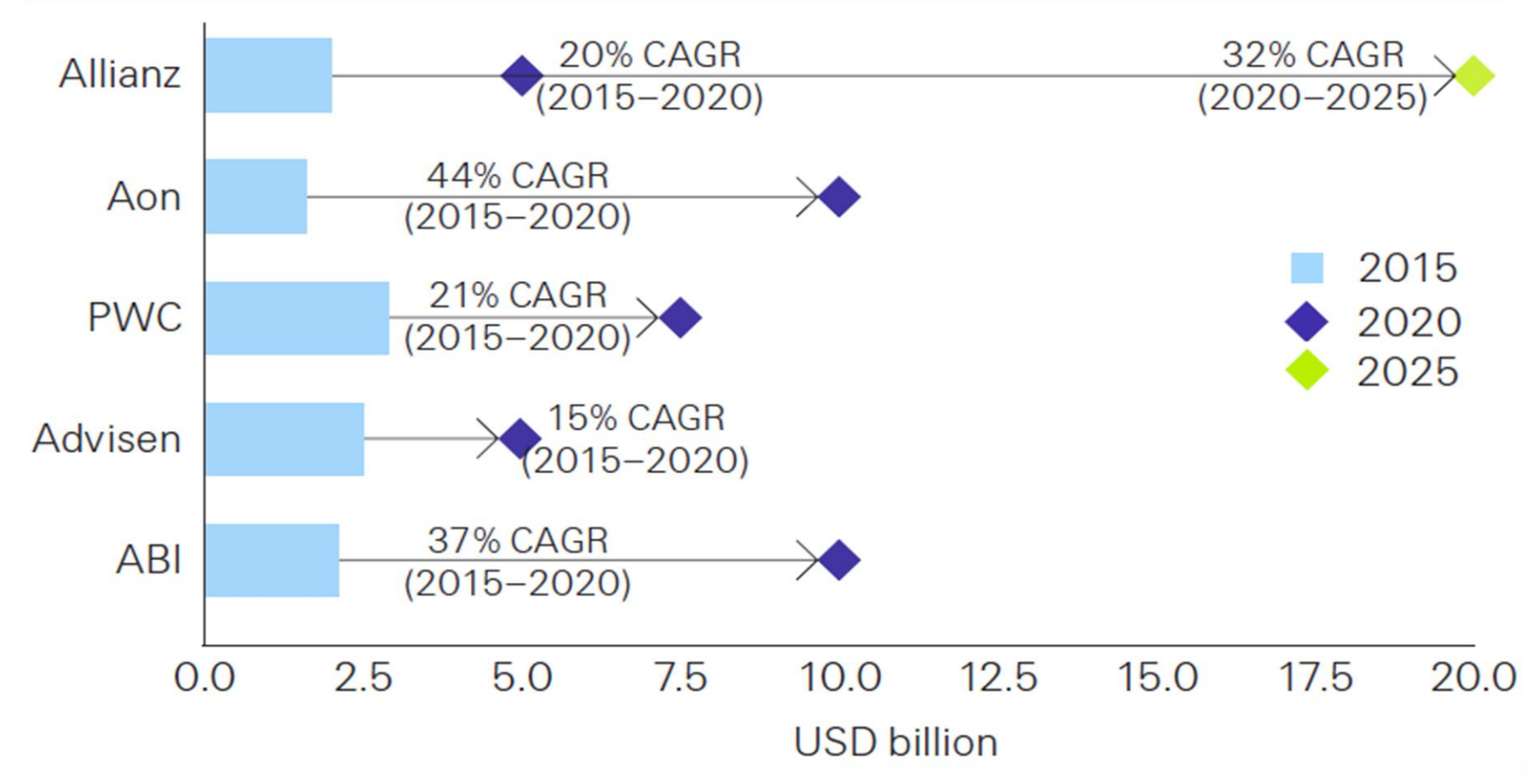
Published two months after a ransomware cyber-attack that hobbled NHS hospitals and hit nearly 100 countries, a 56-page report from the world's oldest insurance market says the threat posed by such global attacks has spiralled and poses a huge risk to business and governments over the next decade.

The most likely scenario is a malicious hack that takes down a cloud service

Cyber Insurance Markets

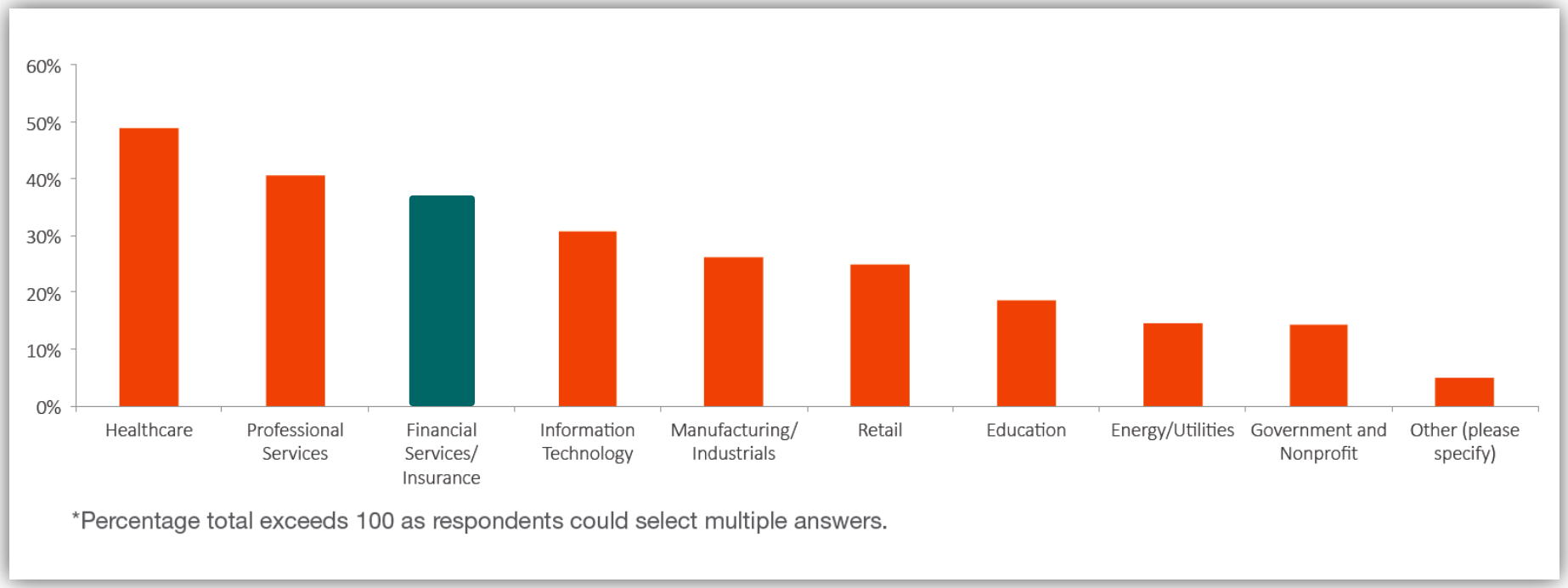
Cyber Insurance Markets

Estimates of Global Cyber Insurance Premiums (2015-2025)



Swiss Re (2017)

Industries Bringing Most New Buyers (2016)

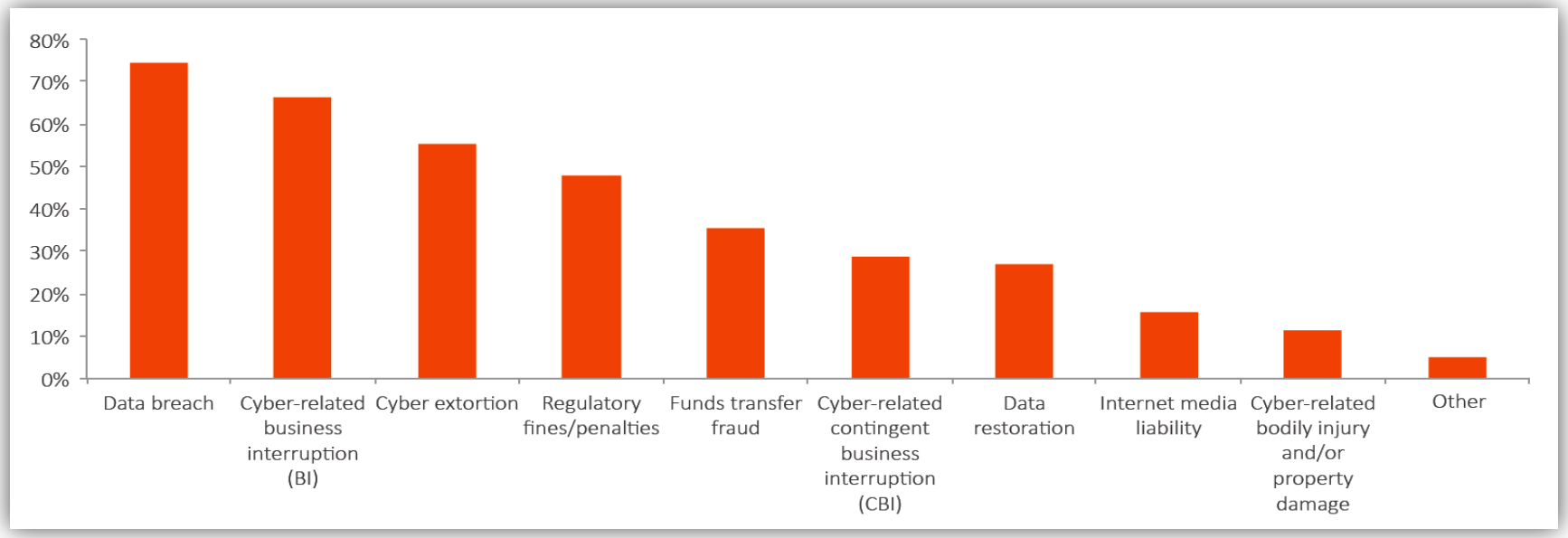


Advisen and PartnerRe (2016)

Cyber Insurance Consumption

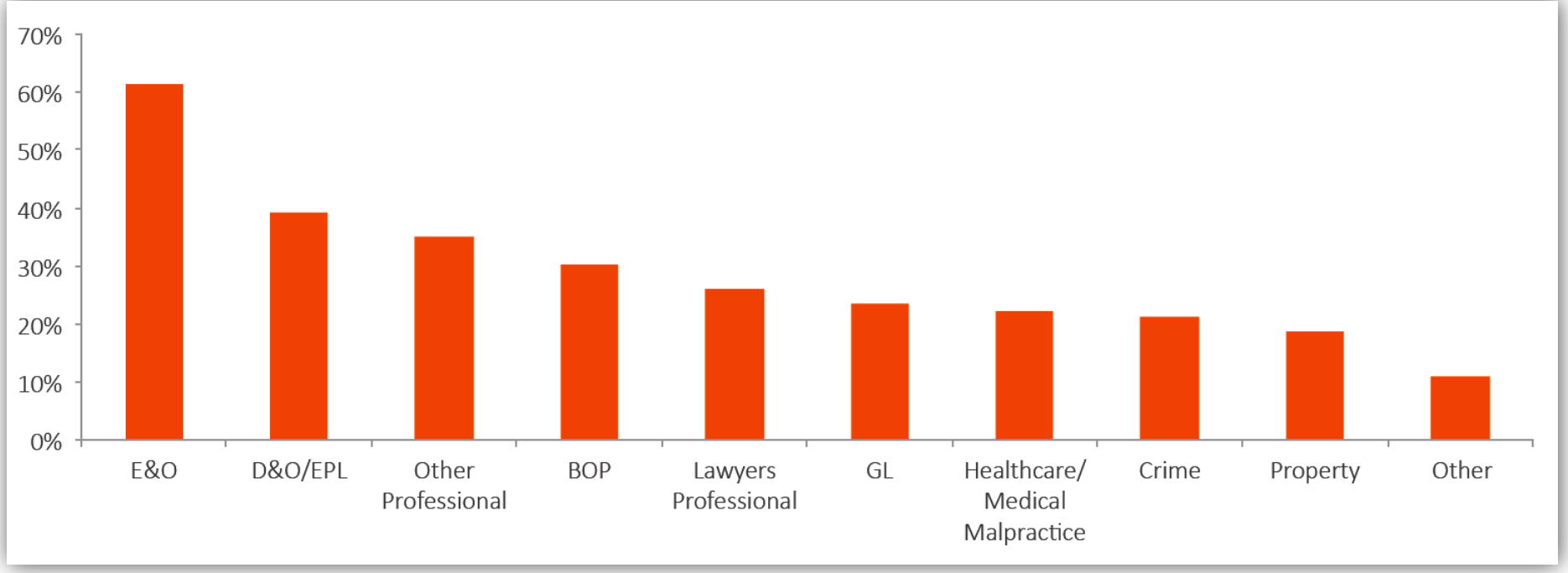
Cause of Consumption of First Party Coverages (New and Renewal)

- Data breach
- Cyber-related business income
- Cyber-extortion (ransomware)
- Regulatory fines and penalties



Cyber Insurance Consumption

Popularity of Coverage via Endorsement



Advisen and PartnerRe (2016)

Obstacles in the Cyber Insurance Market

2017 Deloitte Report

Insurer's Perspective

- Dearth of data
- Cyber attacks keep evolving
- Potential catastrophic accumulation
- Tunnel vision in coverages offered

Consumer's Perspective

- Buyers often don't understand cyber risks or their insurance options
- Cyber risk is spread over a wide range of coverages
- Cyber policies lack standardization
- The legal landscape remains in flux

Deloitte University (2017): Demystifying Cyber Insurance Coverage

Cyber Insurance Markets

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

Cyber Insurance Markets

Insurer's Perspective

- Difficulty in writing cyber coverages
  - Lack of historical data
  - Non-presence of contract standardization, potentially leading to claims disputes, litigation and low insurance consumption
- Reinsurers' reluctance in coverage offering due to fears of "concentrated unknown risks"
- Alternative risk transfer options
  - Self insurance
  - Captive (to buy reinsurance directly)
  - Insurance-linked securitization (ILS) (feasible in the near future?)

Deloitte University (2017): Demystifying Cyber Insurance Coverage

Cyber Insurance Policies Today

- No standard forms, different names
  - Digital risk, e-risk
  - First party and/or third party (liability) coverages
- Stand-alone or endorsement
  - ISO Exclusion Endorsement (CG 21 06 05 14) (2014)
- Frequently on claims-made
  - 30-60 day reporting period (after policy expiry)

Cyber Insurance Coverage Classification

Chief Risk Office Forum

Risk Management Society (RIMS)

Swiss Re

Cyber Risk Defined by the CRO Forum

- Any risks emanating from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks
- Physical damage that can be caused by cyber attacks
- Fraud committed by misuse of data
- Any liability arising from data use, storage and transfer
- The availability, integrity and confidentiality of electronic information – be it related to individuals, companies or governments

CRO Forum (2016)

Cyber Risk Defined by the CRO Forum

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
- D&O
- Tech E&O
- Professional services E&O, professional indemnity
- Environmental damage
- Physical asset damage
- Bodily injury and death

Cyber Insurance Coverages

RIMS (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

Santos (2017)

Cyber Insurance Coverages

Swiss Re (2017); Regrouped by Kwon

- First-party coverages
  - Network, IT security failure (BI)
  - Network, IT system failure (BI)
  - Contingent business interruption (CBI)
  - Cyber extortion
- Third-party coverages
  - Privacy breaches
  - Network liability
  - Errors and omissions (E&O)

Swiss Re (2017)

Issues in Cyber Risk Coverages and Gaps in the Market

Definitions?

Other Definitions

- Cyber attack
  - [AIG, denial of service attack] used but not defined
  - [Chubb] 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
  - [Zurich, 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

* Defined in Zurich Security and Privacy Protection Insurance.

Definitions

- Data
  - [AIG; electronic data] any software or electronic data stored electronically on, or that forms part of, a Computer System, but excluding Personal Information
  - [Chubb] a representation of information, knowledge, facts, concepts, or instructions which are being processed or have been processed in a Computer
    - Defines “record” (of a natural person) separately.
  - [Zurich; electronic data] information that exists in electronic form, including Personal Information; provided, however, [it] does not include Software

Cyber Insurance Policies

AIG - CyberEdge

AIG – CyberEdge

- Coverages
  - Cyber event response: event response costs incurred in response to a Security Failure that an Insured knows caused, or Suspects is likely to have caused, a Triggering Event
  - Cyber Follow Form Excess: coverage excess of the Underlying Limits for Loss caused by a Security Failure…in accordance with the same terms, conditions and limitations of the applicable Followed Policy….
  - Cyber Difference in Conditions: drop down and pay Loss caused by a Security Failure that would have been covered within an Underlying Policy…had one or more of the following not applied: (a) a Cyber Coverage Restriction; and/or (b) a Negligent Act* Requirement.

* Negligent Act defined as "the event, action or conduct…[resulting] from a negligent act, error or omission.

AIG – CyberEdge

- "Security failure" defined:
  - A failure or violation of the security of a Computer System that:
    - Results in, facilitates or fails to mitigate any: (i) unauthorized access or use; (ii) denial of service attack; or (iii) receipt, transmission or behavior of a malicious code; or
    - Results from the theft of a password or access code from an Entity Insured's premises, the Computer System, or an officer, director or employee of an Entity Insured by non-electronic means.
  - Not including any of the foregoing that results, directly or indirectly, from any: (1) natural or man-made earth movement, flood, earthquake, seaquake, shock, explosion, tremor, seismic event, lightning, fire, smoke, wind, water, landslide, submarine landslide, avalanche, subsidence, sinkhole collapse, mud flow, rock fall, volcanic activity, including eruption and lava flow, tidal wave, hail, or act of God; or (2) satellite or other infrastructure failure.

AIG – CyberEdge

- "Triggering event" defined:
  - A failure or violation of the security of a Computer System that the event, action or conduct that first triggers coverage under any Underlying Policy or would have triggered such coverage had a Cyber Coverage Restriction or a Negligent Act Requirement not applied.
  - A "Triggering Event" shall not mean a notice of circumstance; however, any event, action or conduct that first triggers coverage under an Underlying Policy due to a notice of circumstance will be deemed a Triggering Event under this policy at the time of such notice of circumstance to the Underlying Insurer.
  - "Triggering Event" shall not mean the Security Failure itself.

AIG – CyberEdge

- Exclusions including but not limited to:
  - Privacy and personal information and confidential information arising out of, based upon or attributable to any invasion of privacy; or any:
    - Theft, disappearance, destruction or other loss, disclosure, publication, collection, use or storage of;
    - Failure to protect, or exercise any duty of care with respect to; or
    - Failure to comply with any law (statutory or common), rule or regulation, or any policy concerning….

Cyber Insurance Policies

Chubb – Cyber Security Policy (2009 -)

Chubb – Cyber Security Policy

- Coverages
  - Privacy notification expenses
  - Crisis management and reward expenses (e.g., information security forensic investigation expenses, public relations expenses…)
  - E-business interruption and extra expenses
  - E-theft loss
  - E-communication loss
  - E-threat expenses
  - E-vandalism expenses
- Other contract elements (e.g., coverage limits, exclusions) relatively standard to other Chubb policies

Cyber Insurance Policies

Zurich – Security And Privacy Protection Policy (UK)

Zurich – Security And Privacy Protection Policy

- Coverages
  - Security and privacy liability
  - Regulatory proceedings
  - Internet media liability
  - Non-liability coverages
    - Privacy breach costs
    - Business income loss, dependent business income loss and extra expenses
    - Digital asset replacement expense
    - Cyber extortion threat and reward payments
- Other contract elements (e.g., coverage limits, exclusions) relatively standard to other Zurich policies

Summing Up…,

- Cyber risk is so dynamic and its definition constantly changing (although not necessarily expanding)
  - Claims-made coverages with a reasonable tail period thus suitable.
  - Still, challenges not only in capturing more client firms but also in competing with alternative risk financial tools
- Strong human behavioral and IT factors affecting cyber attack types and severities
- Policy standardization – stand-alone and endorsement – likely a requisite for the expansion of the cyber insurance market

W. Jean Kwon, Ph.D., CPCU
Edwin A.G. Manton Chair Professor in Int'l Insurance and Risk Management
Technical Committee (Insurance), Finance Accreditation Agency (Malaysia)
Director, Center for the Study of Insurance Regulation
Research Director, International Insurance Society
Chief Editor, Asia-Pacific Journal of Risk and Insurance

School of Risk Management, Insurance and Actuarial Science
St. John's University
101 Astor Place, New York, NY

KwonW@stjohns.edu